JUNIPER NETWORKS

# Junos® OS

## CLI Reference

Release
12.1X44-D10

Published: 2013-01-15

Copyright © 2013, Juniper Networks, Inc.

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

*Junos® OS CLI Reference*
Release 12.1X44-D10
Copyright © 2013, Juniper Networks, Inc.
All rights reserved.

Revision History
December 2012—Junos OS 12.1X44-D10

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions. Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details. For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

## END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

# Table of Contents


About This Guide . . . . . xlvii

J Series and SRX Series Documentation and Release Notes . . . . . xlvii
Objectives . . . . . xlviii
Audience . . . . . xlviii
Supported Routing Platforms . . . . . xlviii
Document Conventions . . . . . xlviii
Documentation Feedback . . . . . l
Requesting Technical Support . . . . . l
Self-Help Online Tools and Resources . . . . . li
Opening a Case with JTAC . . . . . li

Part 1 Configuration Statements

Chapter 1 Access Hierarchy and Statements . . . . . 3

Access Configuration Statement Hierarchy . . . . . 3
address-assignment (Access) . . . . . 8
address-pool (Access) . . . . . 10
admin-search . . . . . 11
assemble . . . . . 11
authentication-order (Access Profile) . . . . . 12
banner (Access FTP HTTP Telnet Authentication) . . . . . 12
banner (Access Web Authentication) . . . . . 13
base-distinguished-name . . . . . 14
client-group . . . . . 15
client-idle-timeout (Access Profile) . . . . . 15
client-name-filter . . . . . 16
client-session-timeout (Access Profile) . . . . . 16
configuration-file . . . . . 17
count . . . . . 17
default-profile . . . . . 18
dhcp-attributes (Access IPv4 Address Pools) . . . . . 19
dhcp-attributes (Access IPv6 Address Pools) . . . . . 20
distinguished-name (Access) . . . . . 21
domain-name (Access Profile) . . . . . 21
fail . . . . . 22
firewall-authentication . . . . . 23
firewall-user . . . . . 24
ftp (Access) . . . . . 24
group-profile (Access) . . . . . 25
http (Access) . . . . . 26
ip-address (Access Profile) . . . . . 26


Copyright © 2013, Juniper Networks, Inc.

ldap-options . . . 27
ldap-server . . . 28
link (Access) . . . 28
login (Access) . . . 29
name-server (Access) . . . 29
neighbor-discovery-router-advertisement (Access) . . . 30
network (Access) . . . 30
pass-through . . . 31
password (Access) . . . 32
pool (Access) . . . 33
port (Access LDAP) . . . 34
port (Access RADIUS) . . . 35
prefix (Access IPv6) . . . 35
profile (Access) . . . 36
radius-options (Access) . . . 37
radius-server (Access) . . . 38
range (Access) . . . 39
retry (Access LDAP) . . . 39
retry (Access RADIUS) . . . 40
revert-interval (Access LDAP) . . . 40
revert-interval (Access RADIUS) . . . 41
routing-instance (Access LDAP) . . . 41
routing-instance (Access RADIUS) . . . 42
search . . . 42
search-filter . . . 43
secret (Access Profile) . . . 43
securid-server . . . 44
separator . . . 45
session-options (Access Profile) . . . 45
source-address (Access LDAP) . . . 46
source-address (Access RADIUS) . . . 46
success . . . 47
telnet (Access) . . . 47
timeout (Access LDAP) . . . 48
timeout (Access RADIUS) . . . 48
traceoptions (Access) . . . 49
web-authentication (Access) . . . 50
wins-server (Access) . . . 51
xauth-attributes . . . 51

Chapter 2 **Accounting-Options Hierarchy . . . 53**

Accounting-Options Configuration Statement Hierarchy . . . 53

Chapter 3 **Applications Hierarchy and Statements . . . 55**

Applications Configuration Statement Hierarchy . . . 55
alg (Applications) . . . 57
application-protocol (Applications) . . . 58
description (Applications) . . . 59
destination-port (Applications) . . . 60
icmp-code (Applications) . . . 64


Copyright © 2013, Juniper Networks, Inc.

icmp-type (Applications) . . . 64
inactivity-timeout (Applications) . . . 65
protocol (Applications) . . . 66
rpc-program-number (Applications) . . . 67
source-port (Applications) . . . 67
term (Applications) . . . 68
uuid (Applications) . . . 69

Chapter 4 Bridge-Domains Hierarchy and Statements . . . 71

Bridge-Domains Configuration Statement Hierarchy . . . 71
bridge-domains (Bridge Domains) . . . 72
bridge-options (Bridge Domains) . . . 73
domain-type (Bridge Domains) . . . 73
interface (Bridge Domains) . . . 74
routing-interface (Bridge Domains) . . . 74
static-mac (Bridge Domains) . . . 75
vlan-id (Bridge Domain) . . . 76
vlan-id-list (Bridge Domains) . . . 77

Chapter 5 Chassis Hierarchy and Statements . . . 79

Chassis Configuration Statement Hierarchy . . . 79
apply-groups (Chassis Cluster) . . . 83
cluster (Chassis) . . . 84
control-link-recovery . . . 85
control-ports . . . 86
framing (Chassis) . . . 86
fru-poweron-sequence . . . 87
global-threshold . . . 88
global-weight . . . 89
gratuitous-arp-count . . . 90
heartbeat-interval . . . 91
heartbeat-threshold . . . 92
hold-down-interval . . . 93
interface (Chassis Cluster) . . . 94
interface-monitor . . . 95
ip-monitoring . . . 96
network-management . . . 97
node (Chassis Cluster) . . . 97
node (Chassis Cluster Redundancy Group) . . . 98
pic-mode (Chassis G.SHDSL) . . . 98
pic-mode (Chassis T1 Mode) . . . 99
pic-mode (Chassis uPIM) . . . 100
preempt (Chassis Cluster) . . . 101
priority (Chassis Cluster) . . . 101
redundancy-group (Chassis Cluster) . . . 102
reth-count (Chassis Cluster) . . . 103
retry-count (Chassis Cluster) . . . 104
retry-interval (Chassis Cluster) . . . 104
services-offload . . . 105
traceoptions (Chassis Cluster) . . . 106

Copyright © 2013, Juniper Networks, Inc.

tunnel-queuing . . . 107
weight . . . 108

Chapter 6 Class-of-Service Hierarchy and Statements . . . 109

Class-of-Service Configuration Statement Hierarchy . . . 109
adaptive-shaper . . . 113
adaptive-shapers . . . 114
application-traffic-control . . . 115
classifiers (CoS) . . . 116
code-points . . . 117
default (CoS) . . . 118
forwarding-classes (CoS) . . . 119
frame-relay-de (CoS Interfaces) . . . 120
frame-relay-de (CoS Loss Priority) . . . 121
frame-relay-de (CoS Rewrite Rule) . . . 122
interfaces (CoS) . . . 123
loss-priority (CoS Loss Priority) . . . 124
loss-priority (CoS Rewrite Rules) . . . 125
loss-priority-maps (CoS Interfaces) . . . 126
loss-priority-maps (CoS) . . . 127
rate-limiters . . . 128
rewrite-rules (CoS) . . . 129
rewrite-rules (CoS Interfaces) . . . 130
rule-sets (CoS AppQoS) . . . 131
scheduler-map (CoS Virtual Channels) . . . 133
shaping-rate (CoS Adaptive Shapers) . . . 134
shaping-rate (CoS Interfaces) . . . 135
shaping-rate (CoS Virtual Channels) . . . 136
trigger (CoS) . . . 137
virtual-channels . . . 137
virtual-channel-group (CoS Interfaces) . . . 138
virtual-channel-groups . . . 139

Chapter 7 Event-Options Hierarchy . . . 141

Event-Options Configuration Statement Hierarchy . . . 141

Chapter 8 Firewall Hierarchy and Statements . . . 143

Firewall Configuration Statement Hierarchy . . . 143
policer (Firewall) . . . 146
simple-filter (Firewall) . . . 147

Chapter 9 Forwarding-Options Hierarchy and Statements . . . 149

Forwarding-Options Configuration Statement Hierarchy . . . 149
hash-key (Forwarding Options) . . . 154
vpn (Forwarding Options) . . . 155

Chapter 10 Groups Hierarchy . . . 157

Groups Configuration Statement Hierarchy . . . 157


Copyright © 2013, Juniper Networks, Inc.

Chapter 11 Interfaces Hierarchy and Statements . . . . . 159

Interfaces Configuration Statement Hierarchy . . . . . 159
accept-source-mac . . . . . 172
access-point-name . . . . . 173
activation-priority (Interfaces) . . . . . 173
annex (Interfaces) . . . . . 174
apply-groups . . . . . 174
arp-resp . . . . . 175
authentication-method (Interfaces) . . . . . 175
bandwidth (Interfaces) . . . . . 176
bearer-bandwidth-limit (Interfaces) . . . . . 176
bundle (Interfaces) . . . . . 177
cbr rate . . . . . 177
cellular-options . . . . . 178
client-identifier (Interfaces) . . . . . 179
client-identifier (dhcp-client) . . . . . 179
compression-device (Interfaces) . . . . . 180
credit (Interfaces) . . . . . 180
data-rate . . . . . 181
dhcp (Interfaces) . . . . . 181
dhcp-client . . . . . 182
dynamic-call-admission-control (Interfaces) . . . . . 183
encapsulation (Interfaces) . . . . . 184
fabric-options . . . . . 185
family bridge . . . . . 186
family inet (Interfaces) . . . . . 187
family inet6 . . . . . 188
flag (Interfaces) . . . . . 189
flexible-vlan-tagging (Interfaces) . . . . . 190
flow-control (Interfaces) . . . . . 190
fpc (Interfaces) . . . . . 191
gsm-options . . . . . 191
hub-assist . . . . . 192
interface (PIC Bundle) . . . . . 192
interval (Interfaces) . . . . . 193
lacp (Interfaces) . . . . . 193
latency (Interfaces) . . . . . 194
lease-time . . . . . 194
lease-time (dhcp-client) . . . . . 195
line-rate (Interfaces) . . . . . 195
link-speed (Interfaces) . . . . . 196
loopback (Interfaces) . . . . . 196
media-type (Interfaces) . . . . . 197
member-interfaces . . . . . 197
minimum-links (Interfaces) . . . . . 198
native-vlan-id (Interfaces) . . . . . 199
next-hop-tunnel . . . . . 199
periodic (Interfaces) . . . . . 200
ppp-over-ether . . . . . 200

Copyright © 2013, Juniper Networks, Inc.

prefix . . . 201
profiles . . . 201
promiscuous-mode (Interfaces) . . . 202
quality (Interfaces) . . . 202
radio-router (Interfaces) . . . 203
redundancy-group (Interfaces) . . . 204
redundant-ether-options . . . 205
redundant-parent (Interfaces Fast Ethernet) . . . 205
redundant-parent (Interfaces Gigabit Ethernet) . . . 206
resource (Interfaces) . . . 206
retransmission-attempt . . . 207
retransmission-attempt (dhcp-client) . . . 207
retransmission-interval (dhcp-client) . . . 208
retransmission-interval (Interfaces) . . . 208
roaming-mode . . . 209
select-profile . . . 209
server-address . . . 210
server-address (dhcp-client) . . . 210
simple-filter (Interfaces) . . . 211
sip-password . . . 211
sip-user-id . . . 212
source-address-filter (Interfaces) . . . 213
source-filtering (Interfaces) . . . 214
speed (Interfaces) . . . 214
threshold (Interfaces) . . . 215
traceoptions (Interfaces) . . . 215
unframed | no-unframed (Interfaces) . . . 216
update-server . . . 216
update-server (dhcp-client) . . . 217
use-interface . . . 217
user-id . . . 217
vbr rate . . . 218
vdsl-profile . . . 219
vendor-id . . . 219
vendor-id (Interfaces) . . . 220
vlan-tagging (Interfaces) . . . 220
web-authentication (Interfaces) . . . 221

Chapter 12 **Logical-Systems Hierarchy and Statement . . . 223**

Logical-Systems Configuration Statement Hierarchy . . . 223
logical-systems (All) . . . 225

Chapter 13 **Power Over Ethernet Hierarchy and Statements . . . 227**

PoE Configuration Statement Hierarchy . . . 227
disable (PoE) . . . 228
duration (PoE) . . . 228
guard-band (PoE) . . . 229
interface (PoE) . . . 230
interval (PoE) . . . 231
management (PoE) . . . 231


Copyright © 2013, Juniper Networks, Inc.

maximum-power (PoE) . . . 232
priority (PoE) . . . 233
telemetries (PoE) . . . 234

Chapter 14 Policy-Options Hierarchy and Statements . . . 235

Policy-Options Configuration Statement Hierarchy . . . 235
condition (Policy Options) . . . 236
load-balance (Security Devices) . . . 237
multicast-scope . . . 238
route-active-on . . . 238

Chapter 15 Protocols Hierarchy and Statements . . . 239

Protocols Configuration Statement Hierarchy . . . 239
demand-circuit (Protocols RIP) . . . 261
disable (Protocols R2CP) . . . 262
global-mac-limit (Protocols) . . . 262
global-mac-table-aging-time (Protocols) . . . 263
global-no-mac-learning (Protocols) . . . 263
interface (Protocols R2CP) . . . 264
l2-learning (Protocols) . . . 264
max-retrans-time . . . 265
neighbor-discovery . . . 266
node-terminate-count . . . 266
node-terminate-interval . . . 267
onlink-subnet-only . . . 267
packet-action (Protocols) . . . 268
preference (Protocols ES-IS) . . . 268
r2cp . . . 269
radio . . . 270
radio-interface . . . 270
server-port . . . 271
session-terminate-count . . . 271
session-terminate-interval . . . 272
traceoptions (Protocols ES-IS) . . . 273
traceoptions (Protocols R2CP) . . . 275
virtual-channel-group . . . 276

Chapter 16 Routing-Instances Hierarchy . . . 277

Routing-Instances Configuration Statement Hierarchy . . . 277
mesh-group . . . 288
local-switching . . . 289

Chapter 17 Routing-Options Hierarchy . . . 291

Routing-Options Configuration Statement Hierarchy . . . 291

Chapter 18 Schedulers Hierarchy and Statements . . . 297

Schedulers Configuration Statement Hierarchy . . . 297
all-day . . . 298
daily . . . 299
description (Schedulers) . . . 300
exclude (Schedulers) . . . 301

Copyright © 2013, Juniper Networks, Inc. 

friday . . . 302
monday . . . 303
saturday . . . 304
scheduler (Security Policies) . . . 305
schedulers (Security Policies) . . . 306
start-date . . . 306
start-time (Schedulers) . . . 307
stop-date . . . 308
stop-time . . . 309
sunday . . . 310
thursday . . . 311
tuesday . . . 312
wednesday . . . 313

Chapter 19 Security Hierarchy and Statements . . . 315

[edit security] Hierarchy Level . . . 315
[edit security address-book] Hierarchy Level . . . 316
[edit security alarms] Hierarchy Level . . . 316
[edit security alg] Hierarchy Level . . . 317
[edit security analysis] Hierarchy Level . . . 322
[edit security application-firewall] Hierarchy Level . . . 322
[edit security application-tracking] Hierarchy Level . . . 322
[edit security certificates] Hierarchy Level . . . 323
[edit security datapath-debug] Hierarchy Level . . . 323
[edit security dynamic-vpn] Hierarchy Level . . . 324
[edit security firewall-authentication] Hierarchy Level . . . 325
[edit security flow] Hierarchy Level . . . 325
[edit security forwarding-options] Hierarchy Level . . . 326
[edit security forwarding-process] Hierarchy Level . . . 327
[edit security gprs] Hierarchy Level . . . 327
[edit security group-vpn] Hierarchy Level . . . 330
[edit security idp] Hierarchy Level . . . 333
[edit security ike] Hierarchy Level . . . 342
[edit security ipsec] Hierarchy Level . . . 344
[edit security log] Hierarchy Level . . . 345
[edit security nat] Hierarchy Level . . . 346
[edit security pki] Hierarchy Level . . . 349
[edit security policies] Hierarchy Level . . . 350
[edit security resource-manager] Hierarchy Level . . . 354
[edit security screen] Hierarchy Level . . . 354
[edit security softwires] Hierarchy Level . . . 356
[edit security ssh-known-hosts] Hierarchy Level . . . 356
[edit security traceoptions] Hierarchy Level . . . 357
[edit security user-identification] Hierarchy Level . . . 357
[edit security utm] Hierarchy Level . . . 357
[edit security zones] Hierarchy Level . . . 365
access-profile (Security Dynamic VPN) . . . 367
access-profile (Security IKE Gateway) . . . 367
ack-number . . . 368


Copyright © 2013, Juniper Networks, Inc.

action (APN GTP) . . . 369
action (Security Application-Level DDoS) . . . 370
action (Security Rulebase IPS) . . . 371
action (Security UTM Web Filtering) . . . 372
action-profile . . . 373
active-policy . . . 374
address (Security Address Book) . . . 375
address (Security ARP Proxy) . . . 376
address (Security Destination NAT) . . . 376
address (Security IKE Gateway) . . . 377
address (Security IKE Gateway Server) . . . 377
address (Security NDP Proxy) . . . 378
address (Security Source NAT) . . . 378
address-blacklist . . . 379
address-book . . . 380
address-mapping . . . 381
address-persistent . . . 382
address-set . . . 382
address-whitelist . . . 383
admin-email . . . 383
administrator . . . 384
administrator-email (Security Fallback Block) . . . 384
administrator-email (Security Virus Detection) . . . 385
aging . . . 385
alarm-threshold . . . 386
alarm-without-drop . . . 386
alarms (Security) . . . 387
alert . . . 388
alg . . . 389
ike-esp-nat . . . 394
alg-manager . . . 394
support-lib . . . 395
algorithm (Security) . . . 395
all-tcp . . . 396
allow-dns-reply . . . 396
allow-email (Security Fallback Block) . . . 397
allow-email (Security Virus Detection) . . . 397
allow-icmp-without-flow . . . 398
always-send . . . 398
analysis . . . 399
anomaly . . . 399
anti-spam (Security Feature Profile) . . . 400
anti-spam (Security UTM Policy) . . . 400
anti-virus (Security Feature Profile) . . . 401
anti-virus (Security UTM Policy) . . . 405
apn . . . 406
application (Security Alarms) . . . 407
application (Security Application-Level DDoS) . . . 408
application (Security Custom Attack) . . . 408

Copyright © 2013, Juniper Networks, Inc.

application (Security IDP) . . . 409
application (Security Policies) . . . 409
application-ddos . . . 410
application-ddos (Security IDP) . . . 411
application-ddos (Security IDP Policy) . . . 411
application-firewall . . . 412
application-firewall (Application Services) . . . 413
application-identification . . . 413
application-proxy (Security UTM) . . . 414
application-screen (Security H323) . . . 414
application-screen (Security MGCP) . . . 415
application-screen (Security SCCP) . . . 416
application-screen (Security SIP) . . . 417
application-services (Security Forwarding Process) . . . 418
application-services (Security Policies) . . . 420
application-tracking . . . 421
application-tracking (Security Zones) . . . 421
application-traffic-control (Application Services) . . . 422
association-timeout . . . 422
attach . . . 423
attack-threshold . . . 423
attacks (Security Exempt Rulebase) . . . 424
attacks (Security IPS Rulebase) . . . 425
attack-type (Security Anomaly) . . . 425
attack-type (Security Chain) . . . 426
attack-type (Security IDP) . . . 428
attack-type (Security Signature) . . . 432
audible (Security Alarms) . . . 436
authentication (Security Alarms) . . . 436
authentication (Security IPsec) . . . 437
authentication-algorithm (Security) . . . 438
authentication-algorithm (Security IPsec) . . . 439
authentication-method . . . 440
authentication-source . . . 441
auto-re-enrollment (Security) . . . 441
automatic (Security) . . . 442
bind-interface . . . 442
block-command . . . 443
block-content-type . . . 443
block-extension . . . 444
block-message (Security UTM) . . . 444
block-mime . . . 445
bridge . . . 446
c-timeout . . . 447
ca-identity (Security) . . . 447
ca-profile (Security) . . . 448
ca-profile-name . . . 449
cache . . . 449
cache (Security Log) . . . 450


Copyright © 2013, Juniper Networks, Inc.

cache-prune-chunk-size . . . 451
cache-size (Security) . . . 451
call-flood . . . 452
capture-file (Security) . . . 453
category (Security Dynamic Attack Group) . . . 454
category (Security Logging) . . . 455
category (Security Web Filtering) . . . 456
certificate . . . 462
certificate-id (Security) . . . 462
certificates . . . 463
certification-authority . . . 464
chain . . . 465
challenge-password (Security) . . . 466
clear-threshold . . . 466
clients (Security) . . . 467
co-location . . . 467
code . . . 468
config-check (Security Dynamic VPN) . . . 468
connection-flood . . . 469
connection-rate-threshold . . . 469
connections-limit . . . 470
container . . . 471
content-decompression-max-memory-kb . . . 472
content-decompression-max-ratio . . . 473
content-filtering (Security Feature Profile) . . . 474
content-filtering (Security UTM Policy) . . . 475
content-size . . . 476
content-size (Security Antivirus Sophos Engine) . . . 477
content-size-limit . . . 478
context (Security Application-Level DDoS) . . . 479
context (Security Custom Attack) . . . 479
corrupt-file . . . 480
count (Security Custom Attack) . . . 480
count (Security Policies) . . . 481
crl (Security) . . . 482
cryptographic-self-test . . . 483
custom-attack . . . 484
custom-attack-group . . . 489
custom-attack-groups (Security IDP) . . . 489
custom-attacks . . . 490
custom-block-message . . . 490
custom-message (Security Content Filtering) . . . 491
custom-message (Security Email Notify) . . . 491
custom-message (Security Fallback Block) . . . 492
custom-message (Security Fallback Non-Block) . . . 493
custom-message (Security Virus Detection) . . . 494
custom-message-subject (Security Email Notify) . . . 494
custom-message-subject (Security Fallback Block) . . . 495
custom-message-subject (Security Fallback Non-Block) . . . 496

Copyright © 2013, Juniper Networks, Inc.

custom-message-subject (Security Virus Detection) . . . . . 497
custom-objects . . . . . 498
custom-tag-string . . . . . 499
custom-url-category . . . . . 500
data-length . . . . . 501
datapath-debug . . . . . 502
dead-peer-detection . . . . . 503
decompress-layer . . . . . 504
decompress-layer-limit . . . . . 504
decryption-failures . . . . . 505
default (Security UTM) . . . . . 506
default (Security Antivirus) . . . . . 506
default (Security Antivirus Sophos Engine) . . . . . 507
default (Security Web Filtering) . . . . . 508
default-policy . . . . . 509
default-rule . . . . . 510
deny (Security Policies) . . . . . 510
deny (Security SIP) . . . . . 511
description (Security Address Book) . . . . . 512
description (Security IDP Policy) . . . . . 513
description (Security NAT Pool) . . . . . 514
description (Security NAT Rule) . . . . . 515
description (Security NAT Rule-Set) . . . . . 516
description (Security Policies) . . . . . 517
description (Security Screen) . . . . . 518
description (Security Zone) . . . . . 519
destination (Security Destination NAT) . . . . . 520
destination (Security IP Headers Attack) . . . . . 521
destination-address (Security Destination NAT) . . . . . 522
destination-address (Security IDP Policy) . . . . . 523
destination-address (Security Policies) . . . . . 524
destination-address (Security Policies Flag) . . . . . 525
destination-address (Security Source NAT) . . . . . 526
destination-address (Security Static NAT) . . . . . 526
destination-address-name (Security Destination NAT) . . . . . 527
destination-address-name (Security Source NAT) . . . . . 527
destination-address-name (Security Static NAT) . . . . . 528
destination-except . . . . . 528
destination-ip (Security Alarms) . . . . . 529
destination-ip (Security IPsec) . . . . . 530
destination-ip-based . . . . . 530
destination-nat . . . . . 531
destination-port (Security Destination NAT) . . . . . 531
destination-port (Security Signature Attack) . . . . . 532
destination-port (Security Source NAT) . . . . . 532
destination-port (Security Static NAT) . . . . . 533
destination-threshold . . . . . 533
detect-shellcode . . . . . 534
detector . . . . . 534


Copyright © 2013, Juniper Networks, Inc.

df-bit . . . 535
dh-group (Security) . . . 536
direction (Security Custom Attack) . . . 537
direction (Security Dynamic Attack Group) . . . 538
disable (Application Tracking) . . . 539
disable (PKI) . . . 539
disable-call-id-hiding . . . 539
display-host (Security Fallback Block) . . . 540
display-host (Security Virus Detection) . . . 540
distinguished-name (Security) . . . 541
dns . . . 542
download-profile (Security Antivirus FTP) . . . 543
download-profile (Security Content Filtering FTP) . . . 543
drop (Security GTP) . . . 544
drop (Security SCTP) . . . 549
dscp-rewrite . . . 551
dynamic (Security) . . . 552
dynamic-application . . . 552
dynamic-application-group . . . 553
dynamic-attack-group . . . 554
dynamic-attack-groups (Security IDP) . . . 555
dynamic-vpn . . . 556
early-ageout . . . 557
email-notify . . . 557
enable (GPRS GTP) . . . 558
enable . . . 558
enable-all-qmodules . . . 559
enable-packet-pool . . . 559
encryption (Security) . . . 560
encryption-algorithm (Security) . . . 561
encryption-failures . . . 562
endpoint-registration-timeout . . . 562
engine-not-ready . . . 563
engine-not-ready (Security Antivirus Sophos Engine) . . . 564
enrollment (Security) . . . 565
establish-tunnels . . . 566
event-rate . . . 566
exception (Security Antivirus Mime Whitelist) . . . 567
exception (Security Content Filtering) . . . 567
exclude (Security Log) . . . 568
exclude-context-values . . . 569
expression . . . 570
external-interface (Security IKE Gateway) . . . 571
external-interface (Security Manual SA) . . . 571
fallback-block (Security Antivirus) . . . 572
fallback-non-block (Security Antivirus) . . . 573
fallback-options (Security Antivirus Juniper Express Engine) . . . 574
fallback-options (Security Antivirus Kaspersky Lab Engine) . . . 575
fallback-options (Security Antivirus Sophos Engine) . . . 576

Copyright © 2013, Juniper Networks, Inc.

fallback-settings (Security Web Filtering) . . . 576
fallback-settings (Security Web Filtering Juniper Local) . . . 577
fallback-settings (Security Web Filtering Websense Redirect) . . . 577
false-positives . . . 578
family (Security Forwarding Options) . . . 579
feature-profile . . . 580
fifo-max-size (Security IDP) . . . 586
fifo-max-size (IPS) . . . 586
file (Security Log) . . . 587
filename-extension . . . 588
filters . . . 589
fin-no-ack . . . 590
firewall-authentication (Security) . . . 590
firewall-authentication (Security Policies) . . . 591
first-update . . . 591
first-update-interval . . . 592
flood (Security ICMP) . . . 593
flood (Security UDP) . . . 594
flow (Security Flow) . . . 595
flow (Security IDP) . . . 597
force-ip-reassembly . . . 597
force-upgrade . . . 598
format (Security Log) . . . 598
format (Security Log Stream) . . . 599
forwarding-options (Security) . . . 600
forwarding-process . . . 601
fragment . . . 601
from (Security NAT) . . . 602
from-zone (Security IDP Policy) . . . 602
from-zone (Security Policies) . . . 603
ftp (Security ALG) . . . 606
ftp (UTM Policy Anti-Virus) . . . 607
ftp (UTM Policy Content Filtering) . . . 607
functional-zone . . . 608
gatekeeper . . . 609
gateway (Security Group VPN Member IKE) . . . 609
gateway (Security Group VPN Server IKE) . . . 610
gateway (Security IKE) . . . 611
gateway (Security IPsec VPN) . . . 612
gateway (Security Manual SA) . . . 612
general-ikeid . . . 613
global (Security IDP) . . . 613
global (Security Policies) . . . 614
gprs . . . 616
gprs-gtp-profile . . . 619
gprs-sctp-profile . . . 619
gre-in . . . 620
gre-out . . . 621
group (Security Group VPN) . . . 622


Copyright © 2013, Juniper Networks, Inc.

group-members . . . 624
group-vpn . . . 625
gtp . . . 628
gtp-in-gtp-denied . . . 630
h323 . . . 631
handshake-timeout . . . 632
hash-based . . . 632
hash-table-size (Security IDP) . . . 633
header-length . . . 633
high-availability (Security IDP) . . . 634
high-watermark . . . 634
history . . . 635
hit-rate-threshold . . . 636
host (Security IDP Sensor Configuration) . . . 637
host (Security Log) . . . 637
host (Security Web Filtering) . . . 638
host-address-base . . . 638
host-inbound-traffic . . . 639
host (SSH Known Hosts) . . . 640
hostname . . . 641
http-profile (Security Antivirus) . . . 641
http-profile (Security Content Filtering) . . . 642
http-profile (Security Web Filtering) . . . 642
icmp (Security IDP Custom Attack) . . . 643
icmp (Security IDP Signature Attack) . . . 644
icmp (Security Screen) . . . 645
icmpv6 (Security IDP) . . . 645
identification (Security ICMP Headers) . . . 646
identification (Security IP Headers) . . . 646
idle-time . . . 647
idp (Application Services) . . . 647
idp (Security) . . . 648
idp (Security Alarms) . . . 657
idp-policy (Security) . . . 658
ids-option . . . 661
ignore-memory-overflow . . . 662
ignore-reassembly-overflow . . . 663
ignore-reassembly-memory-overflow |
no-ignore-reassembly-memory-overflow . . . 663
ignore-regular-expression . . . 664
ike (Security) . . . 665
ike (Security Group VPN Member) . . . 667
ike (Security Group VPN Server) . . . 668
ike (Security IPsec VPN) . . . 669
ike-phase1-failures . . . 670
ike-phase2-failures . . . 671
ike-policy (Security Gateway) . . . 672
ike-user-type . . . 672
imap-profile (Security UTM Policy Antivirus) . . . 673

Copyright © 2013, Juniper Networks, Inc.

imap-profile (Security UTM Policy Content Filtering) . . . 673
inactive-media-timeout (Security MGCP) . . . 674
inactive-media-timeout (Security SCCP) . . . 674
inactive-media-timeout (Security SIP) . . . 675
inactivity-timeout (Security Persistent NAT) . . . 675
include-destination-address . . . 676
inet (Security Dynamic Peer) . . . 676
inet (Security Static NAT) . . . 677
inet6 (Security Forwarding Options) . . . 677
inet6 (Security IKE Gateway) . . . 678
inline-tap . . . 678
install . . . 679
install-interval . . . 679
intelligent-prescreening . . . 680
interface (Security NAT ARP Proxy) . . . 681
interface (Security NAT NDP Proxy) . . . 681
interface (Security Source NAT) . . . 682
interface (Security Source NAT Rule Set) . . . 682
interface (Security Dynamic VPN) . . . 683
interfaces (Security Zones) . . . 684
interval (Security Antivirus) . . . 685
interval (Security IDP) . . . 686
interval (Security IKE) . . . 686
ip (Security IDP Custom Attack) . . . 687
ip (Security Screen) . . . 688
ipv4 (Security IDP Signature Attack) . . . 690
ip-action (Security Application-Level DDoS) . . . 691
ip-action (Security IDP Rulebase IPS) . . . 692
ip-block . . . 693
ip-close . . . 693
ip-connection-rate-limit . . . 694
ip-flags . . . 695
ip-notify . . . 695
ip-sweep . . . 696
ipc . . . 697
ips . . . 698
ipsec (Security) . . . 699
ipsec (Security Group VPN Member) . . . 701
ipsec (Security Group VPN Server) . . . 702
ipsec-group-vpn (Security Policies) . . . 702
ipsec-policy (Security) . . . 703
ipsec-sa . . . 704
ipsec-vpn (Security Dynamic VPNs) . . . 705
ipsec-vpn (Security Flow) . . . 705
ipsec-vpn (Security Policies) . . . 706
ipv6 (Security IDP) . . . 706
iso (Security Forwarding Options) . . . 707
juniper-enhanced . . . 708
juniper-express-engine . . . 709


Copyright © 2013, Juniper Networks, Inc.

juniper-local . . . 710
kaspersky-lab-engine . . . 711
key-generation-self-test . . . 712
key-protection (Security) . . . 713
key-protection (Security IDP Sensor Configuration) . . . 713
land . . . 714
large . . . 714
lifetime-kilobytes . . . 715
lifetime-seconds (Security Group VPN) . . . 715
lifetime-seconds (Security IKE) . . . 716
lifetime-seconds (Security IPsec) . . . 716
limit (Security Log) . . . 717
limit (Security SCTP) . . . 718
limit (UTM Policy) . . . 719
limit-session . . . 719
list (Security Antivirus Mime Whitelist) . . . 720
list (Security Content Filtering Block Mime) . . . 720
load-distribution . . . 721
local (Certificates) . . . 721
local (Security IPsec) . . . 722
local-address (Security Group VPN) . . . 722
local-authentication-table . . . 723
local-certificate (Security) . . . 724
local-identity . . . 725
log (Security) . . . 726
log (Security GTP) . . . 728
log (Security IDP) . . . 729
log (Security IDP Policy) . . . 729
log (Security Policies) . . . 730
log (Security SCTP) . . . 730
log-attacks . . . 731
log-create . . . 731
log-errors . . . 732
log-supercede-min . . . 732
low-watermark . . . 733
management (Security Zones) . . . 734
manual (Security IPsec) . . . 735
mapped-port (Security Static NAT) . . . 736
application-firewall . . . 737
match (Security Destination NAT) . . . 738
match (Security IDP Policy) . . . 739
match (Security Policies) . . . 740
match (Security Rulebase DDoS) . . . 741
match (Security Source NAT) . . . 742
match (Security Static NAT) . . . 742
max-context-values . . . 743
max-flow-mem . . . 743
max-logs-operate . . . 744
max-message-length . . . 744

Copyright © 2013, Juniper Networks, Inc.

max-packet-mem . . . 745
max-packet-memory . . . 745
max-session-number . . . 746
max-sessions (Security Packet Log) . . . 746
max-tcp-session-packet-memory . . . 747
max-time-report . . . 747
max-timers-poll-ticks . . . 748
max-udp-session-packet-memory . . . 748
maximize-idp-sessions . . . 749
maximum-cache-size . . . 749
maximum-call-duration (Security) . . . 750
maximum-capture-size (Datapath Debug) . . . 750
maximum-message-length . . . 751
imsi-prefix . . . 751
media-source-port-any . . . 752
member (Security Group VPN) . . . 753
member (Security IDP) . . . 754
message-flood (Security H323) . . . 755
message-flood (Security MGCP) . . . 756
mgcp . . . 757
mime-pattern . . . 758
mime-whitelist . . . 759
min-message-length . . . 760
mode (Security Forwarding Options) . . . 761
mode (Security IKE Policy) . . . 762
mode (Security Log) . . . 763
mpls (Security Forwarding Options) . . . 764
msrpc . . . 765
mss (Security IDP) . . . 766
nat . . . 767
nat-keepalive . . . 770
negate . . . 771
nested-application (Security IDP) . . . 771
no-anti-replay (Security) . . . 772
no-autoupdate . . . 772
no-intelligent-prescreening . . . 773
no-nat-traversal . . . 773
no-notify-mail-recipient . . . 774
no-notify-mail-sender (Security Content Filtering Notification Options) . . . 774
no-notify-mail-sender (Security Fallback Block) . . . 775
no-notify-mail-sender (Security Virus Detection) . . . 776
no-policy-cold-synchronization . . . 776
no-sbl-default-server . . . 777
no-sequence-check . . . 777
no-syn-check . . . 778
no-syn-check-in-tunnel . . . 778
no-uri-check . . . 779
non-cryptographic-self-test . . . 779
notification . . . 780


Copyright © 2013, Juniper Networks, Inc.

notification (Security IDP Policy) . . . 781
notification-options (Security Antivirus) . . . 782
notification-options (Security Content Filtering) . . . 783
notify-mail-recipient . . . 783
notify-mail-sender (Security Content Filtering Notification Options) . . . 784
notify-mail-sender (Security Fallback Block) . . . 784
notify-mail-sender (Security Virus Detection) . . . 785
number . . . 785
optimized . . . 786
option (Security IDP) . . . 786
order (Security IDP) . . . 787
out-of-resources . . . 787
out-of-resources (Security Antivirus Sophos Engine) . . . 788
over-limit . . . 788
overflow-pool . . . 789
packet-filter . . . 790
packet-log (Security IDP Policy) . . . 791
packet-log (Security IDP Sensor Configuration) . . . 792
pair-policy . . . 793
pass-through . . . 794
password (Security Antivirus) . . . 795
password-file . . . 795
pattern (Security IDP) . . . 796
pattern-update (Security Antivirus) . . . 797
peer-certificate-type . . . 798
pending-sess-queue-length . . . 798
perfect-forward-secrecy (Security IPsec) . . . 799
performance . . . 800
permit (Security Persistent NAT) . . . 801
permit (Security Policies) . . . 802
permit-command . . . 803
persistent-nat . . . 804
ping-death . . . 804
pki . . . 805
policies . . . 807
policy (Security Alarms) . . . 811
policy (Security IKE) . . . 812
policy (Security IPsec) . . . 813
policy (Security Policies) . . . 814
policy-lookup-cache . . . 816
policy-match . . . 817
policy-rematch . . . 818
pool (Security Destination NAT) . . . 818
pool (Security Source NAT) . . . 819
pool (Security Source NAT Rule Set) . . . 820
pool-default-port-range . . . 820
pool-utilization-alarm . . . 821
pop3-profile (Security UTM Policy Antivirus) . . . 821
pop3-profile (Security UTM Policy Content Filtering) . . . 822

Copyright © 2013, Juniper Networks, Inc.

port (Security Antivirus) . . . 822
port (Security NAT) . . . 823
port (Security Web Filtering Server) . . . 823
port-overloading (Security NAT Source) . . . 824
port-overloading-factor . . . 824
port-randomization . . . 825
port-scan . . . 826
post-attack . . . 827
post-attack-timeout . . . 827
potential-violation . . . 828
pptp . . . 829
pre-attack . . . 830
pre-filter-shellcode . . . 830
pre-shared-key (Security IKE Policy) . . . 831
predefined-attack-groups . . . 831
predefined-attacks . . . 832
prefix (Security Static NAT) . . . 833
prefix-name (Security Static NAT) . . . 834
process-ignore-s2c . . . 834
process-override . . . 835
process-port . . . 835
products . . . 836
profile (Security Antispam SBL) . . . 836
profile (Security Antivirus Juniper Express Engine) . . . 837
profile (Security Antivirus Kaspersky Lab Engine) . . . 839
profile (Security Content Filtering) . . . 840
profile (Security GTP) . . . 841
profile (Security SCTP) . . . 843
profile (Security Sophos Engine Antivirus) . . . 845
profile (Security Web Filtering Juniper Enhanced) . . . 846
profile (Security Web Filtering Juniper Local) . . . 847
profile (Security Web Filtering Surf Control Integrated) . . . 848
profile (Security Web Filtering Websense Redirect) . . . 849
proposal (Security Group VPN Server IKE) . . . 850
proposal (Security IKE) . . . 851
proposal (Security IPsec) . . . 852
proposal-set (Security IKE) . . . 853
proposal-set (Security IPsec) . . . 854
proposals (Security IKE) . . . 855
proposals (Security IPsec) . . . 855
protect . . . 856
protocol (Security Destination NAT) . . . 856
protocol (Security IDP IP Headers) . . . 857
protocol (Security IDP Signature Attack) . . . 858
protocol (Security IPsec) . . . 861
protocol (Security IPsec Manual SA) . . . 862
protocol (Security Source NAT) . . . 862
protocol-binding . . . 863
protocol-command . . . 864


Copyright © 2013, Juniper Networks, Inc.

protocol-name . . . 865
protocols (Security Zones Host Inbound Traffic) . . . 866
protocols (Security Zones Interfaces) . . . 868
proxy (Security Antivirus) . . . 869
proxy-arp (Security NAT) . . . 870
proxy-identity . . . 870
proxy-ndp (Security NAT) . . . 871
quarantine-message (Security UTM) . . . 871
raise-threshold . . . 872
range-address . . . 872
rate-limit (Security GTP) . . . 873
re-assembler . . . 873
re-enroll-trigger-time-percentage (Security PKI) . . . 874
re-generate-keypair . . . 874
real . . . 875
recommended . . . 875
recommended-action . . . 876
redirect-wx (Application Services) . . . 877
refresh-timeout . . . 877
regexp . . . 878
reject (Security) . . . 878
reject-timeout . . . 879
remote (Security IPsec) . . . 879
remote-exceptions . . . 880
remote-identity . . . 881
remote-protected-resources . . . 882
remove-ie . . . 882
replay-attacks . . . 883
reset (Security IDP) . . . 883
reset-on-policy . . . 884
resource-manager . . . 884
respond-bad-spi . . . 885
restart-path . . . 886
retain-hold-resource . . . 886
revocation-check (Security PKI) . . . 887
route-change-timeout . . . 887
routing-instance (Security Destination NAT) . . . 888
routing-instance (Security PKI) . . . 888
routing-instance (Security Source NAT) . . . 889
routing-engine (SNMP) Global Level . . . 890
routing-engine (SNMP) Resource Level . . . 891
rpc . . . 892
rsh . . . 893
rst-invalidate-session . . . 893
rst-sequence-check . . . 894
rtsp . . . 894
rule (Security DDoS Rulebase) . . . 895
rule (Security Destination NAT) . . . 896
rule (Security Exempt Rulebase) . . . 897

Copyright © 2013, Juniper Networks, Inc.

rule (Security IPS Rulebase) . . . 898
rule (Security Source NAT) . . . 900
rule (Security Static NAT) . . . 901
rule-set (Security Destination NAT) . . . 902
rule-set (Security Source NAT) . . . 903
rule-set (Security Static NAT) . . . 905
rule-sets (Security Application Firewall) . . . 906
rulebase-ddos . . . 907
rulebase-exempt . . . 908
rulebase-ips . . . 909
sbl . . . 910
sbl-default-server . . . 911
scan-extension . . . 911
scan-mode . . . 912
scan-options (Security Antivirus Juniper Express Engine) . . . 912
scan-options (Security Antivirus Kaspersky Lab Engine) . . . 913
scan-options (Security Antivirus Sophos Engine) . . . 913
sccp . . . 914
scheduler-name . . . 915
scope (Security IDP Chain Attack) . . . 915
scope (Security IDP Custom Attack) . . . 916
screen (Security) . . . 917
screen (Security Zones) . . . 919
sctp . . . 920
security-log-percent-full . . . 921
security-package . . . 922
security-zone . . . 923
sensor-configuration . . . 925
sequence-check-required . . . 927
sequence-number (Security IDP ICMP Headers) . . . 927
sequence-number (Security IDP TCP Headers) . . . 928
server (Security Antivirus) . . . 928
server (Security Group VPN) . . . 929
server (Security Web Filtering) . . . 931
server-connectivity . . . 932
server-member-communication . . . 933
service (Security IDP Anomaly Attack) . . . 934
service (Security IDP DDoS) . . . 934
service (Security IDP Dynamic Attack Group) . . . 935
service (Security IPsec) . . . 935
services-offload (Security) . . . 936
session-affinity . . . 936
session-close . . . 936
session-distribution-mode . . . 937
session-id-cache-timeout . . . 937
session-init . . . 938
session-update-interval . . . 938
sessions . . . 939
sessions-per-client . . . 939


Copyright © 2013, Juniper Networks, Inc.

severity (Security IDP Custom Attack) . . . 940
severity (Security IDP Dynamic Attack Group) . . . 941
severity (Security IDP IPS Rulebase) . . . 942
severity (Security Log) . . . 943
shellcode . . . 944
signature (Security IDP) . . . 945
sip (Security) . . . 949
site-reputation-action . . . 950
size (Security Web Filtering Cache) . . . 951
smtp-profile (Security UTM Policy Antispam) . . . 951
smtp-profile (Security UTM Policy Antivirus) . . . 952
smtp-profile (Security UTM Policy Content Filtering) . . . 952
sockets . . . 953
softwires . . . 954
sophos-engine . . . 955
source (Security IDP IP Headers) . . . 956
source (Security Source NAT) . . . 957
source-address (Security Destination NAT) . . . 959
source-address (Security IDP) . . . 959
source-address (Security IDP Policy) . . . 960
source-address (Security IDP Sensor Configuration) . . . 960
source-address (Security Policies) . . . 961
source-address (Security Source NAT) . . . 962
source-address-name (Security Destination NAT) . . . 962
source-address-name (Security Source NAT) . . . 963
source-except . . . 963
source-identity . . . 964
source-interface (Security) . . . 965
source-ip (Security Alarms) . . . 966
source-ip-based . . . 967
source-nat . . . 968
source-port (Security IDP) . . . 969
source-threshold . . . 970
spam-action . . . 970
spi (Security IPsec) . . . 971
sql . . . 972
ssh-known-hosts . . . 973
ssl-encryption . . . 974
ssl-inspection . . . 974
ssl-proxy (Application Services) . . . 975
ssl-termination-profile . . . 975
start-log . . . 976
start-time (Security IDP) . . . 976
static (Security NAT) . . . 977
static-nat . . . 978
statistics (Security IDP) . . . 979
stream (Security Log) . . . 980
strict-syn-check . . . 980
sunrpc . . . 981

Copyright © 2013, Juniper Networks, Inc.

suppression . . . 982
surf-control-integrated . . . 983
sxl-retry . . . 984
sxl-timeout . . . 984
syn-ack-ack-proxy . . . 985
syn-check-required . . . 985
syn-fin . . . 986
syn-flood . . . 986
syn-flood-protection-mode . . . 987
syn-frag . . . 987
system-services (Security Zones Host Inbound Traffic) . . . 988
system-services (Security Zones Interfaces) . . . 990
t1-interval . . . 991
t4-interval . . . 992
talk . . . 993
target (Security IDP) . . . 994
tcp (Security IDP Protocol Binding) . . . 995
tcp (Security IDP Signature Attack) . . . 996
tcp (Security Screen) . . . 998
tcp-flags . . . 999
tcp-initial-timeout . . . 1000
tcp-mss (Security Flow) . . . 1001
tcp-no-flag . . . 1001
tcp-options (Security Policies) . . . 1002
tcp-rst . . . 1002
tcp-session . . . 1003
tcp-sweep . . . 1004
terminal . . . 1004
test (Security IDP) . . . 1005
tftp (Security ALG) . . . 1006
then (Security Application Firewall) . . . 1007
then (Security Destination NAT) . . . 1008
then (Security IDP Policy) . . . 1009
then (Security Policies) . . . 1010
then (Security Rulebase DDos) . . . 1012
then (Security Source NAT) . . . 1013
then (Security Static NAT) . . . 1014
threshold (Security IKE Gateway) . . . 1015
time-binding . . . 1016
time-binding-count . . . 1016
time-binding-period statement . . . 1017
time-wait-state . . . 1018
timeout (Security Antivirus Fallback Options) . . . 1019
timeout (Security Antivirus Fallback Options Sophos Engine) . . . 1020
timeout (Security Antivirus Scan Options) . . . 1021
timeout (Security IDP Policy) . . . 1022
timeout (Security GTP) . . . 1022
timeout (Security Screen) . . . 1023
timeout (Security Web Filtering) . . . 1023


Copyright © 2013, Juniper Networks, Inc.

timeout (Security Web Filtering Cache) . . . 1024
timeout (Security Web Filtering Fallback Settings) . . . 1024
to (Security Source NAT) . . . 1025
to-zone (Security IDP Policy) . . . 1025
to-zone (Security Policies) . . . 1026
too-many-requests (Security Antivirus Fallback Options) . . . 1028
too-many-requests (Security Antivirus Fallback Options Sophos Engine) . . . 1029
too-many-requests (Security Web Filtering Fallback Settings) . . . 1030
tos . . . 1031
total-length . . . 1032
total-memory . . . 1032
traceoptions (Security) . . . 1033
traceoptions (Security ALG) . . . 1035
traceoptions (Security Antispam) . . . 1036
traceoptions (Security Antivirus) . . . 1037
traceoptions (Security Application Firewall) . . . 1038
traceoptions (Security Application Proxy) . . . 1040
traceoptions (Security Content Filtering) . . . 1041
traceoptions (Security Datapath Debug) . . . 1042
traceoptions (Security Dynamic VPN) . . . 1043
traceoptions (Security Firewall Authentication) . . . 1044
traceoptions (Security Flow) . . . 1045
traceoptions (Security Group VPN) . . . 1047
traceoptions (Security GTP) . . . 1049
traceoptions (Security H323 ALG) . . . 1051
traceoptions (Security IDP) . . . 1052
traceoptions (Security IKE) . . . 1054
traceoptions (Security IPsec) . . . 1056
traceoptions (Security Log) . . . 1057
traceoptions (Security MGCP ALG) . . . 1059
traceoptions (Security NAT) . . . 1060
traceoptions (Security PKI) . . . 1062
traceoptions (Security Policies) . . . 1064
traceoptions (Security SCCP ALG) . . . 1066
traceoptions (Security Screen) . . . 1067
traceoptions (Security SCTP) . . . 1069
traceoptions (Security SIP ALG) . . . 1071
traceoptions (Security User Identification) . . . 1072
traceoptions (Security UTM) . . . 1073
traceoptions (Security Web Filtering) . . . 1074
traffic-options . . . 1075
transaction-timeout . . . 1075
trickling . . . 1076
ttl (Security IDP) . . . 1077
tunable-name . . . 1078
tunable-value . . . 1078
tunnel (Security Policies) . . . 1079
type (Security Antivirus Feature Profile) . . . 1079
type (Security Content Filtering Notification Options) . . . 1080

Copyright © 2013, Juniper Networks, Inc.

type (Security Fallback Block) . . . 1080
type (Security IDP Dynamic Attack Group) . . . 1081
type (Security IDP ICMP Headers) . . . 1081
type (Security Virus Detection) . . . 1082
type (Security Web Filtering) . . . 1083
uac-policy (Application Services) . . . 1083
udp (Security IDP Protocol Binding) . . . 1084
udp (Security IDP Signature Attack) . . . 1085
udp (Security Screen) . . . 1086
udp-anticipated-timeout (Security IDP) . . . 1086
udp-sweep . . . 1087
unified-access-control . . . 1088
unknown-message (Security H323 ALG) . . . 1089
unknown-message (Security MGCP ALG) . . . 1090
unknown-message (Security SCCP ALG) . . . 1091
unknown-message (Security SIP ALG) . . . 1092
upload-profile (Security Antivirus FTP) . . . 1093
upload-profile (Security Content Filtering FTP) . . . 1093
urgent-pointer . . . 1094
uri-check . . . 1094
url (Security Antivirus) . . . 1095
url (Security IDP) . . . 1095
url-blacklist . . . 1096
url-pattern . . . 1097
url-whitelist (Security Antivirus) . . . 1098
url-whitelist (Security Web Filtering) . . . 1098
user (Security Dynamic VPN) . . . 1099
user-at-hostname . . . 1099
user-groups (Security Dynamic VPN) . . . 1100
user-identification . . . 1100
username (Security Antivirus) . . . 1101
utm . . . 1102
utm-policy . . . 1110
utm-policy (Application Services) . . . 1111
value-hit-rate-threshold . . . 1112
version (Security GTP) . . . 1113
version (Security IKE Gateway) . . . 1114
virus-detection (Security Antivirus) . . . 1115
vpn (Security) . . . 1116
vpn-monitor . . . 1117
vpn-monitor-options . . . 1118
web-authentication . . . 1119
web-filtering . . . 1120
web-redirect . . . 1122
web-redirect-to-https . . . 1123
websense-redirect . . . 1124
weight (Security) . . . 1125
white-list . . . 1126
wildcard . . . 1127


Copyright © 2013, Juniper Networks, Inc.

window-scale . . . 1128
window-size . . . 1129
winnuke . . . 1129
xauth . . . 1130
zones . . . 1131

Chapter 20 Services Hierarchy and Statements . . . 1133

Services Configuration Statement Hierarchy . . . 1133
actions (Services) . . . 1137
address (Services) . . . 1138
application (Services) . . . 1139
application-group (Services) . . . 1141
application-identification . . . 1142
application-system-cache . . . 1144
application-system-cache-timeout (Services) . . . 1145
ca-profile (Services) . . . 1145
captive-portal (Services UAC) . . . 1146
captive-portal (Services UAC Policy) . . . 1147
certificate-verification . . . 1148
custom-ciphers . . . 1149
download (Services) . . . 1150
dscp-rewrite . . . 1151
enable-flow-tracing (Services) . . . 1151
enable-heuristics (Services) . . . 1152
enable-session-cache . . . 1152
file (Services) . . . 1153
files (Services) . . . 1153
flag (Services) . . . 1154
flow-monitoring (Services) . . . 1154
flow-monitoring version 9 . . . 1155
flow-monitoring version 9 template . . . 1155
flow-server (Forwarding Options) . . . 1156
global-config (Services) . . . 1157
flow-server version 9 . . . 1157
infranet-controller . . . 1158
inline-jflow (Forwarding Options) . . . 1159
interface (Services) . . . 1159
interval (Services) . . . 1160
level (Services) . . . 1160
log (Services) . . . 1161
match (Services) . . . 1162
max-checked-bytes (Services) . . . 1162
max-sessions (Services) . . . 1163
nested-application (Services) . . . 1164
nested-application-settings (Services) . . . 1165
nested-application-system-cache . . . 1166
no-application-identification (Services) . . . 1166
no-application-system-cache (Services) . . . 1167
no-remote-trace (Services) . . . 1167

Copyright © 2013, Juniper Networks, Inc.

option-refresh-rate (Services) . . . 1168
password (Services) . . . 1168
port (Services) . . . 1169
preferred-ciphers . . . 1169
profile (Services) . . . 1170
protocol-version . . . 1171
proxy (Services) . . . 1172
redirect-traffic . . . 1173
redirect-url . . . 1174
renegotiation (Services) . . . 1175
root-ca (Services) . . . 1175
server-certificate (Services) . . . 1176
server-certificate-subject . . . 1176
signature (Services) . . . 1177
ssl (Services) . . . 1179
size (Services) . . . 1181
statistics (Services) . . . 1181
template-refresh-rate (Services) . . . 1182
termination (Services) . . . 1183
test-only-mode . . . 1184
timeout (Services) . . . 1185
timeout-action . . . 1186
traceoptions (Services) . . . 1187
traceoptions (Services Application Identification) . . . 1188
traceoptions (Services UAC) . . . 1189
trusted-ca (Services) . . . 1190
unified-access-control . . . 1191
whitelist (Services) . . . 1192
wireless-wan . . . 1193

Chapter 21 SMTP Hierarchy and Statements . . . 1195

SMTP Configuration Statement Hierarchy . . . 1195
flag (SMTP) . . . 1196
primary-server . . . 1197
secondary-server . . . 1197
traceoptions (SMTP) . . . 1198

Chapter 22 SNMP Hierarchy and Statements . . . 1199

SNMP Configuration Statement Hierarchy . . . 1199
authorization (SNMP) . . . 1203
client-list-name (SNMP) . . . 1204

Chapter 23 System Hierarchy and Statements . . . 1205

System Configuration Statement Hierarchy . . . 1205
address-book . . . 1220
after-keygeneration . . . 1221
allow-duplicates . . . 1221
appfw-rule-set . . . 1222
appfw-rule . . . 1223
auth-entry . . . 1224


Copyright © 2013, Juniper Networks, Inc.

ciphers . . . 1225
cpu . . . 1226
day-of-month . . . 1227
day-of-week . . . 1228
dhcpv6 (System Services) . . . 1229
dhcp-local-server (System Services) . . . 1231
disable (System Services) . . . 1234
dlv . . . 1234
dns (System Services) . . . 1235
dns-proxy . . . 1236
dnssec . . . 1237
dslite-softwire-initiator . . . 1238
dynamic-dns . . . 1239
self-test . . . 1240
firewall-authentication-service . . . 1241
flow-gate . . . 1242
flow-session . . . 1243
general-authentication-service . . . 1244
group (System Services DHCP) . . . 1245
hostkey-algorithm . . . 1246
idp-policy . . . 1247
interface (System Services DHCP) . . . 1248
interface-traceoptions (System Services DHCP) . . . 1249
key-exchange . . . 1251
logical-system (System Security Profile) . . . 1252
lockout-period . . . 1252
macs . . . 1253
month . . . 1254
nat-cone-binding . . . 1255
nat-destination-pool . . . 1256
nat-destination-rule . . . 1257
nat-nopat-address . . . 1258
nat-pat-address . . . 1259
nat-pat-portnum . . . 1260
nat-port-ol-ipnumber . . . 1261
nat-source-pool . . . 1262
nat-source-rule . . . 1263
nat-static-rule . . . 1264
network-security . . . 1265
overrides (System Services DHCP) . . . 1266
periodic . . . 1267
pki-local-certificate . . . 1268
policy (System Security Profile) . . . 1269
policy-with-count . . . 1270
propagate-settings . . . 1271
reconfigure (System Services DHCP) . . . 1272
reverse ssh . . . 1273
reverse ssh port . . . 1273
reverse telnet . . . 1274

Copyright © 2013, Juniper Networks, Inc.

reverse telnet port . . . 1274
root-logical-system . . . 1275
run-mode . . . 1275
scheduler (System Security Profile) . . . 1276
secure-domains . . . 1277
security-profile . . . 1278
security-profile resources . . . 1281
start-time (FIPS) . . . 1282
system-generated-certificate (System Services) . . . 1282
traceoptions (System Services DHCP) . . . 1283
traceoptions (System Services DNS) . . . 1285
traceoptions (System Processes General Authentication) . . . 1287
traceoptions (System Processes WAN Acceleration) . . . 1289
traceoptions (Wireless WAN Service) . . . 1291
trusted-keys . . . 1293
wan-acceleration . . . 1293
web-management (System Services) . . . 1294
zone (System Security Profile) . . . 1295

Chapter 24 WLAN Hierarchy and Statements . . . 1297

WLAN Configuration Statement Hierarchy . . . 1297
access-point . . . 1304
access-point-options . . . 1308
access-point-queues . . . 1309
arbitration-inter-frame-space . . . 1310
background-queue . . . 1311
beacon-interval . . . 1311
best-effort-queue . . . 1312
broadcast-multicast-rate-limit . . . 1313
channel . . . 1314
console (WLAN) . . . 1314
country . . . 1315
disable-dot11d . . . 1317
dot1x (WLAN) . . . 1317
dot1x-supplicant . . . 1318
dtim-period . . . 1318
ethernet (WLAN) . . . 1319
external . . . 1320
fixed-multicast-rate . . . 1321
fragmentation-threshold . . . 1321
http-redirect . . . 1322
logging-options . . . 1323
mac-authentication-type . . . 1324
management-vlan . . . 1324
maximum-stations . . . 1325
maximum-burst . . . 1325
maximum-contention-window . . . 1326
minimum-contention-window . . . 1326
mode (WLAN) . . . 1327


Copyright © 2013, Juniper Networks, Inc.

name-server (WLAN) . . . 1327
no-acknowledgement . . . 1328
no-auto-power-save . . . 1328
no-broadcast-ssid . . . 1329
no-short-guard-interval-supported . . . 1329
no-wifi-multimedia . . . 1329
ntp-server . . . 1330
protection . . . 1330
quality-of-service . . . 1331
radio (WLAN) . . . 1333
radio-off . . . 1336
radio-options . . . 1337
rts-threshold . . . 1338
security (WLAN) . . . 1339
space-time-block-coding . . . 1340
ssid . . . 1340
static (WLAN) . . . 1341
static-wep . . . 1342
station-isolation . . . 1343
station-mac-filter . . . 1343
station-queues . . . 1344
syslog-options . . . 1345
transmit-opportunity-limit . . . 1345
transmit-power . . . 1346
transmit-rate-sets . . . 1346
untagged-vlan . . . 1347
video-queue . . . 1348
virtual-access-point . . . 1349
vlan (WLAN) . . . 1350
voice-queue . . . 1351
wpa-enterprise . . . 1352
wpa-personal . . . 1353

Part 2 Operational Commands

Chapter 25 Clear Commands . . . 1357

Clear Commands Overview . . . 1357
clear chassis cluster control-plane statistics . . . 1358
clear chassis cluster data-plane statistics . . . 1359
clear chassis cluster failover-count . . . 1360
clear chassis cluster ip-monitoring failure-count . . . 1362
clear chassis cluster ip-monitoring failure-count ip-address . . . 1363
clear chassis cluster statistics . . . 1364
clear dhcp client binding . . . 1365
clear dhcp client statistics . . . 1366
clear dhcp relay binding . . . 1367
clear dhcp relay statistics . . . 1368
clear dhcp server binding . . . 1369
clear dhcp server statistics . . . 1370

Copyright © 2013, Juniper Networks, Inc.

clear dhcpv6 server binding (Local Server) . . . 1371
clear dhcpv6 server statistics (Local Server) . . . 1372
clear ethernet-switching statistics mac-learning . . . 1373
clear firewall . . . 1374
clear gtp tunnels . . . 1375
clear interfaces statistics swfabx . . . 1376
clear lacp statistics interfaces . . . 1377
clear network-access requests pending . . . 1378
clear network-access requests statistics . . . 1379
clear network-access securid-node-secret-file . . . 1380
clear oam ethernet connectivity-fault-management path-database . . . 1381
clear oam ethernet connectivity-fault-management statistics . . . 1382
clear security alarms . . . 1383
clear security alg h323 counters . . . 1386
clear security alg ike-esp-nat . . . 1387
clear security alg mgcp calls . . . 1388
clear security alg mgcp counters . . . 1389
clear security alg sccp calls . . . 1390
clear security alg sccp counters . . . 1391
clear security alg sip calls . . . 1392
clear security alg sip counters . . . 1393
clear security application-firewall rule-set statistics . . . 1394
clear security application-firewall rule-set statistics logical-system . . . 1395
clear security datapath-debug counters . . . 1396
clear security dns-cache . . . 1397
clear security dynamic-vpn all . . . 1398
clear security dynamic-vpn user . . . 1399
clear security firewall-authentication history . . . 1400
clear security firewall-authentication history address . . . 1401
clear security firewall-authentication history identifier . . . 1402
clear security firewall-authentication users . . . 1403
clear security firewall-authentication users address . . . 1404
clear security firewall-authentication users identifier . . . 1405
clear security flow ip-action . . . 1406
clear security flow session all . . . 1408
clear security flow session application . . . 1409
clear security flow session destination-port . . . 1411
clear security flow session destination-prefix . . . 1412
clear security flow session family . . . 1414
clear security flow session interface . . . 1415
clear security flow session protocol . . . 1416
clear security flow session resource-manager . . . 1418
clear security flow session services-offload . . . 1419
clear security flow session session-identifier . . . 1422
clear security flow session source-port . . . 1423
clear security flow session source-prefix . . . 1424
clear security flow statistics . . . 1426
clear security gprs sctp counters . . . 1427
clear security gprs gtp counters . . . 1428


Copyright © 2013, Juniper Networks, Inc.

clear security group-vpn member ike security-associations . . . . . 1430
clear security group-vpn member ipsec security-associations . . . . . 1431
clear security group-vpn member kek security-associations . . . . . 1432
clear security group-vpn server . . . . . 1433
clear security idp . . . . . 1434
clear security idp application-ddos cache . . . . . 1435
clear security idp attack table . . . . . 1436
clear security idp counters application-identification . . . . . 1437
clear security idp counters dfa . . . . . 1438
clear security idp counters flow . . . . . 1439
clear security idp counters http-decoder . . . . . 1440
clear security idp counters ips . . . . . 1441
clear security idp counters log . . . . . 1442
clear security idp counters packet . . . . . 1443
clear security idp counters policy-manager . . . . . 1444
clear security idp counters tcp-reassembler . . . . . 1445
clear security idp ssl-inspection session-id-cache . . . . . 1446
clear security ike respond-bad-spi-count . . . . . 1447
clear security ike security-associations . . . . . 1448
clear security ipsec security-associations . . . . . 1450
clear security ipsec statistics . . . . . 1452
clear security log . . . . . 1454
clear security log file . . . . . 1456
clear security nat incoming-table . . . . . 1457
clear security nat source persistent-nat-table . . . . . 1458
clear security nat statistics destination pool . . . . . 1459
clear security nat statistics destination rule . . . . . 1460
clear security nat statistics source pool . . . . . 1461
clear security nat statistics source rule . . . . . 1462
clear security nat statistics static rule . . . . . 1463
clear security pki key-pair (Local Certificate) . . . . . 1464
clear security pki local-certificate (Device) . . . . . 1465
clear security policies hit-count . . . . . 1466
clear security policies statistics . . . . . 1467
clear security screen statistics . . . . . 1468
clear security screen statistics interface . . . . . 1469
clear security screen statistics zone . . . . . 1470
clear security user-identification local-authentication-table . . . . . 1471
clear security utm anti-spam statistics . . . . . 1472
clear security utm antivirus statistics . . . . . 1473
clear security utm content-filtering statistics . . . . . 1474
clear security utm session . . . . . 1475
clear security utm web-filtering statistics . . . . . 1476
clear services application-identification application-statistics . . . . . 1477
clear services application-identification application-statistics cumulative . . . . 1478
clear services application-identification application-statistics interval . . . . . 1479
clear services application-identification application-system-cache (Junos OS) . . . . . 1480
clear services application-identification counter (Values) . . . . . 1481

Copyright © 2013, Juniper Networks, Inc.

clear services application-identification counter ssl-encrypted-sessions . . . . . 1482
clear services ssl proxy statistics . . . . . 1483
clear system login lockout . . . . . 1484
clear system services dns dns-proxy . . . . . 1485
clear wlan access-point neighbors . . . . . 1486

Chapter 26 Request Commands . . . . . 1487

Request Commands Overview . . . . . 1487
request chassis cluster failover node . . . . . 1488
request chassis cluster failover reset . . . . . 1489
request chassis cluster in-service-upgrade abort (ISSU) . . . . . 1490
request dhcp client renew . . . . . 1491
request modem wireless activate iota . . . . . 1492
request modem wireless activate manual . . . . . 1493
request modem wireless activate otasp . . . . . 1495
request modem wireless gsm sim-unblock . . . . . 1496
request modem wireless gsm sim-unlock . . . . . 1497
request pppoe connect . . . . . 1498
request pppoe disconnect . . . . . 1499
request security datapath-debug capture start . . . . . 1500
request security datapath-debug capture stop . . . . . 1501
request security idp security-package download . . . . . 1502
request security idp security-package install . . . . . 1504
request security idp ssl-inspection key add . . . . . 1506
request security idp ssl-inspection key delete . . . . . 1508
request security idp storage-cleanup . . . . . 1510
request security ike debug-disable . . . . . 1511
request security ike debug-enable . . . . . 1512
request security pki ca-certificate verify (Security) . . . . . 1513
request security pki local-certificate generate-self-signed (Security) . . . . . 1514
request security pki local-certificate load . . . . . 1516
request security pki local-certificate verify (Security) . . . . . 1517
request security pki verify-integrity-status . . . . . 1518
request security user-identification local-authorization-table add . . . . . 1519
request security user-identification local-authentication-table delete . . . . . 1521
request security utm anti-virus juniper-express-engine . . . . . 1522
request security utm anti-virus kaspersky-lab-engine . . . . . 1523
request security utm anti-virus sophos-engine . . . . . 1524
request services application-identification application . . . . . 1525
request services application-identification download . . . . . 1527
request services application-identification download status . . . . . 1528
request services application-identification group . . . . . 1529
request services application-identification install . . . . . 1530
request services application-identification install status . . . . . 1531
request services application-identification uninstall . . . . . 1532
request services application-identification uninstall status . . . . . 1533
request system autorecovery state . . . . . 1534
request services ip-monitoring preempt-restore policy . . . . . 1536
request system download abort . . . . . 1537


Copyright © 2013, Juniper Networks, Inc.

request system download clear . . . . . 1538
request system download pause . . . . . 1539
request system download resume . . . . . 1540
request system download start . . . . . 1541
request system firmware upgrade . . . . . 1542
request system fips self-test . . . . . 1543
request system license update . . . . . 1545
request system partition compact-flash . . . . . 1546
request system services dhcp . . . . . 1547
request system snapshot (Maintenance) . . . . . 1548
request system software abort in-service-upgrade (ICU) . . . . . 1549
request system software add (Maintenance) . . . . . 1550
request system software in-service-upgrade (Maintenance) . . . . . 1551
request system software reboot . . . . . 1556
request system software rollback (Maintenance) . . . . . 1557
request wan-acceleration login . . . . . 1558
request wlan access-point firmware upgrade . . . . . 1559
request wlan access-point restart . . . . . 1560
request wireless-wan adapter firmware upgrade . . . . . 1561

Chapter 27 Restart Commands . . . . . 1563

Restart Commands Overview . . . . . 1563
restart (Reset) . . . . . 1564

Chapter 28 Show Commands . . . . . 1567

Show Commands Overview . . . . . 1567
show accounting . . . . . 1568
show accounting profile (View) . . . . . 1569
show accounting records (View) . . . . . 1570
show bgp neighbor (View) . . . . . 1571
show configuration chassis cluster traceoptions . . . . . 1575
show chassis alarms . . . . . 1576
show chassis cluster control-plane statistics . . . . . 1578
show chassis cluster data-plane interfaces . . . . . 1580
show chassis cluster data-plane statistics . . . . . 1581
show chassis cluster ethernet-switching interfaces . . . . . 1583
show chassis cluster ethernet-switching status . . . . . 1584
show chassis cluster interfaces . . . . . 1586
show chassis cluster ip-monitoring status redundancy-group . . . . . 1590
show chassis cluster statistics . . . . . 1593
show chassis cluster status . . . . . 1598
show chassis fpc (View) . . . . . 1601
show chassis hardware (View) . . . . . 1607
show chassis power . . . . . 1614
show chassis power sequence . . . . . 1616
show chassis routing-engine (View) . . . . . 1617
show chassis usb storage . . . . . 1619
show class-of-service application-traffic-control counter . . . . . 1620
show class-of-service application-traffic-control statistics rate-limiter . . . . . 1622
show class-of-service application-traffic-control statistics rule . . . . . 1624

Copyright © 2013, Juniper Networks, Inc.

show class-of-service forwarding-class . . . 1625
show configuration smtp . . . 1627
show dhcp client binding . . . 1628
show dhcp client statistics . . . 1631
show dhcp relay binding . . . 1633
show dhcp relay statistics . . . 1635
show dhcp server binding . . . 1637
show dhcp server statistics . . . 1639
show dhcpv6 server binding (View) . . . 1641
show dhcpv6 server statistics (View) . . . 1645
show ethernet-switching mac-learning-log (View) . . . 1648
show ethernet-switching table (View) . . . 1651
show firewall (View) . . . 1656
show gtp tunnels . . . 1658
show security gprs gtp counters . . . 1659
show igmp-snooping route (View) . . . 1665
show igmp-snooping vlans (View) . . . 1667
show interfaces (View J Series and SRX Series) . . . 1669
show interfaces (View Aggregated Ethernet) . . . 1676
show interfaces flow-statistics . . . 1688
show interfaces diagnostics optics . . . 1693
show interfaces swfabx . . . 1698
show interfaces statistics (View) . . . 1699
show lacp interfaces (View) . . . 1700
show lacp statistics interfaces (View) . . . 1705
show modem wireless interface . . . 1707
show modem wireless interface firmware . . . 1709
show modem wireless interface network . . . 1711
show modem wireless interface rssi . . . 1713
show network-access address-assignment pool (View) . . . 1714
show network-access requests pending . . . 1715
show network-access requests statistics . . . 1717
show network-access securid-node-secret-file . . . 1718
show oam ethernet connectivity-fault-management adjacencies . . . 1719
show oam ethernet connectivity-fault-management forwarding-state . . . 1720
show oam ethernet connectivity-fault-management interfaces . . . 1722
show oam ethernet connectivity-fault-management mep-database . . . 1723
show oam ethernet connectivity-fault-management mep-statistics . . . 1727
show oam ethernet connectivity-fault-management mip . . . 1730
show oam ethernet connectivity-fault-management path-database . . . 1731
show oam ethernet connectivity-fault-management routes . . . 1733
show oam ethernet link-fault-management . . . 1735
show poe controller (View) . . . 1740
show poe interface (View) . . . 1741
show poe telemetries interface (View) . . . 1743
show pppoe interfaces . . . 1745
show pppoe statistics . . . 1749
show schedulers . . . 1751
show security alarms . . . 1753


Copyright © 2013, Juniper Networks, Inc.

show security alg h323 counters . . . . . 1758
show security alg ike-esp-nat summary . . . . . 1760
show security alg mgcp calls . . . . . 1761
show security alg mgcp counters . . . . . 1763
show security alg mgcp endpoints . . . . . 1766
show security alg msrpc . . . . . 1768
show security alg sccp calls . . . . . 1770
show security alg sccp counters . . . . . 1772
show security alg sip calls . . . . . 1774
show security alg sip counters . . . . . 1776
show security alg sip rate . . . . . 1781
show security alg sip transactions . . . . . 1783
show security alg status . . . . . 1785
show security application-firewall rule-set . . . . . 1787
show security application-firewall rule-set logical-system . . . . . 1789
show security application-tracking counters . . . . . 1792
show security datapath-debug capture . . . . . 1793
show security datapath-debug counter . . . . . 1794
show security dns-cache . . . . . 1795
show security dynamic-policies . . . . . 1797
show security dynamic-vpn client version . . . . . 1802
show security dynamic-vpn users . . . . . 1803
show security dynamic-vpn users terse . . . . . 1804
show security firewall-authentication history . . . . . 1805
show security firewall-authentication history address . . . . . 1807
show security firewall-authentication history identifier . . . . . 1810
show security firewall-authentication users . . . . . 1813
show security firewall-authentication users address . . . . . 1815
show security firewall-authentication users identifier . . . . . 1818
show security flow cp-session . . . . . 1821
show security flow cp-session destination-port . . . . . 1823
show security flow cp-session destination-prefix . . . . . 1825
show security flow cp-session family . . . . . 1827
show security flow cp-session protocol . . . . . 1829
show security flow cp-session source-port . . . . . 1831
show security flow cp-session source-prefix . . . . . 1833
show security flow gate . . . . . 1835
show security flow gate brief node . . . . . 1839
show security flow gate destination-port . . . . . 1845
show security flow gate destination-prefix . . . . . 1849
show security flow gate family . . . . . 1853
show security flow gate protocol . . . . . 1856
show security flow gate source-port . . . . . 1860
show security flow gate source-prefix . . . . . 1864
show security flow gate summary node . . . . . 1868
show security flow ip-action . . . . . 1874
show security flow session . . . . . 1879
show security flow session application . . . . . 1884
show security flow session application-firewall . . . . . 1889

Copyright © 2013, Juniper Networks, Inc. 

show security flow session brief node . . . . . 1896
show security flow session destination-port . . . . . 1900
show security flow session destination-prefix . . . . . 1904
show security flow session extensive node . . . . . 1909
show security flow session family . . . . . 1915
show security flow session idp summary . . . . . 1920
show security flow session interface . . . . . 1922
show security flow session nat . . . . . 1927
show security flow session protocol . . . . . 1931
show security flow session resource-manager . . . . . 1937
show security flow session services-offload . . . . . 1942
show security flow session session-identifier . . . . . 1947
show security flow session source-port . . . . . 1951
show security flow session source-prefix . . . . . 1955
show security flow session summary family . . . . . 1959
show security flow session summary node . . . . . 1961
show security flow session summary services-offload . . . . . 1967
show security flow session tunnel . . . . . 1971
show security flow statistics . . . . . 1976
show security flow status . . . . . 1978
show security gprs sctp association . . . . . 1980
show security gprs sctp counters . . . . . 1981
show security group-vpn member ike security-associations . . . . . 1983
show security group-vpn member ipsec security-associations . . . . . 1987
show security group-vpn member kek security-associations . . . . . 1990
show security group-vpn server ike security-associations . . . . . 1993
show security group-vpn server ipsec security-associations . . . . . 1997
show security group-vpn server kek security-associations . . . . . 2001
show security group-vpn server registered-members . . . . . 2005
show security idp active-policy . . . . . 2007
show security idp application-ddos application . . . . . 2008
show security idp attack description . . . . . 2010
show security idp attack detail . . . . . 2011
show security idp attack table . . . . . 2013
show security idp counters application-ddos . . . . . 2014
show security idp counters application-identification . . . . . 2017
show security idp counters dfa . . . . . 2019
show security idp counters flow . . . . . 2020
show security idp counters http-decoder . . . . . 2023
show security idp counters ips . . . . . 2024
show security idp counters log . . . . . 2027
show security idp counters packet . . . . . 2030
show security idp counters packet-log . . . . . 2033
show security idp counters policy-manager . . . . . 2035
show security idp counters tcp-reassembler . . . . . 2036
show security idp logical-system policy-association . . . . . 2039
show security idp memory . . . . . 2040
show security idp policies . . . . . 2041
show security idp policy-commit-status . . . . . 2042


Copyright © 2013, Juniper Networks, Inc.

show security idp policy-commit-status clear . . . . . 2043
show security idp policy-templates . . . . . 2044
show security idp predefined-attacks . . . . . 2045
show security idp security-package-version . . . . . 2047
show security idp ssl-inspection key . . . . . 2048
show security idp ssl-inspection session-id-cache . . . . . 2050
show security idp status . . . . . 2051
show security idp status detail . . . . . 2053
show security ike active-peer . . . . . 2056
show security ike debug-status . . . . . 2057
show security ike pre-shared-key . . . . . 2058
show security ike security-associations . . . . . 2059
show security ike tunnel-map . . . . . 2066
show security ipsec inactive-tunnels . . . . . 2067
show security ipsec next-hop-tunnels . . . . . 2070
show security ipsec security-associations . . . . . 2071
show security ipsec statistics . . . . . 2079
show security log . . . . . 2082
show security log file . . . . . 2086
show security match-policies . . . . . 2089
show security monitoring fpc fpc-number . . . . . 2095
show security monitoring performance session . . . . . 2098
show security monitoring performance spu . . . . . 2099
show security nat destination pool . . . . . 2100
show security nat destination rule . . . . . 2102
show security nat destination summary . . . . . 2105
show security nat incoming-table . . . . . 2107
show security nat interface-nat-ports . . . . . 2109
show security nat source persistent-nat-table . . . . . 2111
show security nat source pool . . . . . 2114
show security nat source rule . . . . . 2118
show security nat source summary . . . . . 2121
show security nat static rule . . . . . 2123
show security pki ca-certificate (View) . . . . . 2126
show security pki certificate-request (View) . . . . . 2129
show security pki crl (View) . . . . . 2131
show security pki local-certificate (View) . . . . . 2134
show security policies . . . . . 2139
show security policies hit-count . . . . . 2145
show security resource-manager group active . . . . . 2147
show security resource-manager resource active . . . . . 2150
show security resource-manager settings . . . . . 2153
show security resource-manager summary . . . . . 2155
show security screen ids-option . . . . . 2156
show security screen statistics . . . . . 2159
show security shadow-policies logical-system . . . . . 2166
show security softwires . . . . . 2168
show security user-identification local-authentication-table . . . . . 2169
show security user-identification role-provision all . . . . . 2171

Copyright © 2013, Juniper Networks, Inc. 

show security user-identification source-identity-provision all . . . . . 2172
show security user-identification user-provision all . . . . . 2173
show security utm anti-spam statistics . . . . . 2174
show security utm anti-spam status . . . . . 2175
show security utm anti-virus statistics . . . . . 2176
show security utm anti-virus status . . . . . 2178
show security utm content-filtering statistics . . . . . 2180
show security utm session . . . . . 2181
show security utm status . . . . . 2182
show security utm web-filtering statistics . . . . . 2183
show security utm web-filtering status . . . . . 2185
show security zones . . . . . 2186
show security zones type . . . . . 2190
show services accounting . . . . . 2193
show services accounting aggregation (View) . . . . . 2194
show services accounting aggregation template (View) . . . . . 2195
show services accounting flow-detail (View) . . . . . 2196
show services application-identification application . . . . . 2197
show services application-identification application-system-cache (View) . . 2202
show services application-identification counter (AppSecure) . . . . . 2204
show services application-identification counter ssl-encrypted-sessions . . . . 2206
show services application-identification group . . . . . 2208
show services application-identification statistics applications . . . . . 2210
show services application-identification statistics application-groups . . . . . 2212
show services application-identification version . . . . . 2214
show services ip-monitoring status . . . . . 2215
show services rpm probe-results (View) . . . . . 2219
show services ssl proxy statistics . . . . . 2223
show services unified-access-control authentication-table . . . . . 2224
show services unified-access-control counters . . . . . 2226
show services unified-access-control policies . . . . . 2228
show services unified-access-control roles . . . . . 2230
show services unified-access-control status . . . . . 2231
show snmp health-monitor . . . . . 2232
show snmp health-monitor routing engine history . . . . . 2239
show snmp mib (View) . . . . . 2244
show system alarms . . . . . 2246
show system autorecovery state . . . . . 2247
show system download . . . . . 2248
show system license (View) . . . . . 2250
show system security-profile . . . . . 2254
show system services dhcp client . . . . . 2259
show system login lockout . . . . . 2262
show system services dhcp relay-statistics . . . . . 2263
show system services dynamic-dns . . . . . 2265
show system services dns dns-proxy . . . . . 2267
show system snapshot media . . . . . 2270
show system storage partitions (View SRX Series) . . . . . 2271
show wan-acceleration status . . . . . 2272


Copyright © 2013, Juniper Networks, Inc.

show wlan access-points . . . . . 2273
show wlan diagnostics . . . . . 2277
show wireless-wan adapter . . . . . 2278

Part 3 Index

Index . . . . . 2285

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

# About This Guide

This preface provides the following guidelines for using the *Junos® OS CLI Reference*:


- J Series and SRX Series Documentation and Release Notes on page xlvii
- Objectives on page xlviii
- Audience on page xlviii
- Supported Routing Platforms on page xlviii
- Document Conventions on page xlviii
- Documentation Feedback on page l
- Requesting Technical Support on page l


## J Series and SRX Series Documentation and Release Notes

For a list of related J Series documentation, see http://www.juniper.net/techpubs/software/junos-jseries/index-main.html .

For a list of related SRX Series documentation, see http://www.juniper.net/techpubs/hardware/srx-series-main.html .

If the information in the latest release notes differs from the information in the documentation, follow the *Junos OS Release Notes*.

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at http://www.juniper.net/books .

Copyright © 2013, Juniper Networks, Inc.

## Objectives

This reference documents command-line interface (CLI) statements and commands for J Series Services Routers and SRX Series Services Gateways running Junos OS. This reference provides the following information:

- Configuration hierarchies—Complete hierarchies of the configuration statements that you use to configure J Series and SRX Series devices. Hierarchies include all configuration statements—including the statements shared with the Junos OS—and highlight statements specific to the J Series and SRX Series devices in bold type.
- Configuration statements—Descriptions of the configuration statements that are unique to the J Series and SRX Series devices.
- Commands—Descriptions of the operational mode commands that you use to monitor and troubleshoot J Series and SRX Series operations.

## Audience

This manual is designed for anyone who installs, sets up, configures, monitors, or administers a J Series Services Router or an SRX Series Services Gateway running Junos OS. The manual is intended for the following audiences:

- Customers with technical knowledge of and experience with networks and network security, the Internet, and Internet routing protocols
- Network administrators who install, configure, and manage Internet routers

## Supported Routing Platforms

This manual describes features supported on J Series Services Routers and SRX Series Services Gateways running Junos OS.

## Document Conventions

Table 1 on page xlix defines the notice icons used in this guide.


Copyright © 2013, Juniper Networks, Inc.

## Table 1: Notice Icons

| Icon | Meaning | Description |
|---|---|---|
|  | Informational note | Indicates important features or instructions. |
|  | Caution | Indicates a situation that might result in loss of data or hardware damage. |
|  | Warning | Alerts you to the risk of personal injury or death. |
|  | Laser warning | Alerts you to the risk of personal injury from a laser. |

Table 2 on page xlix defines the text and syntax conventions used in this guide.

## Table 2: Text and Syntax Conventions

| Convention | Description | Examples |
|---|---|---|
| **Bold text like this** | Represents text that you type. | To enter configuration mode, type the**configure** command:<br><br>user@host> **configure** |
| `Fixed-width text like this` | Represents output that appears on the terminal screen. | `user@host>` **show chassis alarms**<br><br>`No alarms currently active` |
| *Italic text like this* | • Introduces or emphasizes important new terms.<br>• Identifies book names.<br>• Identifies RFC and Internet draft titles. | • A policy *term* is a named structure that defines match conditions and actions.<br>• *Junos OS System Basics Configuration Guide*<br>• RFC 1997, *BGP Communities Attribute* |
| *Italic text like this* | Represents variables (options for which you substitute a value) in commands or configuration statements. | Configure the machine's domain name:<br><br>[edit]<br>root@# **set system domain-name** *domain-name* |
| **Text like this** | Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components. | • To configure a stub area, include the **stub** statement at the**[edit protocols ospf area area-id]** hierarchy level.<br>• The console port is labeled **CONSOLE**. |
| < > (angle brackets) | Enclose optional keywords or variables. | **stub <default-metric** ***metric*****>;** |

Copyright © 2013, Juniper Networks, Inc.

Table 2: Text and Syntax Conventions *(continued)*

| Convention | Description | Examples |
|---|---|---|
| \| (pipe symbol) | Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity. | **broadcast \| multicast**<br><br>**(*string1* \| *string2* \| *string3*)** |
| # (pound sign) | Indicates a comment specified on the same line as the configuration statement to which it applies. | **rsvp { # Required for dynamic MPLS only** |
| [ ] (square brackets) | Enclose a variable for which you can substitute one or more values. | **community name members [ *community-ids* ]** |
| Indention and braces ( { } ) | Identify a level in the configuration hierarchy. | [edit]<br>routing-options {<br>  static {<br>  route default {<br>  nexthop *address*;<br>  retain;<br>  }<br>  }<br>} |
| ; (semicolon) | Identifies a leaf statement at a configuration hierarchy level. | |
| J-Web GUI Conventions | | |
| **Bold text like this** | Represents J-Web graphical user interface (GUI) items you click or select. | • In the Logical Interfaces box, select **All Interfaces**.<br>• To cancel the configuration, click **Cancel**. |
| > (bold right angle bracket) | Separates levels in a hierarchy of J-Web selections. | In the configuration editor hierarchy, select **Protocols>Ospf**. |

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@juniper.net**, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,


Copyright © 2013, Juniper Networks, Inc.

or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/support/requesting-support.html

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

PART 1

# Configuration Statements


- Access Hierarchy and Statements on page 3
- Accounting-Options Hierarchy on page 53
- Applications Hierarchy and Statements on page 55
- Bridge-Domains Hierarchy and Statements on page 71
- Chassis Hierarchy and Statements on page 79
- Class-of-Service Hierarchy and Statements on page 109
- Event-Options Hierarchy on page 141
- Firewall Hierarchy and Statements on page 143
- Forwarding-Options Hierarchy and Statements on page 149
- Groups Hierarchy on page 157
- Interfaces Hierarchy and Statements on page 159
- Logical-Systems Hierarchy and Statement on page 223
- Power Over Ethernet Hierarchy and Statements on page 227
- Policy-Options Hierarchy and Statements on page 235
- Protocols Hierarchy and Statements on page 239
- Routing-Instances Hierarchy on page 277
- Routing-Options Hierarchy on page 291
- Schedulers Hierarchy and Statements on page 297
- Security Hierarchy and Statements on page 315
- Services Hierarchy and Statements on page 1133
- SMTP Hierarchy and Statements on page 1195
- SNMP Hierarchy and Statements on page 1199
- System Hierarchy and Statements on page 1205
- WLAN Hierarchy and Statements on page 1297


Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 1

# Access Hierarchy and Statements

This section includes the following topics:


- Access Configuration Statement Hierarchy on page 3


## Access Configuration Statement Hierarchy

Use the statements in the **access** configuration hierarchy to configure access to the device and authentication methods, including address assignment and address pool, user and firewall authentication, a group profile, LDAP options and LDAP server configuration, an access profile, RADIUS options and RADIUS server configuration, and SecurID server configuration.

```
access {
    address-assignment {
        neighbor-discovery-router-advertisement ndra-pool-name;
        pool pool-name {
            family {
                inet {
                    dhcp-attributes {
                        boot-file boot file name;
                        boot-server boot server name;
                        domain-name domain name;
                        grace-period seconds;
                        maximum-lease-time seconds;
                        name-server address;
                        netbios-node-type type;
                        option dhcp option-identifier-code;
                        option-match {
                            option-82 {
                                circuit-id match-value;
                                remote-id match-value;
                            }
                        }
                        router IPv4 address;
                        server-identifier IP address;
                        tftp-server server name;
                        wins-server IPv4 address;
                    }
                    host hostname;
                    network network address;
                    range range-name {
```

Copyright © 2013, Juniper Networks, Inc.

```
            high upper-limit;
            low lower-limit;
          }
          xauth-attributes {
            primary-dns IP address;
            primary-wins IP address;
            secondary-dns IP address;
            secondary-wins IP address;
          }
        }
        inet6 {
          dhcp-attributes {
            dns-server IPv6-address;
            grace-period seconds;
            maximum-lease-time seconds;
            option dhcp-option-identifier-code;
            sip-server-address IPv6-address;
            sip-server-domain-name domain-name;
          }
          prefix IPv6-network-prefix;
          range range-name {
            high upper-limit;
            low lower-limit;
            prefix-length delegated-prefix-length;
          }
      link pool-name;
    }
  }
  address-pool pool-name {
    address address or address prefix;
    address-range {
      high upper-limit;
      low lower-limit;
      mask network-mask;
    }
    primary-dns IP address;
    primary-wins IP address;
    secondary-dns IP address;
    secondary-wins IP address;
  }
  domain {
    delimiter delimiter;
    map domain-map-name;
    parse-direction (left-to-right | right-to-left)
  }
  firewall-authentication {
    pass-through {
      default-profile profile-name;
      <ftp | http | telnet> {
        banner {
          fail string;
          login string;
          success string;
        }
      }
    }
```


Copyright © 2013, Juniper Networks, Inc.

```
    traceoptions {
      file filename <files number> <match regular-expression>
      <size maximum-file-size> <world-readable | no-world-readable>
      flag flag;
    }
    web-authentication {
      banner {
        success string;
      }
      default-profile profile-name;
    }
  }
  group-profile profile-name {
    ppp {
      cell-overhead;
      encapsulated-overhead;
      framed-pool address-pool-name;
      idle-timeout seconds;
      interface-id interface-identifier;
      keepalive seconds;
      primary-dns IP address;
      primary-wins IP address;
      secondary-dns IP address;
      secondary-dns IP address;
    }
  }
  ldap-options {
    assemble {
      common-name common-name;
    }
    base-distinguished-name base-distinguished-name;
    revert-interval seconds;
    search {
      admin-search {
        distinguished-name distinguished-name;
        password password;
      }
      search-filter filter-name;
    }
  }
  ldap-server server-address {
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    source-address source-address;
    timeout seconds;
  }
  ppp-options {
    compliance 2486;
  }
  profile profile-name  {
    accounting {
      accounting-stop-on-access-deny;
      accounting-stop-on-failure;
      order [ radius ...]
      statistics;
```

Copyright © 2013, Juniper Networks, Inc.

```
    }
    address-assignment pool pool-name;
    authentication-order [ athentication-method1 authentication-method2 ... ]
    client client-name  {
      chap-secret  chap-secret;
      client-group [ group-names ];
      firewall-user {
        password password;
      }
      no-rfc2486;
      pap-password pap-password;
      x-auth client-ip-address;
      client-name-filter client-name {
        count number;
        domain-name domain-name;
        separator special-character;
      }
      ldap-options {
        assemble {
          common-name common-name;
        }
        base-distinguished-name base-distinguished-name;
        revert-interval seconds;
        search {
          admin-search {
            distinguished-name distinguished-name;
            password password;
          }
          search-filter filter-name;
        }
      }
      ldap-server server-address {
        port port-number;
        retry attempts;
        routing-instance routing-instance-name;
        source-address source-address;
        timeout seconds;
      }
      radius-options {
        revert-interval seconds;
      }
      radius-server server-address {
        port port-number;
        retry attempts;
        routing-instance routing-instance-name;
        secret password;
        source-address source-address;
        timeout seconds;
      }
      session-options {
        client-group [group-names];
        client-idle-timeout minutes;
        client-session-timeout minutes;
      }
    }
  }
```


Copyright © 2013, Juniper Networks, Inc.

```
    radius-options {
      revert-interval seconds;
    }
    radius-server server-address {
      port port-number;
      retry attempts;
      routing-instance routing-instance-name;
      secret password;
      source-address source-address;
      timeout seconds;
    }
    securid-server {
      server-name configuration-file filepath;
    }
  }
```

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Dynamic VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## address-assignment (Access)

**Syntax**

```
address-assignment {
    neighbor-discovery-router-advertisement ndra-pool-name;
    pool pool-name {
        family {
            inet {
                dhcp-attributes {
                    boot-file boot file name;
                    boot-server boot server name;
                    domain-name domain name;
                    grace-period seconds;
                    maximum-lease-time seconds;
                    name-server address;
                    netbios-node-type type;
                    option dhcp option-identifier-code;
                    option-match {
                        option-82 {
                            circuit-id match-value;
                            remote-id match-value;
                        }
                    }
                    router IPv4 address;
                    server-identifier IP address;
                    tftp-server server name;
                    wins-server IPv4 address;
                }
                host hostname;
                network network address;
                range range-name {
                    high upper-limit;
                    low lower-limit;
                }
                xauth-attributes {
                    primary-dns IP address;
                    primary-wins IP address;
                    secondary-dns IP address;
                    secondary-wins IP address;
                }
            }
            inet6 {
                dhcp-attributes {
                    dns-server IPv6-address;
                    grace-period seconds;
                    maximum-lease-time seconds;
                    option dhcp-option-identifier-code;
                    sip-server-address IPv6-address;
                    sip-server-domain-name domain-name;
                }
                prefix IPv6-network-prefix;
                range range-name {
                    high upper-limit;
                    low lower-limit;
                    prefix-length delegated-prefix-length;
```


Copyright © 2013, Juniper Networks, Inc.

```
        }
    link pool-name;
  }
}
```

**Hierarchy Level** [edit access]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** The address-assignment pool feature enables you to create IPv4 and IPv6 address pools that different client applications can share. For example, multiple client applications, such as DHCPv4 or DHCPv6, can use an address-assignment pool to provide addresses for their particular clients.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

- Dynamic VPNs for Security Devices
- Device Configuration

Copyright © 2013, Juniper Networks, Inc.

## address-pool (Access)

**Syntax**

```
address-pool pool-name {
  address address or address prefix;
  address-range {
    high upper-limit;
    low lower-limit;
    mask network-mask;
  }
  primary-dns IP address;
  primary-wins IP address;
  secondary-dns IP address;
  secondary-wins IP address;
}
```

**Hierarchy Level** [edit access]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Create an address-pool for L2TP clients.

**Options**

- **pool-name**—Name assigned to the address-pool.
- **address**—Configure subnet information for the address-pool.
- **address-range**—Defines the address range available for clients.
- **primary-dns**—Specify the primary-dns IP address.
- **secondary-dns**—Specify the secondary-dns IP address.
- **primary-wins**—Specify the primary-wins IP address.
- **secondary-wins**—Specify the secondary-wins IP address.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

## admin-search

**Syntax**

```
admin-search {
  distinguished-name distinguished-name ;
  password password ;
}
```

**Hierarchy Level** [edit access ldap-options search],
[edit access profile *profile-name* ldap-options search]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify that a Lightweight Directory Access Protocol (LDAP) administrator search is performed. By default, the search is an anonymous search. To perform an administrator search, you must specify administrator credentials, which are used in the bind as part of performing the search.

**Options** The remaining statements are explained separately.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

## assemble

**Syntax**

```
assemble {
  common-name common-name;
}
```

**Hierarchy Level** [edit access ldap-options],
[edit access profile *profile-name* ldap-options]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify that a user's LDAP distinguished name (DN) is assembled through the use of a common name identifier, the username, and base distinguished name.

**Options** **common-name** *common-name*—Common name identifier used as a prefix for the username during the assembly of the user's distinguished name. For example, **uid** specifies " user id," and **cn** specifies "common name."

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## authentication-order (Access Profile)

**Syntax** authentication-order [ *athentication-method1 authentication-method2 ...* ]

**Hierarchy Level** [edit access profile *profile-name* ]

**Release Information** Statement modified in Release 9.1 of Junos OS.

**Description** Set the order in which the Junos OS tries different authentication methods when verifying that a client can access the devices. For each login attempt, the software tries the authentication methods in order, from first to last.

**Options**

- **ldap**—Verify the client using LDAP.
- **password**—Verify the client using the information configured at the **[edit access profile *profile-name* client *client-name*]** hierarchy level.
- **radius**—Verify the client using RADIUS authentication services.
- **securid**—Verify the client using SecurID authentication services.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices

## banner (Access FTP HTTP Telnet Authentication)

**Syntax**

```
banner {
  fail string ;
  login string ;
  success string ;
}
```

**Hierarchy Level** [edit access firewall-authentication pass-through (ftp | http | telnet)]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the banners that appear to users during the FTP, HTTP, and Telnet firewall authentication process. The banners appear during login, after successful authentication, and after failed authentication.

**Options** The remaining statements are explained separately.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## banner (Access Web Authentication)

**Syntax**

```
banner {
  success string ;
}
```

**Hierarchy Level** [edit access firewall-authentication web-authentication]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the banners that appear to users during the Web authentication process. The banners appear during login, after successful authentication, and after failed authentication.

**Options** The remaining statement is explained separately.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## base-distinguished-name

**Syntax** base-distinguished-name ***base-distinguished-name***;

**Hierarchy Level** [edit access ldap-options],
[edit access profile ***profile-name*** ldap-options]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the base distinguished name (DN), which can be used in one of the following ways:

- If you are using the **assemble** statement so that the user's distinguished name is being assembled, the base distinguished name is appended to a username to generate the user's distinguished name. The resulting distinguished name is used in the LDAP bind call.
- If you are using the **search** statement so that the user's distinguished name is found by a search, the search is restricted to the subtree of the base distinguished name.

**Options** ***base-distinguished-name***—Series of basic properties that define the user. For example in the base distinguished name **o=juniper, c=us**, where **c** stands for country, and **o** for organization.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## client-group

**Syntax** client-group [ *group-names* ];

**Hierarchy Level** [edit access profile *profile-name* client *client-name*]
[edit access profile *profile-name session-options*]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify a list of client groups that the client belongs to. If the group list is not defined as part of the client profile, the client group configured at the **[edit access profile session-options]** hierarchy level is used.

**Options** *group-names* —Names of one or more groups the client belongs to, separated by spaces—for example **g1, g2, g3**. The total length of the group name string cannot exceed 256 characters.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

## client-idle-timeout (Access Profile)

**Syntax** client-idle-timeout *minutes*;

**Hierarchy Level** [edit access profile *profile-name* session-options]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the grace period that begins after an authenticated user terminates all sessions and connections. Authentication is not required if a new connection is initiated during the grace period by the same user.

**Options** *minutes* —Number of minutes of idle time that elapse before the session is terminated.

**Range:** 10 through 255 minutes

**Default:** 10 minutes

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## client-name-filter

**Syntax**

```
client-name-filter client-name {
    count number;
    domain-name domain-name;
    separator special-character;
}
```

**Hierarchy Level** [edit access profile *profile-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Define client-name-related restrictions. Clients whose names follow these restrictions are authenticated on the server.

**Options** ***client-name*** —Name of the client.

The remaining statements are explained separately.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

## client-session-timeout (Access Profile)

**Syntax** client-session-timeout *minutes*;

**Hierarchy Level** [edit access profile *profile-name* session-options]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the amount of time after which user sessions are terminated, regardless of user activity (also known as a forced or hard authentication timeout).

**Options** ***minutes*** —Number of minutes after which user sessions are terminated.

**Range:** 1 through 10,000 minutes

**Default:** Off

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## configuration-file

**Syntax** *server-name* configuration-file *filepath*;

**Hierarchy Level** [edit access securid-server]

**Release Information** Statement introduced in Release 9.1 of Junos OS.

**Description** Specify the path of the SecurID server configuration file. The file is copied on the devices in some directory location—for example, **/var/db/securid/sdconf.rec**.

**Options**
- ***server-name***—Name of the SecurID authentication server.
- ***filepath***—Path of the SecurID server configuration file.

**Required Privilege Level** secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

**Related Documentation**

## count

**Syntax** count *number*;

**Hierarchy Level** [edit access profile *profile-name* client-name-filter ]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the number of characters to be stripped from a client name, from right to left, until the specified number of characters are deleted. The resulting name is sent to the authentication server.

**Options** ***number***—Number of characters to be stripped in a client name.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## default-profile

**Syntax** default-profile *profile-name*;

**Hierarchy Level** [edit access firewall-authentication pass-through]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the authentication profile to use if no profile is specified in a policy.

**Options** ***profile-name***—Name of the profile.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## dhcp-attributes (Access IPv4 Address Pools)

**Syntax**

```
dhcp-attributes {
  boot-file boot file name;
  boot-server boot server name;
  domain-name domain name;
  grace-period seconds;
  maximum-lease-time seconds;
  name-server address;
  netbios-node-type type;
  option dhcp option-identifier-code;
  option-match {
    option-82 {
      circuit-id match-value;
      remote-id match-value;
    }
  }
  router IPv4 address;
  server-identifier IP address;
  tftp-server server name;
  wins-server IPv4 address;
}
```

**Hierarchy Level** [edit access address-assignment pool pool-name family inet]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Configure attributes for IPv4 address pools that can be used by different clients. The DHCP attributes for this statement uses standard IPv4 DHCP options.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

- Device Configuration

Copyright © 2013, Juniper Networks, Inc.

## dhcp-attributes (Access IPv6 Address Pools)

**Syntax**

```
dhcp-attributes {
  dns-server IPv6-address;
  grace-period seconds;
  maximum-lease-time seconds;
  option dhcp-option-identifier-code;
  sip-server-address IPv6-address;
  sip-server-domain-name domain-name;
}
```

**Hierarchy Level** [edit access address-assignment pool pool-name family inet6]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Configure attributes for address pools that can be used by different clients.

**Options**

- **dns-server** *IPv6-address*—Specify a DNS server to which clients can send DNS queries.
- **grace-period** *seconds* —Specify the grace period offered with the lease.

  **Range:** 0 through 4,294,967,295 seconds

  **Default:** 0 (no grace period)

- **maximum-lease-time** *seconds*—Specify the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.

  **Range:** 30 through 4,294,967,295 seconds

  **Default:** 86,400 seconds (24 hours)

- **option** *dhcp-option-identifier-code*—Specify the DHCP option identifier code.
- **sip-server-address** *IPv6-address*—Specify the IPv6 address of the SIP outbound proxy server.
- **sip-server-domain-name** *domain-name*—Specify the domain name of the SIP outbound proxy server.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

## distinguished-name (Access)

**Syntax** distinguished-name *distinguished-name*;

**Hierarchy Level** [edit access ldap-options search admin-search],
[edit access profile *profile-name* ldap-options search admin-search]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the distinguished name of an administrative user. The distinguished name is used in the bind for performing the LDAP search.

**Options** ***distinguished-name***—Set of properties that define the user. For example, **cn**=admin, **ou**=eng, **o**=juniper, **dc**=net.

**Required Privilege Level** secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

**Related Documentation**

## domain-name (Access Profile)

**Syntax** domain-name ***domain-name***;

**Hierarchy Level** [edit access profile ***profile-name*** client-name-filter]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify a domain name that must be in a client's name during the authentication process.

**Options** ***domain-name***—Domain name that must be in a client name. The name must not exceed 128 characters.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## fail

**Syntax** fail *string*;

**Hierarchy Level** [edit access firewall-authentication pass-through*profile-name* (ftp | http | telnet) banner]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the banner that a client sees if the authentication process fails.

**Options** ***string***—Banner text. Maximum length of the message text is 250 characters. Enclose the banner text within spaces or special characters—for example, quotation marks (" ").

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## firewall-authentication

**Syntax**

```
firewall-authentication {
  pass-through {
    default-profile profile-name;
    <ftp | http | telnet> {
      banner {
        fail string;
        login string;
        success string;
      }
    }
  }
  traceoptions {
    file filename <files number> <match regular-expression>
    <size maximum-file-size> <world-readable | no-world-readable>
    flag flag;
  }
  web-authentication {
    banner {
      success string;
    }
    default-profile profile-name;
  }
}
```

**Hierarchy Level** [edit access]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure default firewall authentication settings used by firewall authentication policies that restrict and permit access for firewall users to protected resources behind a firewall.

**Options** The remaining statements are explained separately.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

- Dynamic VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## firewall-user

**Syntax**

```
firewall-user {
    password password;
}
```

**Hierarchy Level** [edit access profile *profile-name* client *client-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify a client as a firewall user and the associated password (encrypted).

**Options** password *password*—Password used by the firewall user during local authentication.

**Range:** 1 through 128 characters

**Required Privilege Level** secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

**Related Documentation**

## ftp (Access)

**Syntax**

```
ftp {
    banner {
        fail string;
        login string;
        success string;
    }
}
```

**Hierarchy Level** [edit access firewall-authentication pass-through]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure banners for the FTP login prompt, successful authentication, and failed authentication.

**Options** The remaining statements are explained separately.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## group-profile (Access)

**Syntax**

```
group-profile profile-name {
  ppp {
    cell-overhead;
    encapsulated-overhead;
    framed-pool address-pool-name;
    idle-timeout seconds;
    interface-id interface-identifier;
    keepalive seconds;
    primary-dns IP address;
    primary-wins IP address;
    secondary-dns IP address;
    secondary-dns IP address;
  }
}
```

**Hierarchy Level** [edit access]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Configure a group profile to define Point-to-Point Protocol (PPP) attributes. Any client referencing the configured group profile inherits all the group profile attributes.

**Options**

- **ppp**—Configure Point-to-Point Protocol (PPP) attributes.
- **cell-overhead**—Configure the session to use Asynchronous Transfer Mode (ATM)-aware egress shaping.
- **framed-pool *pool-name***—Configure a framed-pool.
- **idle-timeout**—Configure the idle timeout for a user.
- **interface-id**—Configure the interface identifier.
- **keep-alive**—Configure the keepalive interval for an L2TP tunnel.
- **primary-dns**—Specify the primary-dns IP address.
- **secondary-dns**—Specify the secondary-dns IP address.
- **primary-wins**—Specify the primary-wins IP address.
- **secondary-wins**—Specify the secondary-wins IP address.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## http (Access)

**Syntax**

```
http {
  banner {
    fail string;
    login string;
    success string;
  }
}
```

**Hierarchy Level** [edit access firewall-authentication pass-through]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure banners for the HTTP login prompt, successful authentication, and failed authentication.

**Options** The remaining statements are explained separately.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

## ip-address (Access Profile)

**Syntax** ip-address *address*

**Hierarchy Level** [edit access profile *name* client *name* xauth]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Specify the IP address for the client.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## ldap-options

**Syntax**

```
ldap-options {
  assemble {
    common-name common-name;
  }
  base-distinguished-name base-distinguished-name;
  revert-interval seconds;
  search {
    admin-search {
      distinguished-name distinguished-name;
      password password;
    }
    search-filter filter-name;
  }
}
```

**Hierarchy Level** [edit access],
[edit access profile *profile-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure LDAP authentication options.

**Options** The remaining options are explained separately.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## ldap-server

**Syntax**

```
ldap-server server-address {
  port port-number;
  retry attempts;
  routing-instance routing-instance-name;
  source-address source-address;
  timeout seconds;
}
```

**Hierarchy Level** [edit access],
[edit access profile *profile-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify that the device use an LDAP server for authentication.

**Options** ***server-address***—Address of the LDAP authentication server.

The remaining statements are explained separately.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

## link (Access)

**Syntax** link *pool-name*;

**Hierarchy Level** [edit access address-assignment pool*pool-name*]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Configure the name of the secondary address-assignment pool that is linked to a primary address-assignment pool. The secondary pool provides a backup pool for local address assignment.

**Options** *pool-name*—Name of the address assignment pool.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## login (Access)

**Syntax** login *string*;

**Hierarchy Level** [edit access firewall-authentication pass-through default-profile *profile-name* (ftp | http | telnet) banner]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the login banner for users using FTP, HTTP, and Telnet during the authentication process.

**Options** ***string***—Banner text. Maximum length of the message text is 250 characters. Enclose the banner text within spaces or special characters—for example quotation marks (" ").

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

## name-server (Access)

**Syntax** name-server *address*

**Hierarchy Level** [edit access address-assignment pool <name> family (inet | inet6) xauth-attributes]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Specify the DNS server IP address for an address-assignment pool.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

- Device Configuration

Copyright © 2013, Juniper Networks, Inc.

## neighbor-discovery-router-advertisement (Access)

**Syntax** neighbor-discovery-router-advertisement *ndra-pool-name*;

**Hierarchy Level** [edit access address-assignment]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Configure the name of the address-assignment pool used to assign the router advertisement prefix.

**Options** *ndra-pool-name*—Name of the address assignment pool.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration

## network (Access)

**Syntax** network

**Hierarchy Level** [edit access address-assignment pool <name> family (inet | inet6)]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Specify the IPv4 network address for the pool. This attribute is mandatory. For an IPv6 pool, you will set the IPv6 network prefix.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## pass-through

**Syntax**

```
pass-through {
  default-profile profile-name;
  <ftp | http | telnet> {
    banner {
      fail string;
      login string;
      success string;
    }
  }
}
```

**Hierarchy Level** [edit access firewall-authentication]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure pass-through firewall user authentication, when a host or user from one zone needs to access a protected resource in another zone. A user must use an FTP, Telnet, or HTTP client to access the IP address of the protected resource and get authenticated by the firewall. The device uses FTP, Telnet, and HTTP to collect username and password information. Subsequent traffic from the user or host is allowed or denied based on the result of this authentication. After the user is authenticated, the firewall proxies the connection.

**Options** The remaining statements are explained separately.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## password (Access)

**Syntax** password *password*;

**Hierarchy Level** [edit access ldap-options search admin-search],
[edit access profile *profile-name* ldap-options search admin-search]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the plain-text password for the administrative user. This password is used in the bind for performing the LDAP search.

**Options** ***password***—Administrative user password.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## pool (Access)

**Syntax**

```
pool pool-name {
  family {
    inet {
      dhcp-attributes {
        boot-file boot file name;
        boot-server boot server name;
        domain-name domain name;
        grace-period seconds;
        maximum-lease-time seconds;
        name-server address;
        netbios-node-type type;
        option dhcp option-identifier-code;
        option-match {
          option-82 {
            circuit-id match-value;
            remote-id match-value;
          }
        }
        router IPv4 address;
        server-identifier IP address;
        tftp-server server name;
        wins-server IPv4 address;
      }
      host hostname;
      network network address;
      range range-name {
        high upper-limit;
        low lower-limit;
      }
      xauth-attributes {
        primary-dns IP address;
        primary-wins IP address;
        secondary-dns IP address;
        secondary-wins IP address;
      }
    }
    inet6 {
      dhcp-attributes {
        dns-server IPv6-address;
        grace-period seconds;
        maximum-lease-time seconds;
        option dhcp-option-identifier-code;
        sip-server-address IPv6-address;
        sip-server-domain-name domain-name;
      }
      prefix IPv6-network-prefix;
      range range-name {
        high upper-limit;
        low lower-limit;
        prefix-length delegated-prefix-length;
      }
    link pool-name;
```

Copyright © 2013, Juniper Networks, Inc.

}

**Hierarchy Level** [edit access address-assignment]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Configure the name of an address assignment pool. The remaining statements are explained separately.

**Options** ***pool-name***—Name assigned to the address-assignment pool.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

## port (Access LDAP)

**Syntax** port *port-number*;

**Hierarchy Level** [edit access ldap-server *server-address*],
[edit access profile *profile-name* ldap-server *server-address*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the port number on which to contact the LDAP server.

**Options** ***port-number***—Port number on which to contact the LDAP server.
**Default:** 389

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## port (Access RADIUS)

**Syntax** port *port-number*;

**Hierarchy Level** [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Configure the port number on which to contact the RADIUS server.

**Options** ***port-number***—Port number on which to contact the RADIUS server.
**Default:** 1812 (as specified in RFC 2865)

**Required Privilege Level** secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices

## prefix (Access IPv6)

**Syntax** prefix *IPv6-network prefix*;

**Hierarchy Level** [edit access address-assignment pool pool-name family inet6]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Specify the IPv6 prefix for the IPv6 address-assignment pool. This statement is mandatory for IPv6 address-assignment pools.

**Options** *IPv6-network-prefix*—IPv6 prefix.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## profile (Access)

**Syntax**

```
profile profile-name {
  accounting {
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    order [ radius ...]
    statistics;
  }
  address-assignment pool pool-name;
  authentication-order [ athentication-method1 authentication-method2 ... ]
  client client-name {
    chap-secret chap-secret;
    client-group [ group-names ];
    firewall-user {
      password password;
    }
    no-rfc2486;
    pap-password pap-password;
    x-auth client-ip-address;
    client-name-filter client-name {
      count number;
      domain-name domain-name;
      separator special-character;
    }
    ldap-options {
      assemble {
        common-name common-name;
      }
      base-distinguished-name base-distinguished-name;
      revert-interval seconds;
      search {
        admin-search {
          distinguished-name distinguished-name;
          password password;
        }
        search-filter filter-name;
      }
    }
    ldap-server server-address {
      port port-number;
      retry attempts;
      routing-instance routing-instance-name;
      source-address source-address;
      timeout seconds;
    }
    radius-options {
      revert-interval seconds;
    }
    radius-server server-address {
      port port-number;
      retry attempts;
      routing-instance routing-instance-name;
      secret password;
```


Copyright © 2013, Juniper Networks, Inc.

```
        source-address source-address;
        timeout seconds;
      }
      session-options {
        client-group [group-names];
        client-idle-timeout minutes;
        client-session-timeout minutes;
      }
    }
}
```

**Hierarchy Level** [edit access]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Create a profile containing a set of attributes that define device management access.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- Dynamic VPNs for Security Devices
- Master Administrator for Logical Systems on Security Devices
- Modem Interfaces
- Interfaces for Security Devices

## radius-options (Access)

**Syntax**

```
radius-options {
  revert-interval seconds;
}
```

**Hierarchy Level** [edit access],
[edit access profile *profile-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure RADIUS options.

**Options** The remaining statement is explained separately.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## radius-server (Access)

**Syntax**

```
radius-server server-address {
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    secret password;
    source-address source-address;
    timeout seconds;
}
```

**Hierarchy Level**

[edit access],
[edit access profile *profile-name*]

**Release Information**

Statement modified in Release 8.5 of Junos OS.

**Description**

Configure RADIUS for Layer 2 Tunneling Protocol (L2TP) or Point-to-Point Protocol (PPP) authentication.

To configure multiple RADIUS servers, include multiple **radius-server** statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

**Options**

***server-address***—Address of the RADIUS authentication server.

The remaining statements are explained separately.

**Required Privilege Level**

access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## range (Access)

**Syntax**

```
range range-name {
  high upper-limit;
  low lower-limit;
  prefix-length delegated-prefix-length;
}
```

**Hierarchy Level** [edit access address-assignment pool pool-name family inet6]
[edit access address-assignment pool pool-name family inet]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Configure an IP name range used within an address-assignment pool. For IPv4, you do not create a prefix-length.

**Options**

- *range-name*—Name of the range.
- **high** *upper-limit*—Upper limit of IPv6 address range.
- **low** *lower-limit*—Lower limit of IPv6 address range.
- **prefix-length** *delegated-prefix-length*—IPv6 delegated prefix length.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

## retry (Access LDAP)

**Syntax** retry *attempts*;

**Hierarchy Level** [edit access ldap-server *server-address*],
[edit access profile *profile-name* ldap-server *server-address*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the number of retries that a device can attempt to contact an LDAP server.

**Options** ***attempts***—Number of retries that the device is allowed to attempt to contact an LDAP server.

**Range:** 1 through 10

**Default:** 3

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## retry (Access RADIUS)

**Syntax** retry *attempts*;

**Hierarchy Level** [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Specify the number of retries that a device can attempt to contact a RADIUS authentication server.

**Options** ***attempts***—Number of retries that the device is allowed to attempt to contact a RADIUS server.

**Range:** 1 through 10

**Default:** 3

**Required Privilege Level** secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

**Related Documentation**

## revert-interval (Access LDAP)

**Syntax** revert-interval *seconds*;

**Hierarchy Level** [edit access ldap-options],
[edit access profile *profile-name* ldap-options]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the amount of time that elapses before the primary server is contacted if a backup server is being used.

**Options** ***seconds***—Number of seconds that elapse before the primary server is contacted.

**Range:** 60 through 4,294,967,295 seconds

**Default:** 600 seconds

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## revert-interval (Access RADIUS)

**Syntax** revert-interval *seconds*;

**Hierarchy Level** [edit access radius-options]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the amount of time that elapses before the primary server is contacted if a backup server is being used.

**Options** ***seconds***—Number of seconds that elapse before the primary server is contacted.
**Range:** 60 through 4,294,967,295 seconds
**Default:** 600 seconds

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

## routing-instance (Access LDAP)

**Syntax** routing-instance *routing-instance-name*;

**Hierarchy Level** [edit access ldap-server *server-address*],
[edit access profile *profile-name* ldap-server *server-address*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the routing instance used to send LDAP packets to the LDAP server. A routing instance is a collection of routing tables, the interfaces contained in the routing tables, and the routing protocol parameters that control the information in the routing tables.

**Options** ***routing-instance-name***—Name of the routing instance.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## routing-instance (Access RADIUS)

**Syntax** routing-instance *routing-instance-name*;

**Hierarchy Level** [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Configure the routing instance used to send RADIUS packets to the RADIUS server. A routing instance is a collection of routing tables, the interfaces contained in the routing tables, and the routing protocol parameters that control the information in the routing tables.

**Options** ***routing-instance-name*** —Name of the routing instance.

**Required Privilege Level** secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

**Related Documentation**

## search

**Syntax**

```
search {
  admin-search {
    distinguished-name distinguished-name;
    password password;
  }
  search-filter filter-name;
}
```

**Hierarchy Level** [edit access ldap-options],
[edit access profile *profile-name* ldap-options]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify that a search is used to get a user's LDAP distinguished name (DN). The search is performed based on the search filter and the part typed in by the user during authentication.

**Options** The remaining statements are explained separately.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## search-filter

**Syntax** search-filter *filter-name*;

**Hierarchy Level** [edit access ldap-options search],
[edit access profile *profile-name* ldap-options search]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify that a search filter is used to find the user's LDAP distinguished name (DN). For example, a filter of **cn** specifies that the search matches a user whose common name is the username.

**Options** ***filter-name***—Name of the filter used to find the user's distinguished name.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

## secret (Access Profile)

**Syntax** secret *password*;

**Hierarchy Level** [edit access profile *profile-name* radius-server *server-address*]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Specify the RADIUS secret password, which is shared between the router and the RADIUS server. The device uses this secret to encrypt the user's password that is sent to the RADIUS server.

**Options** ***password***—RADIUS secret. Maximum length is 256 characters.

**Required Privilege Level** secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## securid-server

**Syntax**

```
securid-server {
    server-name configuration-file filepath;
}
```

**Hierarchy Level** [edit access]

**Release Information** Statement introduced in Release 9.1 of Junos OS.

**Description** Configure SecurID server for SecurID authentication type.

**Options** The remaining statement is explained separately.



NOTE: You can configure only one SecurID server. SecurID challenges are not yet supported.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## separator

**Syntax** separator *special-character*;

**Hierarchy Level** [edit access profile *profile-name* client-name-filter *client-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify a character to identify where stripping of characters occurs in a client name. Stripping removes characters to the right of each instance of the specified character, plus the character itself. The stripping begins with the rightmost separator character.

Use the **separator** statement with the **count** statement to determine which characters in a client name are stripped. If the specified number of separator characters (count) exceeds the actual number of separator characters in the client name, stripping stops at the last available separator character.

**Options** ***special-character***—Character used to identify where to start the stripping of characters in a client name.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

## session-options (Access Profile)

**Syntax**

```
session-options {
  client-group [group-names];
  client-idle-timeout minutes;
  client-session-timeout minutes;
}
```

**Hierarchy Level** [edit access profile *profile-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Define options that control a user's session after successful authentication.

**Options** The remaining statements are explained separately.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## source-address (Access LDAP)

**Syntax** source-address *source-address*;

**Hierarchy Level** [edit access ldap-server server-address],
[edit access profile *profile-name* ldap-server *server-address*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure a source address for each configured LDAP server. Each LDAP request sent to a LDAP server uses the specified source address.

**Options** ***source-address***—Valid IP address configured on one of the device interfaces.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

## source-address (Access RADIUS)

**Syntax** source-address *source-address*;

**Hierarchy Level** [edit access radius-server *server-address*],
[edit access profile *profile-name* radius-server *server-address*]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Configure a source address for each configured RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address.

**Options** *source-address—Valid IP address configured on one of the device interfaces.*

**Required Privilege Level** secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## success

**Syntax** success *string*;

**Hierarchy Level** [edit access firewall-authentication pass-through default-profile *name* (ftp | http | telnet) banner],
[edit access firewall-authentication web-authentication]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the banner (message) that users see when trying to connect using FTP, HTTP, or Telnet after successful authentication.

**Options** ***string***—Banner text. Maximum length of the message text is 250 characters. Enclose the banner text within spaces or special characters—for example, quotation marks (" ").

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

## telnet (Access)

**Syntax**

```
telnet {
  banner {
    fail string;
    login string;
    success string;
  }
}
```

**Hierarchy Level** [edit access firewall-authentication pass-through]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure banners for Telnet login prompt, successful authentication, and failed authentication.

**Options** The remaining statements are explained separately.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## timeout (Access LDAP)

**Syntax** timeout *seconds*;

**Hierarchy Level** [edit access ldap-server *server-address*]
[edit access profile *profile-name* ldap-server *server-address*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the amount of time that the local device waits to receive a response from an LDAP server.

**Options** ***seconds***—Amount of time to wait.
**Range:** 1 through 90 seconds
**Default:** 3 seconds

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

## timeout (Access RADIUS)

**Syntax** timeout *seconds*;

**Hierarchy Level** [edit access radius-server *server-address*]
[edit access profile *profile-name* radius-server *server-address*]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Configure the amount of time that the local device waits to receive a response from a RADIUS server.

**Options** ***seconds***—Amount of time to wait.
**Range:** 1 through 90 seconds
**Default:** 3 seconds

**Required Privilege Level** secret—To view this statement in the configuration.
secret-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Access)

**Syntax**

```
traceoptions {
  file filename {
    files number;
    match regular-expression;
    size maximum-file-size;
    <world-readable | no-world-readable>;
  }
  flag flag;
}
```

**Hierarchy Level** [edit access firewall-authentication]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Define Routing Engine firewall authentication tracing options.

**Options**

- **file *filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.
- **files *number***—(Optional) Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file.0***, then ***trace-file.1***, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.
- If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

  **Range:** 2 through 1000 files

  **Default:** 10 files

- **match *regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.
- **size*maximum-file-size***—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file.0***. When the **trace-file** again reaches its maximum size, ***trace-file.0*** is renamed ***trace-file.1*** and ***trace-file*** is renamed ***trace-file.0***. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
- If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

  **Syntax:** ***x*** **k** to specify KB, ***x*** **m** to specify MB, or ***x*** **g** to specify GB

  **Range:** 10 KB through 1 GB

  **Default:** 128 KB

- **world-readable | no-world-readable**—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option

Copyright © 2013, Juniper Networks, Inc.

enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag *flag***—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags.
- **all**—All tracing operations
- **authentication**—Trace authentication events
- **configuration**—Trace configuration events
- **setup**—Trace setup of firewall authentication service

**Required Privilege Level**
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

## web-authentication (Access)

**Syntax**

```
web-authentication {
  banner {
    success string
  }
  default-profile default-profile;
}
```

**Hierarchy Level**
[edit access firewall-authentication]

**Release Information**
Statement introduced in Release 8.5 of Junos OS.

**Description**
Specify that users go through the Web authentication process. Users use HTTP to access an IP address on the **device** that is enabled for Web authentication. Users do not use HTTP to access the IP address of the protected resource in this case. Users are prompted for their username and password, which are verified by the device. Subsequent traffic from the user/host to the protected resource is allowed or denied based on the result of this authentication. This method of authentication differs from pass-through authentication in that users need to access the protected resource directly after accessing the Web authentication IP address and being authenticated.

**Options**
The remaining statements are explained separately.

**Required Privilege Level**
access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## wins-server (Access)

**Syntax** wins-server *address*

**Hierarchy Level** [edit access address-assignment pool <name> family (inet | inet6) xauth-attributes]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Specify the wins-server IP address.

**Required Privilege Level** access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**

## xauth-attributes

**Syntax**

```
xauth-attributes {
  primary-dns IP address;
  primary-wins IP address;
  secondary-dns IP address;
  secondary-wins IP address;
}
```

**Hierarchy Level** [edit access address-assignment pool <name> family (inet | inet6)]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Configure Xauth attributes.

**Options**

- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Do not inherit configuration data from these groups.
- **primary-dns**—Specify the primary-dns IP address.
- **secondary-dns**—Specify the secondary-dns IP address.
- **primary-wins**—Specify the primary-wins IP address.
- **secondary-wins**—Specify the secondary-wins IP address.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Dynamic VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 2

# Accounting-Options Hierarchy

This section contains the following topics:


- Accounting-Options Configuration Statement Hierarchy on page 53


## Accounting-Options Configuration Statement Hierarchy

Use the statements in the **accounting-options** configuration hierarchy to collect and log data about basic system operations and services on the device.

```
accounting-options {
  class-usage-profile profile-name {
    destination-classes {
      destination-class-name;
    }
    file filename;
    interval minutes;
    source-classes {
      source-class-name;
    }
  }
  file filename {
    archive-sites {
      site-name;
    }
    files file-number;
    nonpersistent;
    size bytes;
    start-time time;
    transfer-interval minutes;
  }
  filter-profile profile-name {
    counters {
      counter name;
    }
    file filename;
    interval minutes;
  }
  interface-profile profile-name {
    fields {
      field-name;
    }
```

Copyright © 2013, Juniper Networks, Inc.

```
    file filename;
    interval minutes;
  }
  mib-profile profile-name {
    file filename;
    interval minutes;
    object-names {
      mib-object-name;
    }
    operation operation-name;
  }
  routing-engine-profile profile-name {
    fields {
      field-name;
    }
    file filename;
    interval minutes;
  }
}
```

**Related Documentation**

- Initial Configuration for Security Devices
- MPLS for Security Devices


Copyright © 2013, Juniper Networks, Inc.

CHAPTER 3

# Applications Hierarchy and Statements

This section contains the following topics:


- Applications Configuration Statement Hierarchy on page 55


## Applications Configuration Statement Hierarchy

Use the statements in the **applications** configuration hierarchy to configure applications properties and group applications objects for Domain Name Service (DNS), File Transfer Protocol (FTP), Media Gateway Control Protocol with Call Agent, Media Gateway Control Protocol with User Agent, Microsoft RPC, Point-to-Point Tunneling Protocol, ISDN connection control protocol (Q.931), Remote Access Service, RealAudio, UNIX remote shell services, Real-Time Streaming Protocol, Skinny Client Control Protocol, Session Initiation Protocol, Oracle SQLNET v2, Sun Microsystems RPC, the TALK program, and Trivial File Transfer Protocol.

```
applications {
  application application-name {
    application-protocol protocol-name;
    description text;
    destination-port port-number;
    icmp-code value;
    icmp-type value;
    inactivity-timeout seconds ;
    protocol type;
    rpc-program-number number;
    source-port port-number;
    term term-name {
      alg application;
      destination-port port-number;
      icmp-code value;
      icmp-type value;
      inactivity-timeout seconds;
      protocol type;
      rpc-program-number number;
      source-port port-number;
      uuid hex-value;
    }
    uuid hex-value;
  }
  application-set application-set-name {
```

Copyright © 2013, Juniper Networks, Inc.

```
        [application application-name ];
        description text;
    }
}
```

**Related Documentation**

- Application Layer Gateways for Security Devices
- Security Policy Applications for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## alg (Applications)

**Syntax** alg *application*;

**Hierarchy Level** [edit applications application *application-name* term *term-name* ]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Define individual Application Layer Gateway (ALG).

**Options** *application* —Name of the application. The following protocols are supported:

- **dns**—Domain Name Service
- **ftp**—File Transfer Protocol
- **ignore**—Ignore application type
- **mgcp-ca**—Media Gateway Control Protocol with Call Agent
- **mgcp-ua**—MGCP with User Agent
- **ms-rpc**—Microsoft RPC
- **pptp**—Point-to-Point Tunneling Protocol
- **q931**—ISDN connection control protocol (Q.931)
- **ras**—Remote Access Service
- **realaudio**—RealAudio
- **rsh**—UNIX remote shell services
- **rtsp**—Real-Time Streaming Protocol
- **sccp**—Skinny Client Control Protocol
- **sip**—Session Initiation Protocol
- **sqlnet-v2**—Oracle SQLNET v2
- **sun-rpc**—Sun Microsystems RPC
- **talk**—TALK program
- **tftp**—Trivial File Transfer Protocol

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Application Layer Gateways for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## application-protocol (Applications)

**Syntax** application-protocol *protocol-name*;

**Hierarchy Level** [edit applications application *application-name* ]

**Release Information** Statement modified in Junos OS Release 8.5. The **ike-esp-nat** option introduced in Junos OS Release 10.2.

**Description** Identify the application protocol name.

**Options** *protocol-name* —Name of the protocol. The following protocols are supported:

- **dns**—Domain Name Service
- **ftp**—File Transfer Protocol
- **ignore**—Ignore application type
- **ike-esp-nat**—IKE ESP NAT application protocol
- **mgcp-ca**—Media Gateway Control Protocol with Call Agent
- **mgcp-ua**—MGCP with User Agent
- **ms-rpc**—Microsoft RPC
- **pptp**—Point-to-Point Tunneling Protocol
- **q931**—ISDN connection control protocol (Q.931)
- **ras**—Remote Access Service
- **realaudio**—RealAudio
- **rsh**—UNIX remote shell services
- **rtsp**—Real-Time Streaming Protocol
- **sccp**—Skinny Client Control Protocol
- **sip**—Session Initiation Protocol
- **sqlnet-v2**—Oracle SQLNET v2
- **sun-rpc**—Sun Microsystems RPC
- **talk**—TALK program
- **tftp**—Trivial File Transfer Protocol

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Security Policy Applications for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## description (Applications)

**Syntax** description *text*;

**Hierarchy Level** [edit applications application *application-name*]
[edit applications application-set *application-set-name*]

**Release Information** Statement introduced in Junos OS Release 12.1.

**Description** Specify descriptive text for an application or an application set.



NOTE: The descriptive text should not include characters, such as “<”, “>”, “&”, or “\n”.

**Options** ***text***—Descriptive text about an application or an application set.

**Range:** 1 through 300 characters



NOTE: The upper limit of the description text range is related to character encoding, and is therefore dynamic. However, if you configure the descriptive text length beyond 300 characters, the configuration might fail to take effect.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policy Applications for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## destination-port (Applications)

**Syntax** **destination-port** *port-number*;

**Hierarchy Level** **[edit applications application** *application-name* **],**
**[edit applications application** *application-name* **term** *term-name* **]**

**Release Information** Statement modified in Junos OS Release 8.5.

**Description** Specify a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) destination port number.

**Options** ***port-number*** —Range of ports. You can use a numeric value or one of the text synonyms listed in Table 3 on page 61.

 Copyright © 2013, Juniper Networks, Inc.

### Table 3: Port Supported by Services Interfaces

| Port Name | Corresponding Port Number |
|---|---|
| **afs** | 1483 |
| **bgp** | 179 |
| **biff** | 512 |
| **bootpc** | 68 |
| **bootps** | 67 |
| **cmd** | 514 |
| **cvspserver** | 2401 |
| **dhcp** | 67 |
| **domain** | 53 |
| **eklogin** | 2105 |
| **ekshell** | 2106 |
| **excc** | 512 |
| **finger** | 79 |
| **ftp** | 21 |
| **ftp-data** | 20 |
| **http** | 80 |
| **https** | 443 |
| **ident** | 113 |
| **imap** | 143 |
| **kerberos-sec** | 88 |
| **klogin** | 543 |
| **kpasswd** | 761 |
| **krb-prop** | 754 |
| **krbupdate** | 760 |

Copyright © 2013, Juniper Networks, Inc.

Table 3: Port Supported by Services Interfaces *(continued)*

| Port Name | Corresponding Port Number |
|---|---|
| kshell | 544 |
| ldap | 389 |
| ldp | 646 |
| login | 513 |
| mobileip-agent | 434 |
| mobilip-mn | 435 |
| msdp | 639 |
| netbios-dgm | 138 |
| netbios-ns | 137 |
| netbios-ssn | 139 |
| nfsd | 2049 |
| nntp | 119 |
| ntalk | 518 |
| ntp | 123 |
| pop3 | 110 |
| pptp | 1723 |
| printer | 515 |
| radacct | 1813 |
| radius | 1812 |
| rip | 520 |
| rkinit | 2108 |
| smtp | 25 |
| snmp | 161 |
| snmp-trap | 162 |


Copyright © 2013, Juniper Networks, Inc.

Table 3: Port Supported by Services Interfaces *(continued)*

| Port Name | Corresponding Port Number |
|---|---|
| **snpp** | 444 |
| **socks** | 1080 |
| **ssh** | 22 |
| **sunrpc** | 111 |
| **syslog** | 514 |
| **tacacs** | 49 |
| **tacacs-ds** | 65 |
| **talk** | 517 |
| **telnet** | 23 |
| **tftp** | 69 |
| **timed** | 525 |
| **who** | 513 |
| **xdmcp** | 177 |

**Required Privilege Level**
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Security Policy Applications for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## icmp-code (Applications)

**Syntax** **icmp-code** *value*;

**Hierarchy Level** **[edit applications application** *application-name* **term** *term-name* **]**

**Release Information** Statement modified in Junos OS Release 8.5.

**Description** Specify the Internet Control Message Protocol (ICMP) code value.

**Options** *value* —ICMP code value, such as **host-unreachable** or **host-unreachable-for-tos**.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Security Policy Applications for Security Devices

## icmp-type (Applications)

**Syntax** **icmp-type** *value*;

**Hierarchy Level** **[edit applications application** *application-name* **term** *term-name* **]**

**Release Information** Statement modified in Junos OS Release 8.5.

**Description** Specify the ICMP packet type value.

**Options** *value* —ICMP type value, such as **echo** or **echo-reply**.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Security Policy Applications for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## inactivity-timeout (Applications)

**Syntax** inactivity-timeout *seconds*;

**Hierarchy Level** [edit applications application *application-name* term *term-name* ]

**Release Information** Statement modified in Junos OS Release 8.5.

**Description** Inactivity timeout period, in seconds.

**Options** *seconds* —Length of time the application is inactive before it times out.
**Default:** For TCP, 1800 seconds; for UDP, 60 seconds.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Security Policy Applications for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## protocol (Applications)

**Syntax** protocol *type*;

**Hierarchy Level** [edit applications application *application-name* ],
[edit applications application *application-name* term *term-name* ]

**Release Information** Statement modified in Junos OS Release 8.5.

**Description** Specify the networking protocol name or number.

**Options** *protocol-name* —Networking protocol name. The following text values are supported. For a complete list of possible numeric values, see RFC 1700, *Assigned Numbers (for the Internet Protocol Suite)*.

- **ah**—IP Security Authentication Header
- **egp**—Exterior gateway protocol
- **esp**—IPsec Encapsulating Security Payload
- **gre**—Generic routing encapsulation
- **icmp**—Internet Control Message Protocol
- **igmp**—Internet Group Management Protocol
- **ipip**—IP over IP
- **node**—Clear each session that uses the specified IP protocol on a specific node.
- **ospf**—Open Shortest Path First
- **pim**—Protocol Independent Multicast
- **rsvp**—Resource Reservation Protocol
- **sctp**—Stream Control Transmission Protocol
- **tcp**—Transmission Control Protocol
- **udp**—User Datagram Protocol



NOTE: Internet Protocol version 6 (IPv6) is not supported as a network protocol in application definitions

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Security Policy Applications for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## rpc-program-number (Applications)

**Syntax** rpc-program-number *number*;

**Hierarchy Level** [edit applications application *application-name* term *term-name* ]

**Release Information** Statement modified in Junos OS Release 8.5.

**Description** Specify the remote procedure call (RPC) or Distributed Computing Environment (DCE) value.

**Options** *number* —RPC or DCE program value.
**Range:** 0 through 65,535

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Security Policy Applications for Security Devices

## source-port (Applications)

**Syntax** source-port *port-number* ;

**Hierarchy Level** [edit applications application *application-name* ],
[edit applications application *application-name* term *term-name* ]

**Release Information** Statement modified in Junos OS Release 8.5.

**Description** Specify the source port identifier.

**Options** *port-number* —Identifier for the port. You can use a numeric value or one of the text synonyms listed in destination-port (Applications).

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Security Policy Applications for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## term (Applications)

**Syntax**

```
term term-name {
  alg application ;
  destination-port port-number;
  icmp-code value ;
  icmp-type value;
  inactivity-timeout seconds;
  protocol type;
  rpc-program-number number;
  source-port port-number;
  uuid hex-value;
}
```

**Hierarchy Level** [edit applications application *application-name* ]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Define individual application protocols.

**Options** The remaining statements are explained separately.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Security Policy Applications for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## uuid (Applications)

**Syntax** uuid *hex-value*;

**Hierarchy Level** [edit applications application *application-name* term *term-name* ]

**Release Information** Statement modified in Junos OS Release 8.5.

**Description** Specify the Universal Unique Identifier (UUID) for objects. DCE RPC services are mainly used by Microsoft applications. The ALG uses well-known TCP port 135 for port mapping services and uses the Universal Unique Identifier (UUID) instead of the program number to identify protocols. The main application-based DCE RPC is the Microsoft Exchange Protocol.

Support for stateful firewall and NAT services requires that you configure the DCE RPC port map ALG on TCP port 135. The DCE RPC ALG uses the TCP protocol with application-specific UUIDs.

**Options** *hex-value* —Hexadecimal value.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Security Policy Applications for Security Devices

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 4

# Bridge-Domains Hierarchy and Statements

This section contains the following topics:


- Bridge-Domains Configuration Statement Hierarchy on page 71


## Bridge-Domains Configuration Statement Hierarchy

Use the statements in the **bridge-domains** configuration hierarchy to configure a bridging domain that includes a set of logical ports that share the same flooding or broadcast characteristics.

```
bridge-domains bridge-domain-name {
  description description
  domain-type bridge;
  interface interface-name;
  vlan-id (none | number);
  vlan-id-list numbers;
  routing-interface routing-interface-name;
  bridge-options {
    interface interface-name;
    static-mac static-mac-address;
  }
}
```

**Related Documentation**

- Layer 2 Bridging and Transparent Mode for Security Devices
- Layer 2 Bridging and Switching for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## bridge-domains (Bridge Domains)

**Syntax**

```
bridge-domains bridge-domain-name {
  description description
  domain-type bridge;
  interface interface-name;
  vlan-id (none | number);
  vlan-id-list numbers;
  routing-interface routing-interface-name;
  bridge-options {
    interface interface-name;
    static-mac static-mac-address;
  }
}
```

**Hierarchy Level** [edit]

**Release Information** Statement modified in Release 9.5 of Junos OS.

**Description** Configure a domain that includes a set of logical ports that share the same flooding or broadcast characteristics in order to perform Layer 2 bridging.

**Options** ***bridge-domain-name***—Name of the bridge domain.

The remaining statements are explained separately.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**

- Layer 2 Bridging and Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## bridge-options (Bridge Domains)

**Syntax**

```
bridge-options {
  interface interface-name;
    static-mac static-mac-address;
  vlan-id number
}
```

**Hierarchy Level** [edit bridge-domains *bridge-domain-name*]

**Release Information** Statement modified in Release 9.5 of Junos OS.

**Description** Configure Layer 2 learning and forwarding properties for a bridge domain.

The remaining statements are explained separately.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**

- Layer 2 Bridging and Transparent Mode for Security Devices
- Layer 2 Bridging and Switching for Security Devices

## domain-type (Bridge Domains)

**Syntax** domain-type bridge;

**Hierarchy Level** [edit bridge-domains *bridge-domain-name*]

**Release Information** Statement modified in Release 9.5 of Junos OS.

**Description** Define the type of domain for a Layer 2 bridge domain.

**Required Privilege Level** routing—To view this statement in the configuration.
routing–control—To add this statement to the configuration.

**Related Documentation**

- Layer 2 Bridging and Transparent Mode for Security Devices
- Layer 2 Bridging and Switching for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## interface (Bridge Domains)

**Syntax** interface *interface-name*;

**Hierarchy Level** [edit bridge-domains *bridge-domain-name* bridge-options]

**Release Information** Statement modified in Release 9.5 of Junos OS.

**Description** Specify the logical interfaces to include in the bridge domain.

**Options** ***interface-name***—Name of a logical interface.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- Layer 2 Bridging and Transparent Mode for Security Devices
- Layer 2 Bridging and Switching for Security Devices
- Interfaces for Security Devices

## routing-interface (Bridge Domains)

**Syntax** routing-interface *routing-interface-name*;

**Hierarchy Level** [edit bridge-domains *bridge-domain-name*]

**Release Information** Statement modified in Release 9.5 of Junos OS.

**Description** Specify a routing interface to include in a bridge domain.

**Options** ***routing-interface-name***—Name of the integrated routing and bridging (IRB) interface to include in the bridge domain. The format of the interface name is **irb.*x***, where ***x*** is the unit number of the interface you configured at the **[edit interfaces irb]** hierarchy level.



NOTE: You can specify only one IRB interface for each bridge domain.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- Layer 2 Bridging and Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## static-mac (Bridge Domains)

**Syntax** static-mac *mac-address*

**Hierarchy Level** [edit bridge-domains *bridge-domain-name* bridge-options interface *interface-name*]

**Release Information** Statement modified in Release 9.5 of Junos OS.

**Description** Configure a static MAC address for a logical interface in a bridge domain.

**Options** ***mac-address***—MAC address

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**

- Layer 2 Bridging and Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## vlan-id (Bridge Domain)

**Syntax** vlan-id (all | none | *number*);

**Hierarchy Level** [edit bridge-domains *bridge-domain-name*],
[edit logical-systems *logical-system-name* bridge-domainss *bridge-domain-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* bridge-domains *bridge-domain-name*],
[edit routing-instances *routing-instance-name* bridge-domains *bridge-domain-name*]

**Release Information** Statement introduced in Junos OS Release 8.4.
Support for Layer 2 trunk ports added in Junos OS Release 9.2.
Support for logical systems added in Junos OS Release 9.6.

**Description** (MX Series routers only) Specify a VLAN identifier (VID) to include in the packets sent to and from the bridge domain or a VPLS routing instance.



NOTE: When configuring a VLAN identifier for provider backbone bridge (PBB) routing instances, dual-tagged VIDs and the none option are not permitted.

**Options** *number*—A valid VLAN identifier. If you configure multiple bridge domains with a valid VLAN identifier, you must specify a unique VLAN identifier for each domain. However, you can use the same VLAN identifier for bridge domains that belong to different virtual switches. Use this option to send singly tagged frames with the specified VLAN identifier over VPLS VT interfaces.



NOTE: If you specify a VLAN identifier, you cannot also use the all option. They are mutually exclusive.

**all**—Specify that the bridge domain spans all the VLAN identifiers configured on the member logical interfaces.



NOTE: You cannot specify the all option if you include a routing interface in the bridge domain.

**none**—Specify to enable shared VLAN learning or to send untagged frames over VPLS VT interfaces.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.


Copyright © 2013, Juniper Networks, Inc.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- Configuring a Bridge Domain
- Configuring VLAN Identifiers for Bridge Domains and VPLS Routing Instances
- Configuring Bridge Domains as Switches for Layer 2 Trunk Ports
- Configuring a Layer 2 Virtual Switch
- Example: Configuring E-LINE and E-LAN Services for a PBB Network on MX Series Routers

## vlan-id-list (Bridge Domains)

**Syntax** vlan-id-list *numbers*;

**Hierarchy Level** [edit bridge-domains *bridge-domain-name*]

**Release Information** Statement modified in Release 9.5 of Junos OS.

**Description** Specify multiple VLAN identifiers to create a bridge domain for each VLAN identifier.

**Options** *numbers*—A list of valid VLAN identifiers. A bridge domain is created for each VLAN identifier in the list.



NOTE: If you specify a VLAN identifier list, you cannot configure an IRB interface in the bridge domain.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- Layer 2 Bridging and Switching for Security Devices

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 5

# Chassis Hierarchy and Statements

This section contains the following topics:


- Chassis Configuration Statement Hierarchy on page 79


## Chassis Configuration Statement Hierarchy

Use the statements in the **chassis** configuration hierarchy to configure alarms, aggregated devices, clusters, the routing engine, and other chassis properties.

```
chassis {
    aggregated-devices {
        ethernet {
            device-count number;
        }
    }
    alarm {
        ds1 {
            ais (ignore | red | yellow);
            ylw (ignore | red | yellow);
        }
        ethernet {
            link-down (ignore | red | yellow);
        }
        integrated-services {
            failure (ignore | red | yellow);
        }
        management-ethernet {
            link-down (ignore | red | yellow);
        }
        serial {
            cts-absent (ignore | red | yellow);
            dcd-absent (ignore | red | yellow);
            dsr-absent (ignore | red | yellow);
            loss-of-rx-clock (ignore | red | yellow);
            loss-of-tx-clock (ignore | red | yellow);
        }
        services {
            hw-down (ignore | red | yellow);
            linkdown (ignore | red | yellow);
            pic-hold-reset (ignore | red | yellow);
            pic-reset (ignore | red | yellow);
```

Copyright © 2013, Juniper Networks, Inc.

```
    rx-errors (ignore | red | yellow);
    sw-down (ignore | red | yellow);
    tx-errors (ignore | red | yellow);
  }
  sonet {
    alarm-name  (ignore | red | yellow);
  }
  t3 {
    ais (ignore | red | yellow);
    exz (ignore | red | yellow);
    ferf (ignore | red | yellow);
    idle (ignore | red | yellow);
    lcv (ignore | red | yellow);
    lof (ignore | red | yellow);
    los (ignore | red | yellow);
    pll (ignore | red | yellow);
    ylw (ignore | red | yellow);
  }
}
cluster {
  control-link-recovery;
  control-ports {
    fpc slot-number port port-number;
  }
  heartbeat-interval milliseconds;
  heartbeat-threshold number;
  node node-number;
  redundancy-group group-number {
    gratuitous-arp-count number;
    hold-down-interval number;
    interface-monitor interface-name {
      weight number;
    }
    ip-monitoring {
      global-threshold number;
      global-weight number;
      retry-count count;
      retry-interval interval;
      family {
          inet {
            IP address {
                weight number;
                interface rethX.logical-unit-number secondary-ip-address IP address;
              }
          }
      }
    }
    node node-number {
      priority priority-number;
    }
    preempt;
  }
  reth-count number;
  traceoptions {
    file filename {
      <files number>;
```


Copyright © 2013, Juniper Networks, Inc.

```
        <match regular-expression>;
        <size maximum-file-size>;
        <world-readable | no-world-readable>;
      }
      flag {
        all;
        configuration;
        routing-socket;
        snmp;
      }
    }
  }
  config-button {
    no-clear;
    no-rescue;
  }
  container-devices {
    device-count container-devices-number;
  }
  craft-lockout;
  disable-power-management;
  fpc slot-number {
    offline;
    pic pic-number {
      aggregate-ports;
      atm-cell-relay-accumulation;
      atm-l2circuit-mode (cell | aal5 | trunk trunk );
      ce1 {
        e1 port-number {
          channel-group group-number timeslots slot-number;
        }
      }
      ct3 {
        port port-number {
          t1 link-number {
            channel-group group-number timeslots slot-number;
          }
        }
      }
      ds1{
        pic-mode (clear-channel | voice-ct1);
      }
      ethernet {
        pic-mode (enhanced-switching | routing | switching);
      }
      framing (sdh | sonet);
      idle-cell-format {
        itu-t;
        payload-pattern payload-pattern-byte;
      }
      max-queues-per-interface (4 | 8);
      mlfr-uni-nni-bundles number;
      no-concatenate;
      port port-number {
        framing (e3 | t3);
      }
```

```
        q-pic-large-buffer <(large-scale | small-scale)>;
        red-buffer-occupancy {
          weighted-averaged [ instant-usage-weight-exponent weight-value ];
        }
        services-offload;
        shdsl {
          pic-mode (1-port-atm | 2-port-atm);
        }
        sparse-dlcis;
        traffic-manager {
          egress-shaping-overhead number;
          ingress-shaping-overhead number;
          mode ( egress-only | ingress-and-egress);
        }
        tunnel-queuing;
        tunnel-services {
          bandwidth (1g | 10g);
        }
        vtmapping (itu-t | klm);
      }
      power (off | on);
    }
    network-management {
      cluster-master;
    }
    pem {
      minimum number;
    }
    redundancy {
      failover {
        on-disk-failure;
        on-loss-of-keepalives;
      }
      graceful-switchover;
      keepalive-time seconds;
      routing-engine slot-number (backup | disabled | master);
    }
    routing-engine {
      on-disk-failure disk-failure-action (halt | reboot);
      bios {
        no-auto-upgrade;
        }
    }
  }
```

**Related Documentation**

- IP Monitoring
- Chassis Cluster for Security Devices
- Junos OS System Basics Configuration Guide
- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## apply-groups (Chassis Cluster)

**Syntax** apply-groups *[${node}]*

**Hierarchy Level** [edit chassis cluster]

**Release Information** Statement introduced in Junos OS Release 9.0.

**Description** Apply node-specific parameters to each node in a chassis cluster.

**Options** ***${node}*** —Each node (node 0 or node 1) in a chassis cluster.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Chassis Cluster for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## cluster (Chassis)

**Syntax**

```
cluster {
  control-link-recovery;
  control-ports {
    fpc slot-number port port-number;
  }
  heartbeat-interval milliseconds;
  heartbeat-threshold number;
  node node-number ;
  redundancy-group group-number {
    gratuitous-arp-count number;
    hold-down-interval number;
    interface-monitor interface-name {
      weight number;
    }
    ip-monitoring {
      global-weight number;
      global-threshold number;
      retry-count count;
      retry-interval interval;
      family {
          inet {
            IP address {
                weight number;
                interface rethX.logical-unit-number secondary-ip-address IP address;
              }
          }
      }
    }
    node node-number {
      priority priority-number ;
    }
    preempt;
  }
  reth-count number;
  traceoptions {
    file filename {
      <files number >;
      <match regular-expression> ;
      <size maximum-file-size >;
      <world-readable | no-world-readable>;
    }
    flag {
      all;
      configuration;
      routing-socket;
      snmp;
    }
  }
}
```

**Hierarchy Level** [edit chassis]


Copyright © 2013, Juniper Networks, Inc.

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Configure a chassis cluster.

**Options** The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- IP Monitoring
- Chassis Cluster for Security Devices
- Master Administrator for Logical Systems on Security Devices

## control-link-recovery

**Syntax** control-link-recovery;

**Hierarchy Level** [edit **chassis cluster**]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Enable control link recovery to be done automatically by the system. After the control link recovers, the system checks whether it receives at least 30 consecutive heartbeats on the control link. This is to ensure that the control link is not flapping and is perfectly healthy. Once this criterion is met, the system issues an automatic reboot on the node that was disabled when the control link failed. When the disabled node reboots, the node rejoins the cluster. There is no need for any manual intervention.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Chassis Cluster for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## control-ports

**Syntax**

```
control-ports {
  fpc slot-number port port-number;
}
```

**Hierarchy Level** [edit chassis cluster]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for dual control ports added in Release 10.0 of Junos OS.

**Description** Enable the specific control port of the Services Processing Card (SPC) for use as a control link for the chassis cluster. By default, all control ports are disabled. User needs to configure a minimum of one control port per chassis of the cluster. If user configures port 0 only, the Juniper Services Redundancy Protocol process (jsrpd) does not send control heartbeats on control link 1 and the counters it sends will show zeroes.

**Options**

- fpc ***slot-number*** —Flexible PIC Concentrator (FPC) slot number.

  NOTE: FPC slot range depends on platform. The maximum range of 0 through 23 applies to SRX5800 devices; for SRX5600 devices, the only applicable range is 0 through 11.

- port ***port-number*** —Port number on which to configure the control port.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Chassis Cluster for Security Devices

## framing (Chassis)

**Syntax** framing (e3 | t3);

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number* port *port-number*]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Specifies the DS3 (t3) or E3 framing mode for the 1-Port Clear Channel DS3/E3 GPIM on an SRX650 device. By default, the GPIM port is configured in t3 mode.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Interfaces for Security Devices
- Feature Support Reference for SRX Series and J Series Devices


Copyright © 2013, Juniper Networks, Inc.

## fru-poweron-sequence

**Syntax** fru-poweron-sequence *fru-poweron-sequence*;

**Hierarchy Level** [edit chassis]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Configure the power-on sequence for FPCs installed in the chassis.

**Options** **fru-poweron-sequence**—Power-on sequence for the FPCs in the chassis. The numbers indicate the slot number of the FPCs.



NOTE: If the power-on sequence is not configured by including the **fru-poweron-sequence** statement, Junos OS uses the ascending order of the the FPC slot numbers as the sequence for powering on the FPCs.



NOTE: The FPC online sequence is not dependent on the FPC power-on sequence.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Flow-Based Processing for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## global-threshold

**Syntax** global-threshold *number*;

**Hierarchy Level** [edit chassis cluster redundancy-group *group-number* ip-monitoring ]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** Specify the failover value for all IP addresses monitored by the redundancy group. When IP addresses with a configured total weight in excess of the threshold have become unreachable, the weight of IP monitoring is deducted from the redundancy group threshold.

**Options** *number* —Value at which the IP monitoring weight will be applied against the redundancy group failover threshold.

**Range:** 0 through 255

**Default:** 0

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- IP Monitoring
- Chassis Cluster for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## global-weight

**Syntax** global-weight *number*;

**Hierarchy Level** [edit chassis cluster redundancy-group *group-number* ip-monitoring ]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** Specify the relative importance of all IP address monitored objects to the operation of the redundancy group. Every monitored IP address is assigned a weight. If the monitored address becomes unreachable, the weight of the object is deducted from the global-threshold of IP monitoring objects in its redundancy group. When the global-threshold reaches 0, the global-weight is deducted from the redundancy group. Every redundancy group has a default threshold of 255. If the threshold reaches 0, a failover is triggered. Failover is triggered even if the redundancy group is in manual failover mode and preemption is not enabled.

**Options** *number*—Combined weight assigned to all monitored IP addresses. A higher weight value indicates a greater importance.

**Range:** 0 through 255

**Default:** 255

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- IP Monitoring
- Chassis Cluster for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## gratuitous-arp-count

**Syntax** gratuitous-arp-count *number*;

**Hierarchy Level** [edit chassis cluster redundancy-group group-number]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Specify the number of gratuitous Address Resolution Protocol (ARP) requests to send on an active interface after failover.

**Options** ***number***—Number of gratuitous ARP requests that a newly elected primary device in a chassis cluster sends out to announce its presence to the other network devices.

**Range:** 1 through 16

**Default:** 4

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Chassis Cluster for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## heartbeat-interval

**Syntax** heartbeat-interval *milliseconds*;

**Hierarchy Level** [edit **chassis cluster**]

**Release Information** Statement introduced in Release 9.0 of Junos OS.
Statement updated in Release 10.4 of Junos OS.

**Description** Set the interval between the periodic signals broadcast to the devices in a chassis cluster to indicate that the active node is operational.

The **heartbeat-interval** option works in combination with the **heartbeat-threshold** option to define the wait time before failover is triggered in a chassis cluster. The default values of these options produce a wait time of 3 seconds. In a large configuration approaching full capacity on an SRX5600 or SRX5800 device, however, we recommend that you increase the failover wait time to 5 seconds. For a large configuration on an SRX3400 or SRX3600 device, increase the failover wait time to 8 seconds.

For example, a **heartbeat-threshold** of 3 and a **heartbeat-interval** of 1000 milliseconds result in a total wait of 3 seconds before failover is triggered. To increase this wait to 5 seconds, you could increase the **heartbeat-threshold**, the **heartbeat-interval**, or both. A **heartbeat-threshold** of 5 and a **heartbeat-interval** of 1000 milliseconds would yield a wait time of 5 seconds. Setting the **heartbeat-threshold** to 4 and the **heartbeat-interval** to 1250 milliseconds would also yield a wait time of 5 seconds.

**Options** ***milliseconds*** —Time interval between any two heartbeat messages.

**Range:** 1000 through 2000 milliseconds

**Default:** 1000 milliseconds

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Chassis Cluster for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## heartbeat-threshold

**Syntax** heartbeat-threshold *number*;

**Hierarchy Level** [edit **chassis cluster**]

**Release Information** Statement introduced in Release 9.0 of Junos OS.
Statement updated in Release 10.4 of Junos OS.

**Description** Set the number of consecutive missed heartbeat signals that a device in a chassis cluster must exceed to trigger failover of the active node.

The **heartbeat-threshold** option works in combination with the **heartbeat-interval** option to define the wait time before failover is triggered in a chassis cluster. The default values of these options produce a wait time of 3 seconds. In a large configuration approaching full capacity on an SRX5600 or SRX5800 device, however, we recommend that you increase the failover wait time to 5 seconds. For a large configuration on an SRX3400 or SRX3600 device, increase the failover wait time to 8 seconds.

For example, a **heartbeat-threshold** of 3 and a **heartbeat-interval** of 1000 milliseconds result in a total wait of 3 seconds before failover is triggered. To increase this wait to 5 seconds, you could increase the **heartbeat-threshold**, the **heartbeat-interval**, or both. A **heartbeat-threshold** of 5 and a **heartbeat-interval** of 1000 milliseconds would yield a wait time of 5 seconds. Setting the **heartbeat-threshold** to 4 and the **heartbeat-interval** to 1250 milliseconds would also yield a wait time of 5 seconds.

**Options** *number* —Number of consecutive missed heartbeats.
**Range:** 3 through 8
**Default:** 3

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Chassis Cluster for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## hold-down-interval

**Syntax** hold-down-interval *number*;

**Hierarchy Level** [edit chassis cluster redundancy-group *group-number*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Set the minimum interval to be allowed between back-to-back failovers for the specified redundancy group (affects manual failovers, as well as automatic failovers associated with monitoring failures).

For redundancy group 0, this setting prevents back-to-back failovers from occurring less than 5 minutes (300 seconds) apart. Note that a redundancy group 0 failover implies a Routing Engine failure.

For some configurations, such as ones with a large number of routes or logical interfaces, the default or specified interval for redundancy group 0 might not be sufficient. In such cases, the system automatically extends the dampening time in increments of 60 seconds until the system is ready for failover.

**Options** *number*—Number of seconds specified for the interval.

**Range:** For redundancy group 0, 300 through 1800 seconds; for redundancy group 1 through 128, 0 through 1800 seconds.

**Default:** For redundancy group 0, 300 seconds; for redundancy group 1 through 128, 1 second.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Chassis Cluster for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## interface (Chassis Cluster)

**Syntax** interface reth*X.logical-unit-number* secondary-ip-address *IP–address*;

**Hierarchy Level** [edit chassis cluster redundancy-group *group-number* ip-monitoring family *family-name IP–address*]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** Specify the redundant Ethernet interface, including its logical-unit-number, through which the monitored IP address must be reachable. The specified redundant Ethernet interface can be in any redundancy group. Likewise specify a secondary IP address to be used as a ping source for monitoring the IP address through the secondary node's redundant Ethernet interface link.

**Options**

- reth*X.logical-unit-number*—Redundant Ethernet interface through which the monitored IP address must be reachable. You must specify the redundant Ethernet interface logical-unit-number. Note that you must also configure a secondary ping source IP address (see below).

  **Range:** reth0.*logical-unit-number* through reth128.*logical-unit-number* (device dependent)

  NOTE: If the redundant Ethernet interface belongs to a VPN routing and forwarding (VRF) routing instance type, then the IP Monitoring feature will not work.

- secondary-ip-address *IP–address*—Specify the IP address that will be used as the source IP address of ping packets for IP monitoring from the secondary child link of the redundant Ethernet interface. An IP address for sourcing the ping packets on the primary link of the redundant Ethernet interface must be configured before you can configure secondary-ip-address. For legacy support reasons, monitoring on an IP address without identifying a redundant Ethernet interface and without configuring a secondary ping source IP address is permitted but not recommended.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Chassis Cluster for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## interface-monitor

**Syntax**

```
interface-monitor interface-name {
  weight number;
}
```

**Hierarchy Level** [edit **chassis cluster redundancy-group** *group-number* ]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Specify a redundancy group interface to be monitored for failover and the relative weight of the interface.

**Options** ***interface-name*** —Name of the physical interface to monitor.

The remaining statement is explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Chassis Cluster for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## ip-monitoring

**Syntax**

```
ip-monitoring {
    global-threshold number;
    global-weight number;
    retry-count count;
    retry-interval interval;
    family {
        inet {
            IP-address {
                weight number;
                interface rethX.logical-unit-number secondary-ip-address IP-address;
            }
        }
    }
}
```

**Hierarchy Level** [edit chassis cluster redundancy-group *group-number* ]

**Release Information** Statement updated in Release 10.1 of Junos OS.

**Description** Specify a global IP address monitoring threshold and weight, and the interval between pings (**retry-interval**) and the number of consecutive ping failures (**retry-count**) permitted before an IP address is considered unreachable for all IP addresses monitored by the redundancy group. Also specify IP addresses, a monitoring weight, a redundant Ethernet interface number, and a secondary IP monitoring ping source for each IP address, for the redundancy group to monitor.

**Options** **family *family-name IP address***—The address to be continually monitored for reachability.



NOTE: All monitored object failures, including IP monitoring, are deducted from the redundancy group threshold priority. Other monitored objects include interface monitor, SPU monitor, cold-sync monitor, and NPC monitor (on supported platforms).

The remaining statement is explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- IP Monitoring
- Chassis Cluster for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## network-management

**Syntax**
```
network-management {
  cluster-master;
}
```

**Hierarchy Level** [edit chassis cluster]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Define parameters for network management. To manage an SRX Series Services Gateway cluster through a non-fxp0 interface, use this command to define the node as a virtual chassis in NSM. This command establishes a single DMI connection from the primary node to the NSM server. This connection is used to manage both nodes in the cluster. Note that the non-fxp0 interface (regardless of which node it is present on) is always controlled by the primary node in the cluster. The output of a *<get-system-information>* RPC returns a *<chassis-cluster>* tag in all SRX Series devices. When NSM receives this tag, it models SRX Series clusters as devices with autonomous control-planes.

**Options** **cluster-master**—Enable in-band management on the primary cluster node through NSM.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Chassis Cluster for Security Devices

## node (Chassis Cluster)

**Syntax** **node** *node-number* ;

**Hierarchy Level** [edit chassis cluster]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Identify the device in a chassis cluster. The node 0 device in the cluster has the chassis ID 1, and the node 1 device in the cluster has the chassis ID 2.

**Options** ***node-number*** —Cluster node number.
**Range:** 0 through 1

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Chassis Cluster for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## node (Chassis Cluster Redundancy Group)

**Syntax**

```
node node-number {
  priority priority-number ;
}
```

**Hierarchy Level** [edit **chassis cluster redundancy-group** *group-number* ]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Identify each cluster node in a redundancy group and set its relative priority for mastership.

**Options** *node-number* —Cluster node number, set with the **chassis cluster node** *node-number* statement.

The remaining statement is explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Chassis Cluster for Security Devices

## pic-mode (Chassis G.SHDSL)

**Syntax** pic-mode

**Hierarchy Level** [set chassis fpc *fpc slot-number* pic *pic slot-number* shdsl]

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Specify the operating mode for the G.SHDSL interface.

**Options**
- 1-port-atm — 8-wire mode
- 2-port-atm —4-wire mode
- 4-port-atm —2-wire mode



NOTE: When chassis clustering is enabled, it is necessary to indicate in the command which node is being configured. In such circumstances, the **edit chassis fpc** command becomes **edit chassis node** *node-id***fpc**.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- DSL Interfaces


Copyright © 2013, Juniper Networks, Inc.

## pic-mode (Chassis T1 Mode)

**Syntax** pic-mode (clear-channel);

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number* ethernet]

**Release Information** Statement added in Release 10.2 of Junos OS.

**Description** Configure normal T1 mode or channelized T1 mode.

**Options**
- **clear-channel**—(default) Normal T1 mode.
- **ct1**—Channelized T1 mode.



NOTE: When chassis clustering is enabled, it is necessary to indicate in the command which node is being configured. In such circumstances, the **edit chassis fpc** command becomes **edit chassis node** *node-id* **fpc**.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices
- Feature Support Reference for SRX Series and J Series Devices

Copyright © 2013, Juniper Networks, Inc.

## pic-mode (Chassis uPIM)

**Syntax** pic-mode (enhanced-switching | routing | switching);

**Hierarchy Level** [edit chassis fpc *slot-number* pic *pic-number* ethernet]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Set the mode to configure the uPIMs.

**Options**

- **enhanced-switching**—Enhanced switching mode of operation. Each port of the uPIMs can be configured for switching or routing mode.

  NOTE: Only one enhanced-switching mode uPIM per chassis is supported currently.

- **routing**—Routing mode of operation. All ports of the uPIMs are in routing mode. Routing mode is the default setting.
- **switching**—Switching mode of operation. All ports of the uPIMs are in switching mode.

  NOTE: When chassis clustering is enabled, it is necessary to indicate in the command which node is being configured. In such circumstances, the edit chassis fpc command becomes edit chassis node *node-id* fpc.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## preempt (Chassis Cluster)

**Syntax** preempt;

**Hierarchy Level** [edit chassis cluster redundancy-group *group-number* ]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Enable chassis cluster node preemption within a redundancy group. If **preempt** is added to a redundancy group configuration, the device with the higher priority in the group can initiate a failover to become master. By default, preemption is disabled.

Initiating a failover with the **request chassis cluster failover node** or **request chassis cluster failover redundancy-group** command overrides the priority settings and preemption.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Chassis Cluster for Security Devices

## priority (Chassis Cluster)

**Syntax** **priority** *priority-number* ;

**Hierarchy Level** [edit **chassis cluster redundancy-group** *group-number* **node** *node-number* ]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Define the priority of a node (device) in a redundancy group. Initiating a failover with the **request chassis cluster failover node** or **request chassis cluster failover redundancy-group** command overrides the priority settings.

**Options** *priority-number* —Priority value of the node. The eligible node with the highest priority is elected master.
**Range:** 1 through 254

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Chassis Cluster for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## redundancy-group (Chassis Cluster)

**Syntax**

```
redundancy-group group-number {
  gratuitous-arp-count number ;
  hold-down-interval number ;
  interface-monitor interface {
    weight number ;
  }
  ip-monitoring {
    global-weight number;
    global-threshold number;
    retry-count count;
    retry-interval interval;
    family {
          inet {
            IP-address {
                weight number;
                interface rethX.logical-unit-number secondary-ip-address IP-address;
              }
          }
    }
  }
  node node-number {
    priority priority-number ;
  }
  preempt;
}
```

**Hierarchy Level** [edit chassis cluster]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Define a redundancy group. Except for redundancy group 0, a redundancy group is a logical interface consisting of two physical Ethernet interfaces, one on each chassis. One interface is active, and the other is on standby. When the active interface fails, the standby interface becomes active. The logical interface is called a redundant Ethernet interface (**reth**).

Redundancy group 0 consists of the two Routing Engines in the chassis cluster and controls which Routing Engine is primary. You must define redundancy group 0 in the chassis cluster configuration.

**Options** *group-number* —Redundancy group identification number.

**Range:** 0 through 128



NOTE: The maximum number of redundancy groups is equal to the number of redundant Ethernet interfaces that you configure.

The remaining statements are explained separately.


Copyright © 2013, Juniper Networks, Inc.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- IP Monitoring
- Chassis Cluster for Security Devices

## reth-count (Chassis Cluster)

**Syntax**
reth-count *number*;

**Hierarchy Level**
[edit **chassis cluster**]

**Release Information**
Statement introduced in Release 9.0 of Junos OS.

**Description**
Specify the number of redundant Ethernet (**reth**) interfaces allowed in the chassis cluster. Note that the number of **reth** interfaces configured determines the number of redundancy groups that can be configured.

**Options**
*number* —Number of redundant Ethernet interfaces allowed.
**Range:** 1 through 128
**Default:** 0

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Chassis Cluster for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## retry-count (Chassis Cluster)

**Syntax** retry-count *count*;

**Hierarchy Level** [edit chassis cluster redundancy-group *group-number* ip-monitoring ]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** Specify the number of consecutive ping attempts that must fail before an IP address monitored by the redundancy group is declared unreachable. (See **retry-interval** for a related redundancy group IP address monitoring variable.)

**Options** *count*—Number of consecutive ping attempt failures before a monitored IP address is declared unreachable.

**Range:** 1 through 15

**Default:** 5

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Chassis Cluster for Security Devices

## retry-interval (Chassis Cluster)

**Syntax** retry-interval *interval*;

**Hierarchy Level** [edit chassis cluster redundancy-group *group-number* ip-monitoring ]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** Specify the ping packet send frequency (in seconds) for each IP address monitored by the redundancy group. (See **retry-count** for a related IP address monitoring configuration variable.)

**Options** *interval*—Pause time between each ping sent to each IP address monitored by the redundancy group.

**Range:** 1 to 30 seconds

**Default:** 1 second

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- IP Monitoring
- Chassis Cluster for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## services-offload

**Syntax** services-offload

**Hierarchy Level** [edit chassis fpc *fpc-slot-number* pic *pic-slot-number*]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Enables the services-offload mode on the selected network processor.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Flow-Based Processing for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Chassis Cluster)

**Syntax**

```
traceoptions {
  file filename {
    <files number >;
    <match regular-expression >;
    <size maximum-file-size >;
    <world-readable | no-world-readable>;
  }
  flag {
    all;
    configuration;
    routing-socket;
    snmp;
  }
}
```

**Hierarchy Level** [edit chassis cluster]

**Release Information** Statement modified in Release 9.5 of Junos OS.

**Description** Define chassis cluster redundancy process tracing operations.

**Options**

- **file** *filename* —Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.
- **files** *number* —(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed to *trace-file* **.0,** then *trace-file.1* **,** and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.
- If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

  **Range:** 2 through 1000 files

  **Default:** 10 files

- **match** *regular-expression* —(Optional) Refine the output to include lines that contain the regular expression.
- **size** *maximum-file-size* —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file* **.0**. When the **trace-file** again reaches its maximum size, *trace-file* **.0** is renamed *trace-file* **.1** and *trace-file* is renamed *trace-file* **.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
- If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

  **Syntax:** *x* **k** to specify KB, *x* **m** to specify MB, or *x* **g** to specify GB

  **Range:** 0 KB through 1 GB

  **Default:** 128 KB


Copyright © 2013, Juniper Networks, Inc.

- **world-readable | no-world-readable**—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag**—Trace operation or operations to perform on chassis cluster redundancy processes. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace all the events
    - **configuration**—Trace configuration events
    - **routing-socket**—Trace logging of rtsock activity
    - **snmp**—Trace SNMP events

**Required Privilege Level**
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**
- Chassis Cluster for Security Devices

## tunnel-queuing

**Syntax**
```
tunnel-queuing;
```

**Hierarchy Level**
[edit chassis fpc *slot-number* pic *pic-number* ]

**Release Information**
Statement modified in Release 9.0 of Junos OS.

**Description**
Enable class-of-service (CoS) queuing for generic routing encapsulation (GRE) and IP-IP tunnels.



NOTE: The **tunnel-queuing** option is not supported in chassis cluster mode.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- CoS Virtual Channels and Tunnels

Copyright © 2013, Juniper Networks, Inc.

## weight

**Syntax** weight *number*;

**Hierarchy Level** [edit chassis cluster **redundancy-group** *group-number* interface-monitor *interface* ]
[edit chassis cluster **redundancy-group** *group-number* ip-monitoring *IP–address*]

**Release Information** Statement modified in Release 10.1 of Junos OS.

**Description** Specify the relative importance of the object to the operation of the redundancy group. This statement is primarily used with interface monitoring and IP address monitoring objects. The failure of an object—such as an interface—with a greater weight brings the group closer to failover. Every monitored object is assigned a weight.

- interface-monitor objects—If the object fails, its weight is deducted from the threshold of its redundancy group;
- ip-monitoring objects—If a monitored IP address becomes unreachable for any reason, the weight assigned to that monitored IP address is deducted from the redundancy group's global-threshold for IP address monitoring.

Every redundancy group has a default threshold of 255. If the threshold reaches 0, a failover is triggered. Failover is triggered even if the redundancy group is in manual failover mode and preemption is not enabled.

**Options** *number* —Weight assigned to the interface or monitored IP address. A higher weight value indicates a greater importance.

**Range:** 0 through 255

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Chassis Cluster for Security Devices


Copyright © 2013, Juniper Networks, Inc.

CHAPTER 6

# Class-of-Service Hierarchy and Statements

This section contains the following topics:


- Class-of-Service Configuration Statement Hierarchy on page 109


## Class-of-Service Configuration Statement Hierarchy

Use the statements in the **class-of-service** configuration hierarchy to configure class-of-services (CoS) features.

```
class-of-service {
  adaptive-shapers {
    adaptive-shaper-name  {
      trigger  type  shaping-rate (percent  percent  |  rate );
    }
  }
  application-traffic-control {
    rate-limiters {
      rate-limiters-name {
        bandwidth-limit value-in-bps;
        burst-size-limit value-in-bytes;
      }
    }
    rule-sets {
      rule-set-name {
        rule rule-name {
          match {
            application application-names;
            application-any;
            application-group application-group-names;
            application-known;
            application-unknown;
          }
          then {
            dscp-code-point dscp-value;
            forwarding-class forwarding-class-name;
            log;
            loss-priority [ high | medium-high | medium-low | low ];
            rate-limit {
              client-to-server rate-limiter-name;
```

Copyright © 2013, Juniper Networks, Inc.

```
                server-to-client rate-limiter-name;
            }
          }
        }
      }
    }
}
classifiers {
  type  classifier-name  {
    forwarding-class class-name  {
      loss-priority (low | high) code-points [ alias  |  bits ];
    }
    import ( classifier-name  | default);
  }
}
code-point-aliases {
  (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence) {
    alias-name  bits;
  }
}
drop-profiles {
  profile-name  {
    fill-level percentage drop-probability percentage;
    interpolate {
      drop-probability value;
      fill-level value;
    }
  }
}
forwarding-classes {
  class queue-num queue-number priority (high | low);
  queue queue-number class-name priority (high | low) < policing-priority (premium |
    normal) > < spu-priority (high | low) >;
}
forwarding-policy {
  class class-name  {
    classification-override {
      forwarding-class class-name;
    }
  }
  next-hop-map map-name  {
    forwarding-class class-name  {
      lsp-next-hop [ lsp-regular-expression ];
      next-hop [ next-hop-name ];
      non-lsp-next-hop [ lsp-regular-expression ];
    }
  }
}
fragmentation-maps {
  map-name  {
    forwarding-class class-name  {
      drop-timeout milliseconds;
      fragment-threshold bytes;
      multilink-class number;
      no-fragmentation;
    }
```


Copyright © 2013, Juniper Networks, Inc.

```
    }
  }
  host-outbound-traffic {
    dscp-code-point value;
    forwarding-class class-name;
  }
  interfaces {
    interface-name {
      input-scheduler-map map-name ;
      input-shaping-rate rate ;
      scheduler-map map-name ;
      scheduler-map-chassis map-name ;
      shaping-rate rate;
      unit logical-unit-number {
        adaptive-shaper adaptive-shaper-name ;
        classifiers {
          (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence)
          ( classifier-name | default);
        }
        forwarding-class class-name ;
        fragmentation-map map-name;
        input-scheduler-map map-name;
        input-shaping-rate (percent percentage | rate );
        input-traffic-control-profile profiler-name shared-instance instance-name ;
        loss-priority-maps {
          default;
          map-name;
        }
        output-traffic-control-profile profile-name shared-instance instance-name ;
        rewrite-rules {
          dscp ( rewrite-name | default);
          dscp-ipv6 ( rewrite-name | default);
          exp ( rewrite-name | default) protocol protocol-types ;
          frame-relay-de ( rewrite-name | default);
          ieee-802.1 ( rewrite-name | default) vlan-tag (outer | outer-and-inner);
          ieee-802.1ad ( rewrite-name | default) vlan-tag (outer | outer-and-inner);
          inet-precedence ( rewrite-name | default);
        }
        scheduler-map map-name;
        shaping-rate rate ;
        virtual-channel-group group-name;
      }
    }
  }
  loss-priority-maps {
    frame-relay-de ( map-name | default) {
      loss-priority level code-points [ values ];
    }
  }
  rewrite-rules {
    type rewrite-name {
      forwarding-class class-name {
        loss-priority level code-point [ aliases ] [ 6-bit-patterns ];
      }
      import ( rewrite-name | default);
    }
```

```
    }
    scheduler-maps {
      map-name {
        forwarding-class class-name scheduler scheduler-name;
      }
    }
    schedulers {
      scheduler-name {
        buffer-size (percent percentage | remainder percent | temporal microseconds );
        drop-profile-map {
          loss-priority (any | high | low | medium-high | medium-low);
          protocol (any | non-tcp | tcp);
        }
        priority (high | low | medium-high | medium-low | strict-high);
        shaping-rate (percent percent age | rate );
        transmit-rate (percent percentage | rate | remainder percent) <exact | rate-limit>;
      }
    }
    traceoptions {
      flag flag {
        all;
        asynch;
        hardware-database;
        init;
        parse;
        process;
        restart;
        route-socket;
        show;
        snmp;
        util;
      }
    }
    traffic-control-profiles profile-name {
      delay-buffer-rate (percent percent | rate );
      guaranteed-rate (percent percent | rate );
      scheduler-map map-name;
      shaping-rate (percent percent | rate );
    }
    virtual-channel-groups {
      virtual-channel-group-name {
        virtual-channel-name {
          default;
          scheduler-map map-name;
          shaping-rate (percent percent | rate );
        }
      }
    }
    virtual-channels {
      virtual-channel-name;
    }
  }
```

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices


Copyright © 2013, Juniper Networks, Inc.

- Application Quality of Service
- IDP Class of Service Action for Security Devices
- CoS Virtual Channels and Tunnels
- CoS and Hierarchical Schedulers
- Link Services and Special Interfaces
- Class of Service for Security Devices

## adaptive-shaper

**Syntax** adaptive-shaper *adaptive-shaper-name*;

**Hierarchy Level** [edit class-of-service interfaces *interface-name* unit *logical-unit-number*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Assign an adaptive shaper to an interface.

Adaptive shapers enable bandwidth limits on Frame Relay interfaces when the device receives frames containing the backward explicit congestion notification (BECN) bit.

**Options** ***adaptive-shaper-name***—Name of the adaptive shaper.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- adaptive-shapers on page 114
- CoS Components
- CoS Virtual Channels and Tunnels

Copyright © 2013, Juniper Networks, Inc.

## adaptive-shapers

**Syntax**

```
adaptive-shapers {
  adaptive-shaper-name {
    trigger type shaping-rate (percent percentage | rate);
  }
}
```

**Hierarchy Level** [edit class-of-service]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Define trigger types and associated rates. Adaptive shapers enable bandwidth limits on Frame Relay interfaces when the Services Router receives frames containing the backward explicit congestion notification (BECN) bit.

**Options** ***adaptive-shaper-name***—Name of the adaptive shaper.

The remaining statements are explained separately.

**Required Privilege Level** interface— view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- adaptive-shaper on page 113
- CoS Components
- CoS Virtual Channels and Tunnels

 Copyright © 2013, Juniper Networks, Inc.

## application-traffic-control

**Syntax**

```
application-traffic-control {
  rate-limiters {
    rate-limiter-name {
      bandwidth-limit value-in-kbps;
      burst-size-limit value-in-bytes;
    }
  }
  rule-sets {
    ruleset-name {
      rule rule-name {
        match {
          application application-name1;
          application-any;
          application-group application-group-name;
          application-known;
          application-unknown;
        }
        then {
          dscp-code-point dscp-value;
          forwarding-class forwarding-class-name;
          log;
          loss-priority [ high | medium-high | medium-low | low ];
          rate-limit {
            client-to-server rate-limiter-name;
            server-to-client rate-limiter-name;
          }
        }
      }
    }
  }
}
```

**Hierarchy Level** [edit class-of-service]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Mark DSCP values for outgoing packets or apply rate limits based on the specified Layer 7 application types.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Quality of Service
- CoS Components
- CoS Virtual Channels and Tunnels

Copyright © 2013, Juniper Networks, Inc.

## classifiers (CoS)

**Syntax**

```
classifiers {
  (dscp | dscp-ipv6 | exp | ieee-802.1 | ieee-802.1ad | inet-precedence) classifier-name {
    import (default | user-defined;
    forwarding-class class-name {
      loss-priority level code-points (alias | bits);
    }
  }
}
```

**Hierarchy Level** [edit class-of-service]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure a user-defined behavior aggregate (BA) classifier.

**Options**

- *classifier-name*—User-defined name for the classifier.
- import (default | *user-defined*)—Specify the template to use to map any code points not explicitly mapped in this configuration. For example, if the classifier is of type **dscp** and you specify **import default**, code points you do not map in your configuration will use the predefined DSCP default mapping; if you specify **import mymap**, for example, code points not mapped in the forwarding-class configuration would use the mappings in a user-defined classifier named **mymap**.
- forwarding-class *class-name*—Specify the name of the forwarding class. You can use the default forwarding class names or define new ones.
- loss-priority *level*—Specify a loss priority for this forwarding class: **high**, **low**, **medium-high**, **medium-low**.
- code-points (*alias* | *bits*)—Specify a code-point alias or the code points that map to this forwarding class.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- CoS Components
- IDP Class of Service Action for Security Devices
- CoS Virtual Channels and Tunnels
- Link Services and Special Interfaces
- Class of Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## code-points

**Syntax** code-points ([ *aliases* ] | [ *bit-patterns* ]);

**Hierarchy Level** [edit class-of-service classifiers *type classifier-name* forwarding-class *class-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Specify one or more DSCP code-point aliases or bit sets for association with a forwarding class.

**Options** ***aliases***—Name of the DSCP alias.

***bit-patterns***—Value of the code-point bits, in six-bit binary form.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Overview of BA Classifier Types
- Example: Configuring CoS for a PBB Network on MX Series Routers
- CoS Virtual Channels and Tunnels
- CoS Components

Copyright © 2013, Juniper Networks, Inc.

## default (CoS)

**Syntax** default;

**Hierarchy Level** [edit class-of-service virtual-channel-groups *group-name virtual-channel-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the default channel. You must configure one of the virtual channels in the group to be the default. Any traffic not explicitly directed to a virtual channel is transmitted by way of this default.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- scheduler-map (CoS Virtual Channels) on page 133
- shaping-rate (CoS Virtual Channels) on page 136
- virtual-channel-group (CoS Interfaces) on page 138
- virtual-channel-groups on page 139
- virtual-channels on page 137
- CoS Components
- CoS Virtual Channels and Tunnels


Copyright © 2013, Juniper Networks, Inc.

## forwarding-classes (CoS)

**Syntax**

```
forwarding-classes {
  class class-name queue-num queue-number< priority (high | low) > <spu-priority (high |
    low)>; queue queue-number < priority (high | low) >;
}
```

**Hierarchy Level** [edit class-of-service]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Statement updated in Release 11.4 of Junos OS. **spu-priority** option introduced in Release 11.4R2 of Junos OS.

**Description** Configure forwarding classes and assign queue numbers.

**Options**

- *class-name*—Display the forwarding class name assigned to the internal queue number.

  NOTE: AppQoS forwarding classes must be different from those defined for interface-based rewriters.

- **policing-priority**—Layer 2 policing. One forwarding class can be configured as **premium** and others are configured as **normal**.
- **priority**—Fabric priority value:
  - **high**—Forwarding class's fabric queuing has high priority.
  - **low**—Forwarding class's fabric queuing has low priority.
- *queue-number*—Specify the internal queue number to which a forwarding class is assigned.
- **spu-priority**—Services Processing Unit (SPU) priority queue, either **high** or **low**.

  NOTE: The spu-priority option is only supported on SRX1400, SRX3000 line, and SRX5000 line devices.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- CoS Components
- CoS Virtual Channels and Tunnels
- Application Quality of Service

Copyright © 2013, Juniper Networks, Inc.

- IDP Class of Service Action for Security Devices

## frame-relay-de (CoS Interfaces)

**Syntax** frame-relay-de (*name* | default);

**Hierarchy Level** [edit class-of-service interfaces *interface-name* unit *logical-unit-number* loss-priority-maps], [edit class-of-service interfaces *interface-name* unit *logical-unit-number* rewrite-rules]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Assign the loss priority map or the rewrite rule to a logical interface.

**Options**

- **default**—Apply default loss priority map or default rewrite rule. The default loss priority map contains the following settings:

  ```
  loss-priority low code-point 0;
  loss-priority high code-point 1;
  ```

- The default rewrite rule contains the following settings:

  ```
  loss-priority low code-point 0;
  loss-priority medium-low code-point 0;
  loss-priority medium-high code-point 1;
  loss-priority high code-point 1;
  ```

- ***name***—Name of loss priority map or rewrite rule to be applied.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- CoS Components
- CoS Virtual Channels and Tunnels


Copyright © 2013, Juniper Networks, Inc.

## frame-relay-de (CoS Loss Priority)

**Syntax**

```
frame-relay-de map-name {
  loss-priority level code-point (0 | 1);
}
```

**Hierarchy Level** [edit class-of-service loss-priority-maps ]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Define a Frame Relay discard-eligible bit loss-priority map.

**Options**

- ***level***—Level of loss priority to be applied based on the specified CoS values. The level can be **low**, **medium-low**, **medium-high**, or **high**.
- ***map-name***—Name of the loss-priority map.

  The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- CoS Components
- CoS Virtual Channels and Tunnels

Copyright © 2013, Juniper Networks, Inc.

## frame-relay-de (CoS Rewrite Rule)

**Syntax**

```
frame-relay-de rewrite-name {
  forwarding-class class-name {
    loss-priority level code-point (0 | 1);
  }
  import (default | rewrite-name);
}
```

**Hierarchy Level** [edit class-of-service rewrite-rules]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Define a Frame Relay discard-eligible bit rewrite rule.

**Options**

- ***level***—Level of loss priority on which to base the rewrite rule. The loss priority level can be **low**, **medium-low**, **medium-high**, or **high**.
- ***rewrite-name***—Name of a rewrite-rules mapping configured at the **[edit class-of-service rewrite-rules]** hierarchy level.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- CoS Components
- CoS Virtual Channels and Tunnels


Copyright © 2013, Juniper Networks, Inc.

## interfaces (CoS)

**Syntax**

```
interfaces {
  interface-name {
    input-scheduler-map map-name ;
    input-shaping-rate rate ;
    scheduler-map map-name ;
    scheduler-map-chassis map-name ;
    shaping-rate rate ;
    unit logical-unit-number {
      adaptive-shaper adaptive-shaper-name ;
      classifiers {
        (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence)
        ( classifier-name | default);
      }
      forwarding-class class-name ;
      fragmentation-map map-name ;
      input-schedular-map map-name ;
      input-shaping-rate (percent percentage | rate );
      input-traffic-control-profile profiler-name shared-instance instance-name ;
      loss-priority-maps {
        default;
        map-name ;
      }
      output-traffic-control-profile profile-name shared-instance instance-name ;
      rewrite-rules {
        dscp ( rewrite-name | default);
        dscp-ipv6 ( rewrite-name | default);
        exp ( rewrite-name | default) protocol protocol-types ;
        frame-relay-de ( rewrite-name | default);
        ieee-802.1 ( rewrite-name | default) vlan-tag (outer | outer-and-inner);
        ieee-802.1ad ( rewrite-name | default) vlan-tag (outer | outer-and-inner);
        inet-precedence ( rewrite-name | default);
      }
      scheduler-map map-name ;
      shaping-rate rate ;
      virtual-channel-group group-name ;
    }
  }
}
```

**Hierarchy Level** [edit class-of-service interface *interface-name* unit *number*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Associate the class-of-service configuration elements with an interface.

**Options** interface *interface-name* unit *number*—The user-specified interface name and unit number.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Copyright © 2013, Juniper Networks, Inc.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- CoS Components
- CoS Virtual Channels and Tunnels
- IDP Class of Service Action for Security Devices

## loss-priority (CoS Loss Priority)

**Syntax** loss-priority *level* code-points[ *values* ];

**Hierarchy Level** [edit class-of-service loss-priority-maps frame-relay-de *map-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Map CoS values to a loss priority.

**Options** ***level*** can be one of the following:

- **high**—Packet has high loss priority.
- **medium-high**—Packet has medium-high loss priority.
- **medium-low**—Packet has medium-low loss priority.
- **low**—Packet has low loss priority.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- CoS Components
- CoS Virtual Channels and Tunnels
- Class of Service for Security Devices
- Link Services and Special Interfaces


Copyright © 2013, Juniper Networks, Inc.

## loss-priority (CoS Rewrite Rules)

**Syntax** loss-priority *level*;

**Hierarchy Level** [edit class-of-service rewrite-rules *type rewrite-name* forwarding-class *class-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify a loss priority to which to apply a rewrite rule. The rewrite rule sets the code-point aliases and bit patterns for a specific forwarding class and packet loss priority (PLP). The inputs for the map are the forwarding class and the PLP. The output of the map is the code-point alias or bit pattern.

**Options** ***level*** can be one of the following:

- **high**—The rewrite rule applies to packets with high loss priority.
- **low**—The rewrite rule applies to packets with low loss priority.
- **medium-high**—The rewrite rule applies to packets with medium-high loss priority.
- **medium-low**—The rewrite rule applies to packets with medium-low loss priority.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- CoS Components
- CoS Virtual Channels and Tunnels
- IDP Class of Service Action for Security Devices
- Class of Service for Security Devices
- Link Services and Special Interfaces

Copyright © 2013, Juniper Networks, Inc.

## loss-priority-maps (CoS Interfaces)

**Syntax**

```
loss-priority-maps {
  frame-relay-de (map-name | default);
}
```

**Hierarchy Level** [edit class-of-service interfaces *interface-name* unit *logical-unit-number*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Assign the loss priority map to a logical interface.

**Options**

- **default**—Apply default loss priority map. The default map contains the following:

  ```
  loss-priority low code-point 0;
  loss-priority high code-point 1;
  ```

- ***map-name***—Name of loss priority map to be applied.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- CoS Components
- CoS Virtual Channels and Tunnels
- Class of Service for Security Devices
- Link Services and Special Interfaces


Copyright © 2013, Juniper Networks, Inc.

## loss-priority-maps (CoS)

**Syntax**

```
loss-priority-maps {
  frame-relay-de map-name {
    loss-priority level code-points [ values ];
  }
}
```

**Hierarchy Level** [edit class-of-service]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Map the loss priority of incoming packets based on CoS values.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- CoS Components
- CoS Virtual Channels and Tunnels
- Class of Service for Security Devices
- Link Services and Special Interfaces

Copyright © 2013, Juniper Networks, Inc.

## rate-limiters

**Syntax**

```
rate-limiters {
  rate-limiter-name {
    bandwidth-limit value-in-kbps;
    burst-size-limit value-in-bytes;
  }
}
```

**Hierarchy Level** [edit class-of-service application-traffic-control]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Share the available bandwidth and burst size of a device's PICs by defining rate limiter profiles and applying them in AppQoS rules.

**Options**

- ***rate-limiter-name***—Name of the rate limiter. It is applied in AppQoS rules to share device resources based on quality of service requirements.

  The combination of rate limiting parameters, namely bandwidth- limit and burst-size-limit rate limit, make up the rate limiter profile. A maximum of 16 profiles are allowed per device. The same profile can be used by multiple rate limiters. For example, a profile with a bandwidth-limit of 200 Kbps and a burst-limit of 130,000 bytes, could be used in several rate limiters.

  A maximum of 1000 rate limiters can be created. Rate limiters are defined for the device, and are assigned in rules in a rule set. A single rate limiter can be used multiple times within the same rule set. However, the rate limiter cannot be used in another rule set.

- **bandwidth-limit *value-in-Kbps***—Maximum number of kilobits to be transmitted per second for this rate limiter. Up to 2 GB of bandwidth can be provisioned among multiple rate limiters to share the resource proportionally.

- **burst-size-limit *value-in-bytes***—Maximum number of bytes to be transferred in a single burst or time-slice. This limit ensures that a high-priority transmission does not keep a lower priority transmission from transmitting.



NOTE: The number of bandwidth-limit and burst-size-limit combinations cannot exceed 16.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Quality of Service
- CoS Components
- CoS Virtual Channels and Tunnels


Copyright © 2013, Juniper Networks, Inc.

## rewrite-rules (CoS)

**Syntax**

```
rewrite-rules {
  type rewrite-name{
    import (rewrite-name | default);
    forwarding-class class-name {
      loss-priority level code-point [ aliases ] [ 6–bit-patterns ];
    }
  }
}
```

**Hierarchy Level** [edit class-of-service]

**Release Information** Statement introduced in Release 8.5 of Junos OS. **ieee-802.1ad** option introduced in 9.2 of Junos OS.

**Description** Specify a rewrite-rules mapping for the traffic that passes through all queues on the interface.

**Options**

- ***rewrite-name***—Name of a **rewrite-rules** mapping.
- ***type***—Traffic type.

  **Values:** **dscp**, **dscp-ipv6**, **exp**, **frame-relay-de** (J Series only), **ieee-802.1**, **ieee-802.1ad**, **inet-precedence**

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- rewrite-rules (CoS Interfaces) on page 130
- CoS Components
- CoS Virtual Channels and Tunnels

Copyright © 2013, Juniper Networks, Inc.

## rewrite-rules (CoS Interfaces)

**Syntax**

```
rewrite-rules {
  dscp (rewrite-name | default);
  dscp-ipv6 (rewrite-name | default);
  exp (rewrite-name | default) protocol protocol-types;
  exp-push-push-push default;
  exp-swap-push-push default;
  ieee-802.1 (rewrite-name | default) vlan-tag (outer | outer-and-inner);
  inet-precedence (rewrite-name | default);
}
```

**Hierarchy Level** [edit class-of-service interfaces *interface-name* unit *logical-unit-number*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Associate a rewrite-rules configuration or default mapping with a specific interface.

**Options**

- ***rewrite-name***—Name of a **rewrite-rules** mapping configured at the **[edit class-of-service rewrite-rules]** hierarchy level.
- **default**—The default mapping.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- rewrite-rules (CoS) on page 129
- CoS Components
- CoS Virtual Channels and Tunnels
- IDP Class of Service Action for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## rule-sets (CoS AppQoS)

**Syntax**

```
rule-sets {
  rule-set-name {
    rule rule-name {
      match {
        application application-name;
        application-any;
        application-group application-group-name;
        application-known;
        application-unknown;
      }
      then {
        dscp-code-point dscp-value ;
        forwarding-class forwarding-class-name;
        log;
        loss-priority [ high | medium-high | medium-low | low ];
        rate-limit {
          client-to-server rate-limiter-name;
          server-to-client rate-limiter-name;
        }
      }
    }
  }
}
```

**Hierarchy Level** [edit class-of-service application-traffic-control]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Defines AppQoS rule sets and the rules that establish priorities based on quality of service requirements for the associated applications. AppQoS rules can be included in policy statements to implement application-aware quality of service control.

**Options**

- ***rule-set-name***—Name used to refer to a collection of AppQoS rules.
- **rule *rule-name***—Name applied to the match criteria and resulting actions that control the quality of service provided to any matching applications.
- **application *application-name***—Name of the application to be used as match criteria for the rule.
- **application-any** —Any application encountering this rule. Note that when you use this specification, all application matching ends. Any application rule following this one will never be encountered.
- **application-group *application-group-name***—Group of applications to be used as match criteria for the rule. Both applications and application groups can be match criteria for a single rule.
- **application-known**—Match criteria specifying any session that is identified, but its corresponding application is not specified.
- **application-unknown**—Match criteria specifying any session that is not identified.

Copyright © 2013, Juniper Networks, Inc.

- **forwarding-class** ***forwarding-class-name***—The AppQoS class with which matching applications will be marked. This field identifies the rewriter that has marked the DSCP value . Therefore, the AppQoS forwarding class must be different from those used by IDP or firewall filters. With this class specified, firewall filter class will not overwrite the existing DSCP value.
- **dscp-code-point**—DSCP alias or bit map with which matching applications will be marked to establish the output queue. This value can be marked by rewriters from IDP, AppQoS, or a firewall filter. The forwarding-class value identifies which rewriter has re-marked the packet with the current DSCP value. If a packet triggers all three rewriters, IDP takes precedence over AppQoS, which takes precedence over a firewall filter.
- **loss-priority**—Loss priority with which matching applications will be marked. This value is used to determine the likelihood that a packet would be dropped when encountering congestion. A high loss priority means that there is an 80% chance of packet loss in congestion. Possible values are high, medium-high, medium-low and low.
- **rate-limit**—Rate limiters to be associated with client-to-server and with server-to-client traffic for this application. The rate limiter profile defines maximum speed and volume limits for matching applications.
- **log**—AppQoS event logging.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Quality of Service
- CoS Components
- CoS Virtual Channels and Tunnels


Copyright © 2013, Juniper Networks, Inc.

## scheduler-map (CoS Virtual Channels)

**Syntax** scheduler-map *map-name*;

**Hierarchy Level** [edit class-of-service virtual-channel-groups *group-name virtual-channel-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Apply a scheduler map to this virtual channel.

**Options** *map-name*—Name of the scheduler map.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- default (CoS) on page 118
- shaping-rate (CoS Virtual Channels) on page 136
- virtual-channel-group (CoS Interfaces) on page 138
- virtual-channel-groups on page 139
- virtual-channels on page 137
- CoS Components
- CoS Virtual Channels and Tunnels
- Link Services and Special Interfaces
- Class of Service for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## shaping-rate (CoS Adaptive Shapers)

**Syntax** shaping-rate (percent *percentage* | *rate*);

**Hierarchy Level** [edit class-of-service adaptive-shapers *adaptive-shaper-name* trigger *type*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Define the list of trigger types and associated rates.

**Options**

- **percent** ***percentage***—Shaping rate as a percentage of the available interface bandwidth.

  **Range:** 0 through 100 percent

- ***rate***—Peak rate, in bits per second (bps). You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

  **Range:** 3200 through 32,000,000,000 bps

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- trigger (CoS) on page 137
- CoS Components
- CoS Virtual Channels and Tunnels

 Copyright © 2013, Juniper Networks, Inc.

## shaping-rate (CoS Interfaces)

**Syntax** shaping-rate *rate*;

**Hierarchy Level** [edit class-of-service interfaces *interface-name*],
[edit class-of-service interfaces *interface-name* unit *logical-unit-number*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** For logical interfaces on which you configure packet scheduling, configure traffic shaping by specifying the amount of bandwidth to be allocated to the logical interface.



NOTE: The **shaping-rate** statement cannot be applied to a physical interface on J Series routing platforms.

Logical and physical interface traffic shaping is mutually exclusive. This means you can include the **shaping-rate** statement at the **[edit class-of-service interfaces interface *interface-name*]** hierarchy level or the **[edit class-of-service interfaces interface *interface-name* unit *logical-unit-number*]** hierarchy level, but not both.

Alternatively, you can configure a shaping rate for a logical interface and oversubscribe the physical interface by including the **shaping-rate** statement at the **[edit class-of-service traffic-control-profiles]** hierarchy level. With this configuration approach, you can independently control the delay-buffer rate. For more information on the delay-buffer rate, see the *Junos OS Class of Service Configuration Guide for Security Devices*.

**Default** If you do not include this statement at the **[edit class-of-service interfaces interface *interface-name* unit *logical-unit-number*]** hierarchy level, the default logical interface bandwidth is the average of unused bandwidth for the number of logical interfaces that require default bandwidth treatment. If you do not include this statement at the **[edit class-of-service interfaces interface *interface-name*]** hierarchy level, the default physical interface bandwidth is the average of unused bandwidth for the number of physical interfaces that require default bandwidth treatment.

**Options** ***rate***—Peak rate, in bits per second (bps). You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

**Range:** For logical interfaces, 1000 through 32,000,000,000 bps.

For physical interfaces, 1000 through 160,000,000,000 bps.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- CoS Components
- CoS Virtual Channels and Tunnels

Copyright © 2013, Juniper Networks, Inc.

- Link Services and Special Interfaces
- Class of Service for Security Devices

## shaping-rate (CoS Virtual Channels)

**Syntax** shaping-rate (percent *percentage* | *rate*);

**Hierarchy Level** [edit class-of-service virtual-channel-groups *group-name virtual-channel-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Define the shaping rates to be associated with the virtual channel.

**Options**

- **percent** ***percentage***—Shaping rate as a percentage of the available interface bandwidth.

  **Range:** 0 through 100 percent

- ***rate***—Peak rate, in bits per second (bps). You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

  **Range:** 3200 through 32,000,000,000 bps

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- default (CoS) on page 118
- scheduler-map (CoS Virtual Channels) on page 133
- virtual-channel-group (CoS Interfaces) on page 138
- virtual-channel-groups on page 139
- virtual-channels on page 137
- CoS Components
- CoS Virtual Channels and Tunnels


Copyright © 2013, Juniper Networks, Inc.

## trigger (CoS)

**Syntax** trigger *type* shaping-rate (percent *percentage* | *rate*);

**Hierarchy Level** [edit class-of-service adaptive-shapers *adaptive-shaper-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify a trigger type and its associated rate.

**Options** ***type***—The type of trigger. Currently, the trigger type can be **becn** only.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- shaping-rate (CoS Adaptive Shapers) on page 134
- CoS Components
- CoS Virtual Channels and Tunnels

## virtual-channels

**Syntax**

```
virtual-channels {
    virtual-channel-name;
}
```

**Hierarchy Level** [edit class-of-service]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify a list of virtual channels.

Each virtual channel has eight transmission queues.

**Options** ***virtual-channel-name***—Name of the virtual channel.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- default (CoS) on page 118
- scheduler-map (CoS Virtual Channels) on page 133
- shaping-rate (CoS Virtual Channels) on page 136
- virtual-channel-group (CoS Interfaces) on page 138
- virtual-channel-groups on page 139
- CoS Components
- CoS Virtual Channels and Tunnels

Copyright © 2013, Juniper Networks, Inc.

## virtual-channel-group (CoS Interfaces)

**Syntax** virtual-channel-group *group-name*;

**Hierarchy Level** [edit class-of-service interfaces *interface-name* unit *logical-unit-number*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Assign a virtual channel group to a logical interface.

If you apply a virtual channel group to multiple logical interfaces, separate queues are created on each of the interfaces. The same virtual channel names are used on all the interfaces. You can specify the scheduler and shaping rates in the virtual channels in percentages so that you can apply the same virtual channel group to logical interfaces with different available bandwidths.

**Options** ***group-name***—Name of the virtual channel group.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- default (CoS) on page 118
- scheduler-map (CoS Virtual Channels) on page 133
- shaping-rate (CoS Virtual Channels) on page 136
- virtual-channels on page 137
- virtual-channel-groups on page 139
- CoS Components
- CoS Virtual Channels and Tunnels


Copyright © 2013, Juniper Networks, Inc.

## virtual-channel-groups

**Syntax**

```
virtual-channel-groups {
  virtual-channel-group-name {
    virtual-channel-name {
      scheduler-map map-name;
      shaping-rate (percent percentage | rate);
      default;
    }
  }
}
```

**Hierarchy Level** [edit class-of-service]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Associate a virtual channel with a scheduler map and a shaping rate. Virtual channels and virtual channel groups enable you to direct traffic into a virtual channel and apply bandwidth limits to the channel.

**Options** *group-name*—Name of the virtual channel group.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- default (CoS) on page 118
- scheduler-map (CoS Virtual Channels) on page 133
- shaping-rate (CoS Virtual Channels) on page 136
- virtual-channel-group (CoS Interfaces) on page 138
- virtual-channels on page 137
- CoS Components
- CoS Virtual Channels and Tunnels

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 7

# Event-Options Hierarchy

This section contains the following topics:


- Event-Options Configuration Statement Hierarchy on page 141


## Event-Options Configuration Statement Hierarchy

Use the statements in the **event-options** configuration hierarchy to configure diagnostic event policies and actions associated with each policy.

```
event-options {
  destinations {
    destination-name {
      archive-sites {
        url password password ;
      }
      transfer-delay seconds ;
    }
  }
  event-script {
    file script-name ;
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
      flag flag ;
    }
  }
  generate-event event-name {
    time-interval seconds ;
    time-of-day hh : mm : ss ;
  }
  policy policy-name {
    attributes-match {
      event1 . attribute-name equals event2 . attribute-name ;
      event .attribute-name matches regular-expression ;
      event1 . attribute-name starts-with event2 . attribute-name ;
    }
    events [ events ];
    then {
      event-script script-name .xml {
        arguments {
          name  value ;
```

Copyright © 2013, Juniper Networks, Inc.

```
        }
        destination destination-name {
          retry-count number {
            retry-interval seconds ;
          }
          transfer-delay seconds ;
        }
        output-filename filename ;
        output-format (text | xml);
        user-name user-name ;
      }
      execute-commands {
        commands {
          "command";
        }
        destination destination-name {
          retry-count number {
            retry-interval seconds ;
          }
          transfer-delay seconds ;
        }
        output-file-name filename ;
        output-format (text | xml);
        user-name user-name ;
      }
      ignore;
      raise-trap;
      upload filename committed destination destination-name ;
      upload filename filename destination destination-name ;
    }
    within seconds not events [ events ];
  }
  traceoptions {
    file filename <files number > <size maximum-file-size >
    <world-readable | no-world-readable>;
    flag flag ;
  }
}
```

**Related Documentation**

- *Junos OS Monitoring and Troubleshooting Guide for Security Devices*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Junos OS Configuration and Operations Automation Guide


Copyright © 2013, Juniper Networks, Inc.

CHAPTER 8

# Firewall Hierarchy and Statements

This section contains the following topics:


- Firewall Configuration Statement Hierarchy on page 143


## Firewall Configuration Statement Hierarchy

Use the statements in the **firewall** configuration hierarchy to configure stateless firewall filters—also known as access control lists (ACLs)—on the device.

```
firewall {
  family family-name {
    dialer-filter filter-name {
      accounting-profile [ profile - name s];
      term term-name {
        from {
          match-conditions ;
        }
        then {
          action
          action-modifiers ;
          policer policer-name ;
          port-mirror;
          virtual-channel virtual-channel-name ;
        }
      }
    }
    filter filter-name {
      accounting-profile [ profile - names ];
      interface-specific;
      simple-filter filter-name {
        term term-name{
          from{
            match-conditions;
          }
          then{
            forwarding-class class-name ;
            loss-priority (high | low | medium) ;
          }
        }
      }
      term term-name {
```

Copyright © 2013, Juniper Networks, Inc.

```
        filter filter-name ;
        from {
          match-conditions ;
        }
        then {
          action ;
          action-modifiers ;
          policer policer-name ;
          port-mirror;
          virtual-channel virtual-channel-name ;
        }
      }
    }
    service-filter filter-name {
      term term-name {
        from {
          match-conditions ;
        }
        then {
          action ;
          action-modifiers ;
        }
      }
    }
    simple-filter filter-name {
      interface-specific;
      term term-name {
        from {
          match-conditions ;
        }
        then {
          action ;
          action-modifiers ;
        }
      }
    }
  }
  filter filter-name {
    accounting-profile [ profile-names ];
    interface-specific;
    term term-name {
      filter filter-name ;
      from {
        match-conditions ;
      }
      then {
        action ;
        action-modifiers ;
        virtual-channel virtual-channel-name ;
      }
    }
  }
  interface-set interface-set-name {
    [ interface-names ];
  }
  policer policer-name {
```


Copyright © 2013, Juniper Networks, Inc.

```
    filter-specific;
    if-exceeding {
      bandwidth-limit rate ;
      bandwidth-percent number ;
      burst-size-limit bytes ;
    }
    logical-bandwidth-policer;
    logical-interface-policer;
    then {
      policer-action;
    }
  }
  three-color-policer policer-name {
    action {
      loss-priority high {
        then {
          discard;
        }
      }
    }
    logical-interface-policer;
    single-rate {
      (color-aware | color-blind);
      committed-burst-size bytes ;
      committed-information-rate bps ;
      excess-burst-size bytes ;
    }
    two-rate {
      (color-aware | color-blind);
      committed-information-rate bps ;
      committed-burst-size bytes ;
      peak-information-rate bps ;
      peak-burst-size bytes ;
    }
  }
}
```

**Related Documentation**

- Routing Protocols and Policies Configuration Guide for Security Devices
- MPLS for Security Devices
- Routing Policy Configuration Guide

Copyright © 2013, Juniper Networks, Inc.

## policer (Firewall)

**Syntax**

```
policer policer-name{
  logical-bandwidth-policer;
  if-exceeding {
    bandwidth-limit rate;
  burst-size-limit bytes;
  }
  then {
  policer-action;
  }
}
```

**Hierarchy Level** [edit firewall]

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** Configure policer rate limits and actions. To activate a policer, you must include the policer action modifier in the **then** statement in a firewall filter term or on an interface.

**Options**

- *policer-name*—Name of the policer to evaluate when packets are received on the interface.
- *Policer-action*—One or more actions to take.
  - **discard**—Always discard non conforming red packets.
  - **forwarding-class** *classname*—Specify the particular forwarding class.
  - **loss-priority**—Set the loss priority to high or low.
- **then** —Action to take on matching packets.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- MPLS for Security Devices
- Routing Policy Configuration Guide


Copyright © 2013, Juniper Networks, Inc.

## simple-filter (Firewall)

**Syntax**

```
simple-filter filter-name {
  term term-name {
    from {
      match-conditions;
    }
    then {
      forwarding-class class-name;
      loss-priority (high | low | medium);
    }
  }
}
```

**Hierarchy Level** [edit firewall family *family-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Define a simple filter. Simple filters are recommended for metropolitan Ethernet applications.

**Options**

- **from**—Match packet fields to values. If the **from** option is not included, all packets are considered to match and the actions and action modifiers in the **then** statement are taken.
- **match-conditions**—One or more conditions to use to make a match.
- ***term-name***—Name that identifies the term. The name can contain letters, numbers, and hyphens (-), and can be up to 255 characters long. To include space in the name, enclose it in quotation marks (“ ”).
- **then**—Actions to take on matching packets. If the then option is not included and a packet matches all the conditions in the from statement, the packet is accepted.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- MPLS for Security Devices
- Routing Policy Configuration Guide

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 9

# Forwarding-Options Hierarchy and Statements

This section contains the following topics:


- Forwarding-Options Configuration Statement Hierarchy on page 149


## Forwarding-Options Configuration Statement Hierarchy

Use the statements in the **forwarding-options** configuration hierarchy to configure forwarding options including protocol family, flow monitoring, accounting properties, load-balancing, port mirroring, traffic sampling, and packet capture.

```
forwarding-options {
  accounting group-name  {
    output {
      aggregate-export-interval value ;
      cflowd [ hostnames ] {
        aggregation {
          autonomous-system;
          destination-prefix;
          protocol-port;
          source-destination-prefix {
            caida-compliant;
          }
          source-prefix;
        }
        autonomous-system-type;
        port;
        version;
      }
    }
  }
  dhcp-relay {
    group group-name {
      relay-option-60;
        interface;
        relay-option-82;
        circuit-id;
      }
    relay-option-60 {
      vendor-option;
```

Copyright © 2013, Juniper Networks, Inc.

```
    }
    relay-option-82 {
      circuit-id;
    }
    server-group server-group-name,
  family family-name {
    inet {
      filter (input | output);
    }
    inet6 {
      filter (input | output);
    }
    mpls {
      filter (input | output);
    }
  }
  hash-key {
    family {
      inet {
        layer-3;
        layer-4;
        session-id;
      }
      inet6 {
        layer-3;
        layer-4;
        session-id;
      }
      mpls {
        label-1;
        label-2;
        label-3;
        no-labels;
        payload {
          ip {
            layer-3-only;
            port-data {
              destination-lsb;
              destination-msb;
              source-lsb;
              source-msb;
            }
          }
        }
      }
    }
  }
  helpers {
    bootp {
      client-response-ttl value ;
      description text ;
      interface interface-name {
        broadcast;
        client-response-ttl number ;
        description description ;
        maximum-hop-count number ;
```


Copyright © 2013, Juniper Networks, Inc.

```
      minimum-wait-time seconds ;
      no-listen;
      server address ;
      vpn;
    }
    maximum-hop-count number ;
    minimum-wait-time seconds ;
    relay-agent-option;
    server address {
      routing-instance [ value ];
    }
    vpn;
  }
  domain {
    description text ;
    interface interface-name;
    server {
      address address ;
      routing-instance [ value ];
    }
  }
  port value {
    description text ;
    interface interface-name;
    server {
      address address ;
      routing-instance [ value ];
    }
  }
  tftp {
    description text ;
    interface interface-name;
    server {
      address address ;
      routing-instance [ value ];
    }
  }
  traceoptions {
    file filename {
      files number ;
      match regular-expression ;
      size maximum-file-size ;
      <world-readable | no-world-readable>;
    }
    flag {
      address;
      all;
      bootp;
      config;
      domain;
      ifdb;
      io;
      main;
      port;
      rtsock;
      tftp;
```

```
        trace;
        ui;
        util;
      }
      level level ;
    }
  }
  packet-capture {
    disable;
    file filename {
      <files number >;
      <size maximum-file-size >;
      <world-readable | no-world-readable>;
    }
    maximum-capture-size [ value ];
  }
  port-mirroring {
    family {
      inet {
        input {
          rate number ;
          run-length number ;
        }
        output {
          interface interface-name {
            next-hop {
              address ;
            }
          }
          no-filter-check;
        }
      }
    }
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
    }
  }
  sampling {
    disable;
    family (inet | inet6 | mpls ) {
      disable;
      output {
        extension-service name;
        file;
        flow-server name {
          aggregation {
            source-destination;
          }
        }
      }
    }
    input {
      max-packets-per-second number;
      rate number ;
      run-length number ;
```


Copyright © 2013, Juniper Networks, Inc.

```
        }
        traceoptions {
          file filename <files number > <size maximum-file-size >
          <world-readable | no-world-readable>;
        }
      }
    }
```

**Related Documentation**

- Routing Policy Configuration Guide
- Interfaces for Security Devices
- Monitoring and Troubleshooting for Security Devices
- MPLS for Security Devices
- Junos OS Services Interfaces Configuration Guide

## hash-key (Forwarding Options)

**Syntax**

```
hash-key {
  family {
    inet {
      layer-3;
      layer-4;
      session-id;
    }
    inet6 {
      layer-3;
      layer-4;
      session-id;
    }
    mpls {
      label-1;
      label-2;
      label-3;
      no-labels;
      payload {
        ip {
          layer-3-only;
          port-data {
            destination-lsb;
            destination-msb;
            source-lsb;
            source-msb;
          }
        }
      }
    }
  }
}
```

**Hierarchy Level** [edit forwarding-options]

**Release Information** Statement modified in Release 10.2 of Junos OS.

**Description** Select which packet header data to use for per-flow load balancing.

**Options**

- **inet**—IPv4 address family.
- **inet6**—IPv6 address family.
- **mpls**—MPLS address family.
- **layer-3**—Incorporate Layer 3 data into the hash key.
- **layer-4**—Incorporate Layer 4 data into the hash key.
- **session-id**—Incorporate session ID data into the hash key (SRX3000 and SRX5000 lines only). The session ID data has higher precedence than the Layer 3 or 4 information.
- **label-1**—Incorporate the first MPLS label into the hash key.
- **label-2**—Incorporate the second MPLS label into the hash key.


Copyright © 2013, Juniper Networks, Inc.

- **label-3**—Incorporate the third MPLS label into the hash key.
- **no-labels**—Include no MPLS labels into the hash key.
- **payload**—Incorporate payload data into the hash key.
- **ip**—Include the IP address of the IPv4 or IPv6 payload into the hash key.
- **layer-3–only**—Include only Layer 3 IP information.
- **port-data**—Include the source and destination port field information.
- **source-msb**—Include the most significant byte of the source port.
- **source-lsb**—Include the least significant byte of the source port.
- **destination-msb**—Include the most significant byte of the destination port.
- **destinatione-lsb**—Include the least significant byte of the destination port.

**Required Privilege Level**
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- MPLS for Security Devices
- Routing Policy Configuration Guide

## vpn (Forwarding Options)

**Syntax**
```
vpn;
```

**Hierarchy Level**
```
[edit forwarding-options helpers bootp]
```

**Release Information**
Statement introduced in Release 9.0 of Junos OS.

**Description**
For Dynamic Host Configuration Protocol (DHCP) or BOOTP client request forwarding, enable virtual private network (VPN) encryption for a client request to pass through a VPN tunnel.

**Required Privilege Level**
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 10

# Groups Hierarchy

This section contains the following topics:


- Groups Configuration Statement Hierarchy on page 157


## Groups Configuration Statement Hierarchy

Use the statements in the **groups** configuration hierarchy to configure information that can be dynamically updated in various parts of the device configuration.

```
groups {
  group-name  {
    configuration-data ;
  }
}
```

**Related Documentation**

- CLI User Guide

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 11

# Interfaces Hierarchy and Statements

This section contains the following topics:


- Interfaces Configuration Statement Hierarchy on page 159


## Interfaces Configuration Statement Hierarchy

Use the statements in the **interfaces** configuration hierarchy to configure interfaces on the device.

```
interfaces {
  interface-name {
    accounting-profile name ;
    atm-options {
      cell-bundle-size cells ;
      ilmi;
      linear-red-profiles profile-name {
        high-plp-max-threshold percent ;
        low-plp-max-threshold percent ;
        queue-depth cells high-plp-threshold percent low-plp-threshold percent ;
      }
      mpls {
        pop-all-labels {
          required-depth number;
        }
      }
      pic-type (atm1 | atm2);
      plp-to-clp;
      promiscuous-mode {
        vpi vpi-identifier;
      }
      scheduler-maps map-name {
        forwarding-class class-name {
          epd-threshold cells plp1 cells ;
          linear-red-profile profile-name ;
          priority (low | high);
          transmit-weight (cells number | percent number );
        }
        vc-cos-mode (alternate | strict);
      }
      vpi vpi-identifier {
        maximum-vcs maximum-vcs ;
```

Copyright © 2013, Juniper Networks, Inc.

```
      oam-liveness {
        down-count cells;
        up-count cells;
      }
      oam-period (disable | seconds);
      shaping {
        (cbr rate | rtvbr peak rate sustained rate burst length
        vbr peak rate sustained rate burst length );
        queue-length number ;
      }
    }
  }
  cellular-options {
    roaming-mode (home only | automatic)
    gsm-options {
      select-profile profile-name;
      profiles {
        profile-name {
          sip-user-id simple-ip-user-id;
          sip-password simple-ip-password;
          access-point-nameapn;
          authentication-method (pap | chap | none)
        }
      }
    }
  }
  clocking (external | internal);
  dce;
  description text ;
  dialer-options {
    pool pool-identifier ;
    priority priority-number ;
  }
  disable;
  dsl-options {
    loopback local;
    operating-mode mode ;
  }
  ds0-options {
    bert-algorithm algorithm ;
    bert-error-rate rate ;
    bert-period seconds ;
    byte-encoding (nx56 | nx64);
    fcs (16 | 32);
    idle-cycle-flag (flags | ones);
    invert data;
    loopback (payload | remote);
    start-end-flag (shared | filler);
  }
  e1-options {
    bert-algorithm algorithm ;
    bert-error-rate rate ;
    bert-period seconds ;
    fcs (16 | 32);
    framing (g704 | g704-no-crc4 | unframed);
    idle-cycle-flag (flags | ones);
```


Copyright © 2013, Juniper Networks, Inc.

```
    invert data;
    loopback (local | remote);
    start-end-flag (shared | filler);
    timeslots time-slot-range;
  }
  e3-options {
    atm-encapsulation (direct | PLCP);
    bert-algorithm algorithm ;
    bert-error-rate rate ;
    bert-period seconds ;
    buildout feet;
    compatibility-mode (digital-link | kentrox | larscom) <subrate value >;
    fcs (16 | 32);
    framing (g.751 | g.832);
    idle-cycle-flag value ;
    loopback (local | remote);
    (payload-scrambler | no-payload-scrambler);
    start-end-flag value ;
    (unframed | no-unframed);
  }
  encapsulation type ;
  ether-vpls-over-atm-llc;
  es-options {
    backup-interface es- pim /0/ port ;
  }
  fabric-options {
    member-interfaces member-interface-name;
  }
  failure-options {
    [trigger-link-failure interface-name ];
  }
  fastether-options {
    (flow-control | no-flow-control);
    ingress-rate-limit rate ;
    (loopback | no-loopback);
    mpls {
      pop-all-labels {
        required-depth [ number ];
      }
    }
    redundant-parent interface-name;
    source-address-filter {
      mac-address ;
    }
    (source-filtering | no-source-filtering);
  }
  framing (lan-phy | sdh | sonet | wan-phy);
  gigether-options {
    (auto-negotiation <remote-fault>
    (local-interface-online | local-interface-offline)> | no-auto-negotiation);
    (flow-control | no-flow-control);
    ignore-l3-incompletes;
    (loopback | no-loopback);
    mpls {
      pop-all-labels {
        required-depth number ;
```

Copyright © 2013, Juniper Networks, Inc.

```
    }
  }
  redundant-parent interface-name;
  source-address-filter {
    mac-address ;
  }
  (source-filtering | no-source-filtering);
  ethernet-switch-profile {
    ethernet-policer-profile {
      input-priority-map {
        ieee802.1p premium [ values ];
      }
      output-priority-map {
        classifier {
          premium {
            forward-class class-name {
              loss-priority (high | low);
            }
          }
        }
      }
      policer cos-policer-name {
        aggregate {
          bandwidth-limit bps ;
          burst-size-limit bytes ;
        }
        premium {
          bandwidth-limit bps ;
          burst-size-limit bytes ;
        }
      }
    }
    (mac-learn-enable | no-mac-learn-enable);
    tag-protocol-id [ tpids ...];
  }
}
(gratuitous-arp-reply | no-gratuitous-arp-reply);
hold-time up milliseconds down milliseconds ;
isdn-options {
  bchannel-allocation (ascending | descending);
  calling-number number;
  incoming-called-number number <reject>;
  media-type (voice | data);
  network-type (cpe | network);
  pool pool-name <priority priority> ;
  spid1 spid-string ;
  spid2 spid-string ;
  static-tei-val value ;
  switch-type (att5e | etsi | ni1 | ntdms100 | ntt);
  t310 seconds ;
  tei-option (first-call | power-up);
}
keepalives <down-count number > <interval seconds > <up-count number >;
lmi {
  lmi-type (ansi | itu);
  n391dte number ;
```


Copyright © 2013, Juniper Networks, Inc.

```
    n392dce number ;
    n392dte number ;
    n393dce number ;
    n393dte number ;
    t391dte seconds ;
    t392dce seconds ;
  }
  mac mac-address ;
  mlfr-uni-nni-bundle-options {
    acknowledge-retries number ;
    acknowledge-timer milliseconds ;
    action-red-differential-delay (disable-tx | remove-link);
    drop-timeout milliseconds ;
    fragment-threshold bytes ;
    hello-timer milliseconds ;
    link-layer-overhead percent ;
    lmi-type (ansi | itu);
    minimum-links number ;
    mrru bytes ;
    n391 number ;
    n392 number ;
    n393 number ;
    red-differential-delay milliseconds ;
    t391 seconds ;
    t392 seconds ;
    yellow-differential-delay milliseconds ;
  }
  modem-options {
    dialin (console | routable);
    init-command-string initialization-command-string ;
  }
  mtu bytes ;
  multiservice-options {
    boot-command filename;
    (core-dump | no-core-dump);
    (syslog | no-syslog);
  }
  native-vlan-idvlan-id;
  no-gratuitous-arp-request;
  no-keepalives;
  no-partition {
    interface-type type ;
  }
  passive-monitor-mode;
  per-unit-scheduler;
  ppp-options {
    chap {
      access-profile name;
      default-chap-secret name ;
      local-name name;
      passive;
    }
    compression {
      acfc;
      pfc;
    }
```

```
    no-termination-request;
    lcp-restart-timer milliseconds ;
    ncp-restart-timer milliseconds ;
    promiscuous-mode;
  }
  redundant-ether-options {
    (flow-control | no-flow-control);
    lacp {
      (active | passive);
      periodic (fast | slow);
    }
    link-speed speed;
    (loopback | no-loopback);
    minimum-links number;
    redundancy-group number;
    source-address-filter mac-address;
    (source-filtering | no-source-filtering);
  }
  serial-options {
    clock-rate rate ;
    clocking-mode (dce | internal | loop);
    control-leads {
      control-signal (assert | de-assert | normal);
      cts (ignore | normal | require);
      dcd (ignore | normal | require);
      dsr (ignore | normal | require);
      dtr signal-handling-option ;
      ignore-all;
      indication (ignore | normal | require);
      rts (assert | de-assert | normal);
      tm (ignore | normal | require);
    }
    control-polarity (positive | negative);
    cts-polarity (positive | negative);
    dcd-polarity (positive | negative);
    dsr-polarity (positive | negative);
    dtr-circuit (balanced | unbalanced);
    dtr-polarity (positive | negative);
    encoding (nrz | nrzi);
    indication-polarity (positive | negative);
    line-protocol protocol ;
    loopback mode;
    rts-polarity (positive | negative);
    tm-polarity (positive | negative);
    transmit-clock invert;
  }
  services-options {
    inactivity-timeout seconds ;
    open-timeout seconds ;
    syslog {
      host hostname {
        facility-override facility-name ;
        log-prefix prefix-number ;
        services priority-level ;
      }
    }
```


Copyright © 2013, Juniper Networks, Inc.

```
}
shdsl-options {
   annex (annex-a |annex-auto | annex-b);
   line-rate line-rate ;
   loopback (local | remote | payload);
   snr-margin {
      current margin ;
      snext margin ;
   }
}
t1-options {
   bert-algorithm algorithm ;
   bert-error-rate rate ;
   bert-period seconds ;
   buildout value ;
   byte-encoding (nx64 | nx56);
   fcs (16 | 32);
   framing (esf | sf);
   idle-cycle-flags (flags | ones);
   invert-data;
   line-encoding (ami | b8zs);
   loopback (local | payload | remote);
   remote-loopback-respond;
   start-end-flag (filler | shared);
   timeslots time-slot-range ;
}
t3-options {
   atm-encapsulation (direct | PLCP);
   bert-algorithm algorithm ;
   bert-error-rate rate ;
   bert-period seconds ;
   buildout feet;
   (cbit-parity | no-cbit-parity);
   compatibility-mode (adtran | digital-link | kentrox | larscom | verilink)
   <subrate value >;
   fcs (16 | 32);
   (feac-loop-respond | no-feac-loop-respond);
   idle-cycle-flag value ;
   (long-buildout | no-long-buildout);
   (loop-timing | no-loop-timing);
   loopback (local | payload | remote);
   (payload-scrambler | no-payload-scrambler);
   start-end-flag value (filler | shared);
}
threshold bytes ;
traceoptions {
   flag flag < flag-modifier > <disable>;
}
(traps | no-traps);
vdsl-options {
   vdsl-profile 17a;
}
unit logical-unit-number {
   accept-source-mac {
      mac-address mac-address ;
      policer {
```

Copyright © 2013, Juniper Networks, Inc.

```
      input policer-name ;
      output policer-name ;
    }
  }
  accounting-profile name ;
  allow-any-vci;
  atm-scheduler-map (default | map-name );
  arp-resp ( resricted | unresricted);
  backup-options {
    interface interface-name ;
  }
  bandwidth rate ;
  cell-bundle-size cells ;
  clear-dont-fragment-bit;
  compression {
    rtp {
      f-max-period number ;
      maximum-contexts number ;
      port {
        maximum port-number ;
        minimum port-number ;
      }
      queues [ queue-numbers ];
    }
  }
  compression-device interface-name;
  copy-tos-to-outer-ip-header;
  description text ;
  dialer-options {
    activation-delay seconds ;
    callback;
    callback-wait-period seconds ;
    deactivation-delay seconds ;
    dial-string [ dial-string-numbers ];
    idle-timeout seconds ;
    incoming-map (accept-all | caller caller-number );
    initial-route-check seconds ;
    load-interval seconds ;
    load-threshold percent ;
    pool pool-name ;
    redial-delay time ;
    watch-list {
      [ routes ];
    }
  }
  disable;
  disable-mlppp-inner-ppp-pfc;
  dlci dlci-identifier ;
  drop-timeout milliseconds ;
  dynamic-call-admission-control {
    activation-priority number ;
    bearer-bandwidth-limit threshold ;
  }
  encapsulation (cisco-hdlc | frame-relay | multilink-frame-relay-uni-nni | ppp |
    ppp-over-ether);
  epd-threshold cells plp1 cells ;
```


Copyright © 2013, Juniper Networks, Inc.

```
f-max-period number ;
family {
  bridge {
    interface-mode {
      access vlan-id vlan-id |
      trunk {
        vlan-id-list vlan-list |
        vlan-rewrite translate from-vlan-id internal-vlan-id
      }
    }
  inet {
    address IP–address ;
    }
  }
  inet6 {
    address IP–address ;
    }
  }
fragment-threshold bytes ;
input-vlan-map {
  (pop | pop-pop | pop-swap | push | push-push | swap
  swap-push | swap-swap);
  inner-tag-protocol-id tpid;
  inner-vlan-id number ;
  tag-protocol-id tpid;
  vlan-id number ;
}
interleave-fragments;
inverse-arp;
(keepalives | no-keepalives);
link-layer-overhead percent ;
minimum-links number ;
mrru bytes ;
multicast-dlci dlci-identifier ;
multicast-vci vpi-identifier.vci-identifier ;
multilink-max-classes number ;
multipoint number ;
multipoint;
oam-liveness {
  up-count cells ;
  down-count cells ;
}
oam-period (disable | seconds );
output-vlan-map {
  (pop | pop-pop | pop-swap | push | push-push | swap
  swap-push | swap-swap);
  inner-tag-protocol-id tpid;
  inner-vlan-id number ;
  tag-protocol-id tpid;
  vlan-id number ;
}
passive-monitor-mode;
peer-unit unit-number ;
plp-to-clp;
point-to-point;
ppp-options {
```

Copyright © 2013, Juniper Networks, Inc.

```
        chap {
            access-profile name ;
            default-chap-secret name ;
            local-name name ;
            passive;
        }
        compression {
            acfc;
            pfc;
        }
        lcp-restart-timer milliseconds ;
        loopback-clear-timer seconds ;
        ncp-restart-timer milliseconds ;
        no-termination-request;
        pap;
        access-profile name ;
        default-password password ;
        local-name name ;
        local-password password ;
        passive;
    }
}
pppoe-options {
    access-concentrator name ;
    auto-reconnect seconds ;
    service-name name ;
    underlying-interface interface-name ;
}
proxy-arp;
service-domain (inside | outside);
shaping{
    (cbr rate | rtvbr peak rate sustained rate burst length
    vbr peak rate sustained rate burst length );
    queue-length number ;
}
short-sequence;
three-color-policer {
    input policer-name ;
    output policer-name ;
}
transmit-weight number ;
(traps | no-traps);
trunk-bandwidth rate ;
trunk-id number ;
tunnel {
    backup-destination address ;
    destination address ;
    key number ;
    routing-instance {
        destination routing-instance-name;
    }
    source source-address ;
    ttl number ;
}
vci vpi-identifier.vci-identifier ;
vpi vpi-identifier ;
```


Copyright © 2013, Juniper Networks, Inc.

```
vlan-id number ;
vlan-tagging native-vlan-id vlan-id;
vlan-tags inner tpid.vlan-id outer tpid.vlan-id ;
family family {
  accounting {
    destination-class-usage;
    source-class-usage {
      direction ;
    }
  }
  address address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    broadcast address ;
    destination address ;
    destination-profile name ;
    eui-64;
    multipoint-destination address dlci dlci-identifier ;
    multipoint-destination address {
      epd-threshold cells ;
      inverse-arp;
      oam-liveness {
        up-count cells ;
        down-count cells ;
      }
      oam-period ( disable | seconds );
      shaping{
        (cbr rate | rtvbr peak rate sustained rate burst length
        vbr peak rate sustained rate burst length );
        queue-length number ;
      }
      vci vpi-identifier.vci-identifier ;
    }
    preferred;
    primary;
    vrrp-group group-number {
      (accept-data | no-accept-data):
      advertise-interval seconds ;
      authentication-type authentication ;
      authentication-key key ;
      fast-interval milliseconds;
      (preempt | no-preempt) {
        hold-time seconds ;
      }
      priority number ;
      track {
        interface interface-name {
          priority-cost priority ;
          bandwidth-threshold bits-per-second {
            priority-cost priority ;
          }
        }
        priority-hold-time seconds ;
      }
      virtual-address [ addresses ];
    }
    web-authentication {
```

Copyright © 2013, Juniper Networks, Inc.

```
      http;
    }
  }
  bundle interface-name ;
  dhcp {
    client-identifier (ascii ascii | hexadecimal hexadecimal);
    lease-time seconds;
    retransmission-attempt number;
    retransmission-interval seconds;
    server-address ip-address;
    update-server;
    vendor-id vendor-id;
  }
  dhcp-client {
    client-identifier {
      user-id {ascii ascii| hexadecimalhexadecimal};
      use-interface-description {logical |device};
      prefix [host-name| logical system-name| routing-instance-name];
    }
    lease-time seconds;
    retransmission-attempt number;
    retransmission-interval seconds;
    server-address ip-address;
    update-server;
    vendor-id vendor-id;
  }
  dialer filter-name;
  filter {
    group filter-group-number;
    input filter-name;
    input-list {
      [filter-names];
    }
    output filter-name ;
    output-list {
      [filter-names];
    }
  }
  keep-address-and-control;
  mtu bytes ;
  multicast-only;
  next-hop-tunnel gateway-address ipsec-vpn vpn-name;
  no-redirects;
  policer {
    arp policer-template-name;
    input policer-template-name;
    output policer-template-name;
  }
  primary;
  proxy inet-address address ;
  receive-options-packets;
  receive-ttl-exceeded;
  remote (inet-address address | mac-address address);
  rpf-check <fail-filter filter-name> {
    <mode loose>;
  }
```


Copyright © 2013, Juniper Networks, Inc.

```
        sampling {
          direction ;
        }
        service {
          input {
            service-set service-set-name <service-filter filter-name >;
            post-service-filter filter-name ;
          }
          output {
            service-set service-set-name <service-filter filter-name >;
          }
        }
        simple-filter{
          input filter-name;
        }
        (translate-discard-eligible | no-translate-discard-eligible);
        (translate-fecn-and-becn | no-translate-fecn-and-becn);
        unnumbered-address {
          interface-name ;
          destination destination-address ;
          destination-profile profile-name ;
          preferred-source-address interface-name ;
        }
        traceoptions {
          flag flag <disable>;
        }
      }
    }
    interface-range interface-range-name {
      aggregated-ether-options {
        lacp {
          (active | passive);
          periodic (fast | slow);
        }
        link-speed speed;
        minimum-links number;
      }
      partition partition-number {
        interface-type type ;
        oc-slice oc-slice-range ;
        timeslots time-slot-range ;
      }
    }
    traceoptions {
      file filename <files number > <match regular-expression >
      <size maximum-file-size > <world-readable | no-world-readable>;
      flag flag <disable>;
    }
  }
```

**Related Documentation**

- Layer 2 Bridging and Transparent Mode for Security Devices
- Interfaces for Security Devices
- Device Configuration
- Upgrades and Downgrades

Copyright © 2013, Juniper Networks, Inc.

## accept-source-mac

**Syntax** accept-source-mac mac-address *mac-address*

**Hierarchy Level** [edit interfaces *interface-name* unit logical-unit-number]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** For Gigabit Ethernet (GE), Fast Ethernet (FE), or 10 Gigabit Ethernet (XE) interfaces, specify the MAC addresses from which the interface can receive packets. Ensure that you update the MAC address if the remote Ethernet card is replaced. Replacing the interface card changes the MAC address. If you do not update the MAC address, the interface cannot receive packets from the new card.



NOTE:

- Source-address filtering is not supported on J Series devices.
- Software-based MAC limiting is supported on SRX100, SRX210, SRX220, SRX240, and SRX650 devices. A maximum of 32 MAC addresses is supported per device.

**Options** ***mac-address*** —MAC address filter. You can specify the MAC address as six hexadecimal bytes in one of the following formats: ***nn:nn:nn:nn:nn:nn:nn*** (for example, **00:11:22:33:44:55**) or ***nnnn:nnnn:nnnn*** (for example, **0011.2233.4455**). You can configure up to 32 source addresses. To specify more than one address, include multiple ***mac-addresses*** in the **source-address-filter** statement.

**Required Privilege Level** interface—To view this statement in the configuration..
interface-control—To add this statement to the configuration.

**Related Documentation**

- Interfaces Overview


Copyright © 2013, Juniper Networks, Inc.

## access-point-name

**Syntax** **access-point-name** *apn*;

**Hierarchy Level** **[edit interfaces** *interface-name* **cellular-options gsm-options profiles** *profile-name***]**

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure the access point name (APN) provided by the service provider for connection to a Global System for Mobile Communications (GSM) cellular network.

**Options** ***apn***—Access point name.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Modem Interfaces
- Interfaces for Security Devices

## activation-priority (Interfaces)

**Syntax** activation-priority *priority*;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* dynamic-call-admission-control]

**Release Information** Statement introduced in Release 8.2 of Junos OS.

**Description** This statement is used only in conjunction with J Series Services Routers that support voice over IP with the TGM550 media gateway module. For Fast Ethernet and Gigabit Ethernet interfaces, ISDN BRI interfaces, and serial interfaces with PPP or Frame Relay encapsulation, configure the dynamic call admission control (dynamic CAC) activation priority value.

**Options** ***priority***—The activation priority at which the interface is used for providing call bandwidth. The interface with the highest activation priority value is the primary link for providing call bandwidth. If the primary link becomes unavailable, the TGM550 switches over to the next active interface with the highest activation priority value, and so on.

**Range:** 0 through 255

**Default:** 50

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices
- ISDN Interfaces
- VoIP Interfaces

Copyright © 2013, Juniper Networks, Inc.

## annex (Interfaces)

**Syntax** annex *annex-type*

**Hierarchy Level** [edit interfaces *interfaces-name* shdsl-options]

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Select an annex type that suits your requirements for configuring G.SHDSL interface.

**Options**
- Annex A
- Annex-auto
- Annex B
- Annex F
- Annex G



NOTE: The default configuration is annex-auto instead of annex-b.

**Required Privilege Level**
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

## apply-groups

**Syntax** apply-groups;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* radio-router]

**Release Information** Statement introduced in Release 9.6 of Junos OS .

**Description** Apply the groups from which to inherit configuration data. If **radio-router** is set without any other attributes specified, the first four values become 100 and threshold stays at 10, and capacity, margin, and delay are deprecated. If **radio-router** is set, do not change the OSPF reference-bandwidth value because this generates an incorrect link cost.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interface Encapsulation


Copyright © 2013, Juniper Networks, Inc.

## arp-resp

**Syntax** arp-resp (restricted|unrestricted);

**Hierarchy Level** [edit interfaces *interfaces-name* unit *logical-unit-number* ]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** Configure Address Resolution Protocol (ARP) response on the interface.

**Options**
- **restricted**—Enable restricted proxy ARP response on the interface. This is the default.
- **unrestricted**—Enable unrestricted ARP response on the interface.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces Overview

## authentication-method (Interfaces)

**Syntax** **authentication-method (pap | chap | none);**

**Hierarchy Level** **[edit interfaces** *interface-name* **cellular-options gsm-options profiles** *profile-name***]**

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Specify the authentication method for connection to a Global System for Mobile Communications (GSM) cellular network.

**Options**
- **pap**—Password Authentication Protocol.
- **chap**—Challenge Handshake Authentication Protocol.
- **none**—No authentication method is used.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Modem Interfaces
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## bandwidth (Interfaces)

**Syntax** bandwidth <*value*>;

**Hierarchy Level** [edit interfaces *interface-name* radio-router]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** This option controls the weight of the current (vs. maximum) data rate (value 0–100).

**Required Privilege Level** **interface**—To view this statement in the configuration.
**interface-control**—To add this statement to the configuration.

**Related Documentation**
- Interfaces Overview

## bearer-bandwidth-limit (Interfaces)

**Syntax** bearer-bandwidth-limit *kilobits-per-second*;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* dynamic-call-admission-control]

**Release Information** Statement introduced in Release 8.2 of Junos OS.

**Description** This statement is used only in conjunction with J Series Services Routers that support voice over IP with the TGM550. For Fast Ethernet and Gigabit Ethernet interfaces, ISDN BRI interfaces, and serial interfaces with PPP or Frame Relay encapsulation, configure the bearer bandwidth limit (BBL). The BBL is used for dynamic call admission control (dynamic CAC) to provide enhanced control over WAN bandwidth.

**Options** ***kilobits-per-second***—The bearer bandwidth limit to be reported to a TGM550, in kilobits per second (Kbps).

**Range:** 0 through 9999 Kbps

**Default:** –1 (dynamic CAC is not enabled on the interface)

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices
- ISDN Interfaces
- VoIP Interfaces


Copyright © 2013, Juniper Networks, Inc.

## bundle (Interfaces)

**Syntax** bundle;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family mlppp ]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Specify the logical interface name the link joins.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Modem Interfaces
- Interfaces for Security Devices

## cbr rate

**Syntax** cbr rate;

**Hierarchy Level** [edit interfaces interface-name atm-options vpi vpi-identifier shaping]

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** For ATM encapsulation only, define a constant bit rate bandwidth utilization in the traffic-shaping profile.

**Options**
- CBR Value–Constant bandwidth utilization (range: 33,000 through 1,199,920)
- CDVT–Cell delay variation tolerance in microseconds (range: 1 through 9999)

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## cellular-options

**Syntax**

```
cellular-options {
  roaming-mode (home only | automatic)
  gsm-options {
    select-profile profile-name;
    profiles {
      profile-name {
        sip-user-id simple-ip-user-id;
        sip-password simple-ip-password;
        access-point-name apn;
        authentication-method (pap | chap | none);
      }
    }
  }
}
```

**Hierarchy Level** [edit interfaces *interface-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure options for connecting a 3G wireless modem interface to a cellular network.

**Options** The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Modem Interfaces
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## client-identifier (Interfaces)

**Syntax** client-identifier (ascii *ascii* | hexadecimal *hexadecimal* );

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family *family-name* dhcp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify an ASCII or hexadecimal identifier for the Dynamic Host Configuration Protocol (DHCP) client. The DHCP server identifies a client by a client-identifier value.

**Options**
- ascii *ascii* —Identifier consisting of ASCII characters.
- hexadecimal *hexadecimal* —Identifier consisting of hexadecimal characters.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Modem Interfaces
- Interfaces for Security Devices

## client-identifier (dhcp-client)

**Syntax**
```
client-identifier {
   user-id {ascii ascii hexadecimal hexadecimal;
   use-interface-description {logical |device};
   prefix [host-name routing-instance-name];
}
```

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** The DHCP server identifies a client by a client-identifier value.

**Options** The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration

Copyright © 2013, Juniper Networks, Inc.

## compression-device (Interfaces)

**Syntax** compression-device *name*;

**Hierarchy Level** [edit interfaces *interface-name* unit (Interfaces) *logical-unit-number*]

**Release Information** Statement introduced before Release 7.4 of Junos OS.

**Description** For J Series routers with PPP over Ethernet interfaces, configure the name of the access concentrator (AC).

**Options** ***name***—Name of the AC.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices
- Link Services and Special Interfaces

## credit (Interfaces)

**Syntax**
```
credit {
interval;
}
```

**Hierarchy Level** [edit interfaces *interface-name* radio—router ]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** This parameter controls credit-based scheduling parameters and includes an interval option to set the grant rate interval to a value between 1–60 seconds.

**Required Privilege Level** **interface**—To view this statement in the configuration.
**interface-control**—To add this statement to the configuration.

**Related Documentation**
- Interfaces Overview


Copyright © 2013, Juniper Networks, Inc.

## data-rate

**Syntax** data-rate *weight*;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* radio-router]

**Release Information** Statement introduced in Release 10.2 of Junos OS .

**Description** Configure the weight of the resource factor when calculating an effective data rate.

**Options** ***weight***—Factor used to calculate data rate.
**Range:** 0 through 100
**Default:** 100

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces Overview

## dhcp (Interfaces)

**Syntax**
```
dhcp {
  client-identifier (ascii ascii | hexadecimal hexadecimal );
  lease-time seconds ;
  retransmission-attempt number ;
  retransmission-interval seconds ;
  server-address ip-address ;
  update-server;
  vendor-id vendor-id ;
}
```

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family *family* ]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the Dynamic Host Configuration Protocol (DHCP) client.

**Options** The statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## dhcp-client

**Syntax**

```
dhcp-client {
  client-identifier {
    user-id {ascii ascii hexadecimal hexadecimal;
    use-interface-description {logical |device};
    prefix [host-name routing-instance-name];
  }
  lease-time seconds;
  retransmission-attempts number;
  retransmission-interval seconds;
  server ip-address;
  update-server;
  vendor-id vendor-id;
}
```

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family *family*]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Configure the Dynamic Host Configuration Protocol (DHCP) client.

**Options** The remaining statements are explained separately.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

## dynamic-call-admission-control (Interfaces)

**Syntax**

```
dynamic-call-admission-control {
  activation-priority priority;
  bearer-bandwidth-limit kilobits-per-second;
}
```

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number*]

**Release Information** Statement introduced in Release 8.2 of Junos OS.

**Description** This statement is used only in conjunction with J Series Services Routers that support voice over IP with the TGM550. For Fast Ethernet and Gigabit Ethernet interfaces, ISDN BRI interfaces, and serial interfaces with PPP or Frame Relay encapsulation, configure dynamic call admission control (CAC). Dynamic CAC provides enhanced control over WAN bandwidth. When dynamic CAC is configured on an interface responsible for providing call bandwidth, the TGM550 informs the Media Gateway Controller (MGC) of the bandwidth limit available for voice packets on the interface and requests that the MGC block new calls when the bandwidth is exhausted.

Dynamic CAC must be configured on each J Series Services Router interface responsible for providing call bandwidth.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Interfaces for Security Devices
- ISDN Interfaces

Copyright © 2013, Juniper Networks, Inc.

## encapsulation (Interfaces)

**Syntax** encapsulation
(cisco-hdlc | frame-relay | multilink-frame-relay-uni-nni | ppp | ppp-over-ether)

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* ]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Specify logical link layer encapsulation.

**Options**

- **cisco-hdlc**—For normal mode (when the device is using only one B-channel). Cisco-compatible High-Level Data Link Control is a group of protocols for transmitting data between network points
- **frame-relay**—Configure a Frame Relay encapsulation when the physical interface has multiple logical units, and the units are either point to point or multipoint.
- **multilink-frame-relay-uni-nni**—Link services interfaces functioning as FRF.16 bundles can use Multilink Frame Relay UNI NNI encapsulation.
- **ppp**—For normal mode (when the device is using only one ISDN B-channel per call). Point-to-Point Protocol is for communication between two computers using a serial interface.
- **ppp-over-ether**—This encapsulation is used for underlying interfaces of pp0 interfaces.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Interfaces for Security Devices
- Feature Support Reference for SRX Series and J Series Devices


Copyright © 2013, Juniper Networks, Inc.

## fabric-options

**Syntax**

```
fabric-options {
  member-interfaces member-interface-name ;
}
```

**Hierarchy Level** [edit interfaces *interface-name* ]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure fabric interface properties.

**Options** The remaining statement is explained separately.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## family bridge

**Syntax**

```
family bridge {
  interface-mode {
    access vlan-id vlan-id |
    trunk {
      vlan-id-list vlan-list |
      vlan-rewrite translate from-vlan-id internal-vlan-id
    }
  }
}
```

**Hierarchy Level** [edit interfaces *interface* unit *unit* ]

**Release Information** Statement modified in Release 9.6 of Junos OS.

**Description** Configure a Layer 2 logical interface.



NOTE: If a physical interface has a bridge family logical interface, it cannot have any other family type in its logical interfaces.

**Options** **interface-mode**—Either **access** or **trunk**:

- An access mode interface accepts untagged packets, assigns the specified VLAN identifier to the packet, and forwards the packet within the bridge domain that is configured with the matching VLAN identifier.
- A trunk mode interface accepts any packet tagged with a VLAN identifier that matches a specified list of VLAN identifiers.

  **vlan-rewrite translate**—Rewrites the ***from-vlan-id*** VLAN identifier with the ***internal-vlan-id*** in packets arriving on a Layer 2 trunk port. The ***internal-vlan-id*** must be in the ***vlan-list*** for the trunk port.



NOTE: The *from-vlan-id* and *internal-vlan-id* must not be the same VLAN identifier configured with the native-vlan-id statement for the trunk port.

**Required Privilege Level** **interface**—To view this statement in the configuration.
**interface-control**—To add this statement to the configuration.

**Related Documentation**

- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## family inet (Interfaces)

**Syntax**

```
family inet {
    address ip-address;
    }
}
```

**Hierarchy Level** [edit interfaces *interface* unit *unit* ]

**Release Information** Statement introduced in a prior release of Junos OS.

**Description** Assign an IP address to a logical interface.

**Options** *ipaddress*—Specifies the IP address for the interface.



NOTE: You use family inet to assign an IPv4 address. You use family inet6 to assign an IPv6 address. An interface can be configured with both an IPv4 and IPv6 address.

**Required Privilege Level**
**interface**—To view this statement in the configuration.
**interface-control**—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## family inet6

**Syntax**

```
family inet6 {
    address ip-address;
    }
}
```

**Hierarchy Level** [edit interfaces *interface* unit *unit* ]

**Release Information** Statement supported in Junos 10.2 for SRX Series and J Series devices.

**Description** Assign an IP address to a logical interface.

**Options** *ipaddress*—Specifies the IP address for the interface.



NOTE: You use family inet6 to assign an IPv6 address. You use family inet to assign an IPv4 address. An interface can be configured with both an IPv4 and IPv6 address.

**Required Privilege Level**
**interface**—To view this statement in the configuration.
**interface-control**—To add this statement to the configuration.

**Related Documentation**

- Layer 2 Bridging and Transparent Mode for Security Devices
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## flag (Interfaces)

**Syntax** flag

**Hierarchy Level** [edit interfaces interface-name traceoptions]

**Release Information** Command introduced in Release 10.1 of Junos OS.

**Description** Define tracing operations for individual interfaces. To specify more than one tracing operation, include multiple flag statements.

**Options**

- **all**—Enable all interface trace flags.
- **event** —Trace interface events.
- **cache**—Enable interface flags for Web filtering cache maintained on the routing table.
- **enhanced**—Enable interface flags for processing through Enhanced Web Filtering.
- **ipc**—Trace interface IPC messages.
- **media**—Trace interface media changes.
- **critical**—Trace critical events.
- **major**—Trace major events.



NOTE:

- MTU is limited to 1518 on this interface.
- **Cache** and **enhanced** options are applicable only to Enhanced Web Filtering.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## flexible-vlan-tagging (Interfaces)

**Syntax** flexible-vlan-tagging native-vlan-id *vlan-id*;

**Hierarchy Level** [edit interfaces *interface* ]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Simultaneously supports transmission of 802.1Q VLAN single-tag and dual-tag frames on logical interfaces on the same Ethernet port.

**Options** **native-vlan-id**—Configures a VLAN identifier for single-tag frames, dual-tag frames, or a mixture of single-tag and dual-tag frames.

**Required Privilege Level** **interface**—To view this statement in the configuration.
**interface-control**—To add this statement to the configuration.

**Related Documentation**
- Interfaces Overview

## flow-control (Interfaces)

**Syntax** **(flow-control | no-flow-control);**

**Hierarchy Level** **[edit interfaces *interface-name* fastether-options],**
**[edit interfaces *interface-name* gigether-options],**
**[edit interfaces *interface-name* redundant-ether-options]**

**Release Information** Statement modified in Release 9.0 of Junos OS.

**Description** For Fast Ethernet, Gigabit Ethernet, and redundant Ethernet interfaces only, explicitly enable flow control, which regulates the flow of packets from the device to the remote side of the connection. Enabling flow control is useful when the device is a Gigabit Ethernet switch.



NOTE: **The flow-control option is not supported on Fast Ethernet and Gigabit Ethernet interfaces on J Series devices.**

**Default** Flow control is the default behavior.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## fpc (Interfaces)

**Syntax** fpc;

**Hierarchy Level** [edit interfaces pic-set pic-set-name]

**Release Information** Command introduced in Release 9.6 of Junos OS.

**Description** Sets the PIC bundle and the FPC slot.

**Options**
- ***apply-groups***—Inherit configuration data from these groups.
- ***apply-groups-except***—Do not inherit configuration data from these groups.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces Overview

## gsm-options

**Syntax**
```
gsm-options {
  select-profile profile-name;
  profiles {
    profile-name {
      sip-user-id simple-ip-user-id;
      sip-password simple-ip-password;
      access-point-name apn;
      authentication-method (pap | chap | none);
    }
  }
}
```

**Hierarchy Level** [edit interfaces *interface-name* cellular-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure the 3G wireless modem interface to establish a data call with a Global System for Mobile Communications (GSM) cellular network.

**Options** The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Modem Interfaces
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## hub-assist

**Syntax** hub-assist *weight*;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* radio-router]

**Release Information** Statement introduced in Release 10.2 of Junos OS..

**Description** Configure the weight of the resource factor when calculating an effective interface bandwidth.

**Options** ***weight***—Factor used to calculate interface bandwidth.
**Range:** 0 through 100
**Default:** 100

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Configuring PPPoE-Based Radio-to-Router Protocols
- Modem Interfaces
- Interfaces for Security Devices

## interface (PIC Bundle)

**Syntax** interface *interface-name*;

**Hierarchy Level** [edit interfaces pic-set pic-set-name]

**Release Information** Command introduced in Release 9.6 of Junos OS.

**Description** Sets the PIC bundle and the interface.

**Options**
- ***apply-groups***— Groups from which to inherit configuration data.
- ***apply-groups-except***— Do not inherit configuration data from these groups.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces Overview


Copyright © 2013, Juniper Networks, Inc.

## interval (Interfaces)

**Syntax** interval *seconds*;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* radio-router credit]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** Configure the frequency that the router generates credit announcement messages.

**Options** ***seconds***—Interval between PADG credit announcements for each session.
**Range:** 0 through 60
**Default:** 1

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces Overview

## lacp (Interfaces)

**Syntax**
```
lacp {
  (active | passive);
  periodic (fast | slow);
}
```

**Hierarchy Level** [edit interfaces *interface-name* redundant-ether-options]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** For redundant Ethernet interfaces in a chassis cluster only, configure Link Aggregation Control Protocol (LACP).

**Options**
- **active**—Initiate transmission of LACP packets.
- **passive**—Respond to LACP packets.

**Default:** If you do not specify **lacp** as either **active** or **passive**, LACP remains off (the default).

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## latency (Interfaces)

**Syntax** latency <*value*>;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* radio—router ]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** This option controls the latency weight (value 0–100).

**Required Privilege Level** **interface**—To view this statement in the configuration.
**interface-control**—To add this statement to the configuration.

**Related Documentation**
- Interfaces Overview

## lease-time

**Syntax** lease-time (*seconds* | infinte);

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family inet dhcp]

**Release Information** Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** Request a specific lease time for the IP address.

**Default** Iif no lease time is requested by client, then the server sends the lease time. The default lease time on a JUNOS OS DHCP server is one day.

**Options** ***seconds*** —Request a lease time of a specific duration.
**Range:** 60 through 2147483647 seconds

**infinite**—Request that the lease never expire.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## lease-time (dhcp-client)

**Syntax** lease-time *seconds*;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the time to negotiate and exchange Dynamic Host Configuration Protocol (DHCP) information.

**Options** **seconds**— Request time to negotiate and exchange information.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration

## line-rate (Interfaces)

**Syntax** line-rate

**Hierarchy Level** [edit interfaces *interfaces name* shdsl-options]

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Specify a line rate for an G.SHDSL interface.

**Options**
- **auto**— Automatically selects a line rate.
- **value** — Select the values between 192 kbps and 22784 kbps for the speed of transmission of data on the G.SHDSL connection.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## link-speed (Interfaces)

**Syntax** **link-speed** ***speed*;**

**Hierarchy Level** **[edit interfaces** ***interface-name*** **redundant-ether-options]**

**Release Information** Statement modified in Release 9.0 of Junos OS.

**Description** For redundant Ethernet interfaces in a chassis cluster only, set the required link speed.

**Options** ***speed*** —For redundant Ethernet links, you can specify ***speed*** in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

## loopback (Interfaces)

**Syntax** **(loopback | no-loopback);**

**Hierarchy Level** **[edit interfaces** ***interface-name*** **redundant-ether-options]**

**Release Information** Statement modified in Release 9.0 of Junos OS.

**Description** For Fast Ethernet, Gigabit Ethernet, and redundant Ethernet interfaces, enable or disable loopback mode.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## media-type (Interfaces)

**Syntax** media-type

**Hierarchy Level** [edit interfaces *interface-name* media-type]

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Configure the operating modes for the 2-Port 10 Gigabit Ethernet XPIM.

**Options**
- copper
- fiber

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

## member-interfaces

**Syntax** member-interfaces ***member-interface-name***;

**Hierarchy Level** [edit **interfaces** ***interface-name*** fabric-options]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the member interface name. Member interfaces that connect to each other must be of the same type.

**Options** ***member-interface-name*** —Member interface name.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## minimum-links (Interfaces)

**Syntax** **minimum-links** *number*;

**Hierarchy Level** **[edit interfaces** *interface-name* **redundant-ether-options]**

**Release Information** Statement added in Release 10.1 of Junos OS.

**Description** For redundant Ethernet interfaces configured as 802.3ad redundant Ethernet interface link aggregation groups (LAGs) in a chassis cluster only, set the required minimum number of physical child links on the primary node that must be working to prevent the interface from being down. Interfaces configured as redundant Ethernet interface LAGs typically have between 4 and 16 physical interfaces, but only half, those on the primary node, are relevant to the minimum-links setting.

If the number of operating interfaces on the primary node falls below the configured value, it will cause the interface to be down even if some of the interfaces are still working.

**Options** *number*—For redundant Ethernet interface link aggregation group links, specify the number of physical child links on the primary node in the redundant Ethernet interface that must be working. The default **minimum-links** value is 1. The maximum value is half of the total number of physical child interfaces bound to the redundant Ethernet interface being configured or 8, whichever is smaller.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## native-vlan-id (Interfaces)

**Syntax** native-vlan-id *vlan-id*;

**Hierarchy Level** [edit interfaces *interface-name* ]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure VLAN identifier for untagged packets received on the physical interface of a trunk mode interface.

**Options** ***vlan-id***—Configure a VLAN identifier for untagged packets. Enter a number from 0 through 4094.

**Required Privilege Level** **interface**—To view this statement in the configuration.
**interface-control**—To add this statement to the configuration

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- Interfaces for Security Devices

## next-hop-tunnel

**Syntax** **next-hop-tunnel** ***gateway-address*** **ipsec-vpn** ***vpn-name*****;**

**Hierarchy Level** **[edit interfaces** ***interface-name*** **unit** ***logical-unit-number*** **family** ***family-name*****]**

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** For the secure tunnel (**st**) interface, create entries in the Next-Hop Tunnel Binding (NHTB) table, which is used to map the next-hop gateway IP address to a particular IP Security (IPsec) Virtual Private Network (VPN) tunnel. NHTB allows the binding of multiple IPsec VPN tunnels to a single IPsec tunnel interface.

**Options**

- ***gateway-address***—Next-hop gateway IP address.
- **ipsec-vpn** ***vpn-name*** —VPN to which the next-hop gateway IP address is mapped.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## periodic (Interfaces)

**Syntax** **periodic (fast | slow);**

**Hierarchy Level** **[edit interfaces *interface-name* redundant-ether-options lacp]**

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** For redundant Ethernet interfaces in a chassis cluster only, configure the interval at which the interfaces on the remote side of the link transmit link aggregation control protocol data units (PDUs) by configuring the **periodic** statement on the interfaces on the local side. It is the configuration on the local side that specifies the behavior of the remote side. That is, the remote side transmits link aggregation control PDUs at the specified interval.

**Options**
- **fast**—Transmit link aggregation control PDUs every second.
- **slow**—Transmit link aggregation control PDUs every 30 seconds.

**Default: fast**

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

## ppp-over-ether

**Syntax** ppp-over-ether

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number encapsulation*]

**Release Information** Statement introduced before Release 11.2 of Junos OS.
This encapsulation is supported for Redundant Ethernet interface in Release 11.2 of Junos OS.

**Description** This encapsulation is used for underlying interfaces of pp0 interfaces. This encapsulation is supported on Fast Ethernet interface, Gigabit Ethernet interface, and Redundant Ethernet interface. When Redundant Ethernet interface is used as underlying interface, an existing pppoe session can be continued in case of failover.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

 Copyright © 2013, Juniper Networks, Inc.

## prefix

**Syntax** prefix [host-name logical-system-name routing-instance-name];

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client client-identifier]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify a prefix as a client identifier.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration

## profiles

**Syntax**
```
profiles {
  profile-name {
    sip-user-id simple-ip-user-id;
    sip-password simple-ip-password;
    access-point-name apn;
    authentication-method (pap | chap | none);
  }
}
```

**Hierarchy Level** [edit interfaces *interface-name* cellular-options gsm-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a profile to establish a data call with a Global System for Mobile Communications (GSM) cellular network. You can configure up to 16 profiles.

**Options** *profile-name*—Name of the profile.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Modem Interfaces
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## promiscuous-mode (Interfaces)

**Syntax** promiscuous-mode;

**Hierarchy Level** [edit interfaces *interface-name* ]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** Enable promiscuous mode on Layer 3 Ethernet interfaces. When promiscuous mode is enabled on an interface, all packets received on the interface are sent to the central point or Services Processing Unit regardless of the destination MAC address of the packet.

You can also enable promiscuous mode on chassis cluster redundant Ethernet interfaces and on aggregated Ethernet interfaces. If you enable promiscuous mode on a redundant Ethernet interface, promiscuous mode is then enabled on any child physical interfaces. If you enable promiscuous mode on an aggregated Ethernet interface, promiscuous mode is then enabled on all member interfaces.

**Required Privilege Level** **interface**—To view this statement in the configuration.
**interface-control**—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

## quality (Interfaces)

**Syntax** quality <*value*>;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* radio—router ]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** This option controls relative link quality weight (value 0–100).

**Required Privilege Level** **interface**—To view this statement in the configuration.
**interface-control**—To add this statement to the configuration.

**Related Documentation**
- Interfaces Overview


Copyright © 2013, Juniper Networks, Inc.

## radio-router (Interfaces)

**Syntax**

```
radio-router {
bandwidth;
   credit {
   interval;
   }
   latency;
   quality;
   resource;
threshold;
}
```

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number*]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** Point-to-Point Protocol over Ethernet (PPPoE)-based radio-to-router protocols include messages that define how an external system will provide the device with timely information about the quality of a link's connection. They also include a flow control mechanism to indicate how much data the device can forward. The device can then use the information provided in the PPPoE messages to dynamically adjust the interface speed of PPP links.

**Options** The remaining statements are explained separately.

**Required Privilege Level** **interface**—To view this statement in the configuration.
**interface-control**—To add this statement to the configuration.

**Related Documentation**

- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## redundancy-group (Interfaces)

**Syntax** **redundancy-group** *number* ;

**Hierarchy Level** **[edit interfaces** *interface-name* **redundant-ether-options]**

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Specify the redundancy group that a redundant Ethernet interface belongs to.

**Options** *number* —Number of the redundancy group that the redundant interface belongs to. Failover properties of the interface are inherited from the redundancy group.

**Range:** 1 through 255

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## redundant-ether-options

**Syntax**

```
redundant-ether-options {
  (flow-control | no-flow-control);
  lacp {
    (active | passive);
    periodic (fast | slow);
  }
  link-speed speed;
  (loopback | no-loopback);
  minimum-links number;
  redundancy-group number;
  source-address-filter mac-address;
  (source-filtering | no-source-filtering);
}
```

**Hierarchy Level** [edit interfaces *interface-name*]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Configure Ethernet redundancy options for a chassis cluster.

**Options** The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

## redundant-parent (Interfaces Fast Ethernet)

**Syntax** redundant-parent *interface-name* ;

**Hierarchy Level** [edit interfaces *interface-name* fastether-options]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Configure Fast Ethernet-specific interface properties for Ethernet redundancy in a chassis cluster.

**Options** ***interface*** —Parent redundant interface of the Fast Ethernet interface.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## redundant-parent (Interfaces Gigabit Ethernet)

**Syntax** redundant-parent *interface-name* ;

**Hierarchy Level** [edit interfaces *interface-name* gigether-options]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Configure Gigabit Ethernet-specific interface properties for Ethernet redundancy in a chassis cluster.

**Options** ***interface*** —Parent redundant interface of the Gigabit Ethernet interface.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

## resource (Interfaces)

**Syntax** resource <*value*>;

**Hierarchy Level** [edit interfaces *interface-name* radio—router ]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** This option controls the resource weight (value 1–100).

**Required Privilege Level** **interface**—To view this statement in the configuration.
**interface-control**—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## retransmission-attempt

**Syntax** retransmission-attempt *number*;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family inet dhcp]

**Release Information** Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** Specify the number of times the device retransmits a Dynamic Host Control Protocol (DHCP) packet if a DHCP server fails to respond. After the specified number of attempts, no further attempts at reaching a server are made.

**Options** *number*—Number of retransmit attempts..

**Range:** 0 through 6

**Default:** 4

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Configuring a DHCP Client (CLI Procedure)
- Interfaces for Security Devices

## retransmission-attempt (dhcp-client)

**Syntax** retransmission-attempts *number*;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the number of times the device attempts to retransmit a Dynamic Host Control Protocol (DHCP) packet fallback.

**Options** **number**—Number of attempts to retransmit the packet.

**Range**: 0 through 6

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration

Copyright © 2013, Juniper Networks, Inc.

## retransmission-interval (dhcp-client)

**Syntax** retransmission-interval *seconds*;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family *family*dhcp-client]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the time between successive retransmission attempts.

**Options** **seconds**—Number of seconds between successive retransmission attempts.

**Range**: 4 through 64 seconds

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration

## retransmission-interval (Interfaces)

**Syntax** retransmission-interval ***seconds***;

**Hierarchy Level** [edit **interfaces** ***interface-name*** unit ***logical-unit-number*** family *family-name* dhcp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the time between successive retransmission attempts.

**Options** ***seconds*** —Number of seconds between successive retransmission.
**Range:** 4 through 64 seconds
**Default:** 4 seconds

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## roaming-mode

**Syntax** **roaming-mode (home-only | automatic)**

**Hierarchy Level** **[edit interfaces *interface-name* cellular-options]**

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Specify whether the 3G wireless modem interface can access networks other than the home network.

**Options**
- **home-only**—No roaming is allowed.
- **automatic**—Allows access to networks other than the home network. This is the default.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Modem Interfaces
- Interfaces for Security Devices

## select-profile

**Syntax** **select-profile *profile-name***

**Hierarchy Level** **[edit interfaces *interface-name* cellular-options gsm-options]**

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Select the active profile to establish a data call with a Global System for Mobile Communications (GSM) cellular network.

**Options** ***profile-name***—Name of a configured profile that is to be used to establish a data call.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Modem Interfaces
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## server-address

**Syntax** server-address *ip-address*;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family inet dhcp]

**Release Information** Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** Specify the address of the DHCP server that the client should accept DHCP offers from. If this option is included in the DHCP configuration, the client accepts offers only from this server and ignores all other offers.

**Default** The client accepts the first offer it receives from any DHCP server.

**Options** ***ip-address***—DHCP server address.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Configuring a DHCP Client (CLI Procedure)
- Interfaces for Security Devices

## server-address (dhcp-client)

**Syntax** server address *ip-address*;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the preferred DHCP server address that is sent to DHCP clients.

**Options** **ip-address**—DHCP server address.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

## simple-filter (Interfaces)

**Syntax**

```
simple-filter{
  input filter-name;
}
```

**Hierarchy Level** [edit interfaces *interfaces-name* unit *logical-unit-number* family *family-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Apply a simple filter to an interface. You can apply simple filters on ingress interfaces only.

**Options** input ***filter-name***: Name of one filter to evaluate when packets are received on the interface.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Interfaces for Security Devices

## sip-password

**Syntax** sip-password *simple-ip-password*;

**Hierarchy Level** [edit interfaces *interface-name* cellular-options gsm-options profiles *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure the password provided by the service provider for connection to a Global System for Mobile Communications (GSM) cellular network.

**Options** ***simple-ip-password***—Password.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Modem Interfaces
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## sip-user-id

**Syntax** **sip-user-id** *simple-ip-user-id*;

**Hierarchy Level** **[edit interfaces** *interface-name* **cellular-options gsm-options profiles** *profile-name***]**

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure the username provided by the service provider for connection to a Global System for Mobile Communications (GSM) cellular network.

**Options** ***simple-ip-user-id***—Username.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Modem Interfaces
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## source-address-filter (Interfaces)

**Syntax** source-address-filter *mac-address* ;

**Hierarchy Level** [edit interfaces *interface-name* redundant-ether-options]

**Release Information** Statement modified in Release 9.0 of Junos OS.

**Description** For redundant Ethernet interfaces, specify the MAC addresses from which the interface can receive packets. For this statement to have any effect, you must include the **source-filtering** statement in the configuration to enable source address filtering.

Be sure to update the MAC address if the remote Ethernet card is replaced. Replacing the interface card changes the MAC address. Otherwise, the interface cannot receive packets from the new card.



NOTE:

- The source address filtering is not supported on the Gigabit Ethernet Interfaces on J Series devices.
- Software based MAC limiting is supported on SRX100, SRX210, SRX220, SRX240, and SRX650 devices.

  A maximum of 32 devices are supported per device.

**Options** ***mac-address*** —MAC address filter. You can specify the MAC address as six hexadecimal bytes in one of the following formats: ***nn:nn:nn:nn:nn:nn*** (for example, **00:11:22:33:44:55**) or ***nnnn:nnnn:nnnn*** (for example, **0011.2233.4455**). You can configure up to 64 source addresses. To specify more than one address, include multiple ***mac-address*** options in the **source-address-filter** statement.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## source-filtering (Interfaces)

**Syntax** **(source-filtering | no-source-filtering);**

**Hierarchy Level** **[edit interfaces *interface-name* redundant-ether-options]**

**Release Information** Statement modified in Release 9.0 of Junos OS.

**Description** For redundant Ethernet interfaces, enable the filtering of MAC source addresses, which blocks all incoming packets to that interface. To allow the interface to receive packets from specific MAC addresses, include the **source-address-filter** statement.

If the remote Ethernet card is changed, the interface cannot receive packets from the new card because it has a different MAC address.

By default, source address filtering is disabled.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

## speed (Interfaces)

**Syntax** speed;

**Hierarchy Level** [edit interfaces *interface-name* speed]

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Configure the operating speed for the 2-Port 10 Gigabit Ethernet XPIM.

**Options**
- 100m — Link speed of 100 Mbps
- 10g — Link speed of 10 Gbps
- 10m — Link speed of 10 Mbps
- 1g — Link speed of 1 Gbps

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## threshold (Interfaces)

**Syntax** threshold <*value*>;

**Hierarchy Level** [edit interfaces *interface-name* radio–router ]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** This option controls the percentage of bandwidth change required for routing updates.

**Required Privilege Level** **interface**—To view this statement in the configuration.
**interface-control**—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

## traceoptions (Interfaces)

**Syntax** traceoptions

**Hierarchy Level** [edit interfaces interface-name traceoptions]

**Release Information** Command introduced in Release 10.1 of Junos OS.

**Description** Define tracing operations for individual interfaces. To specify more than one tracing operation, include multiple flag statements.

**Options** **flag** - Tracing parameters

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## unframed | no-unframed (Interfaces)

**Syntax** (unframed | no-unframed);

**Hierarchy Level** [edit interfaces *interface-name* t3-options]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Enable or disable framing for the T3 interface on a 1-Port Clear Channel DS3/E3 GPIM on an SRX650 device. By default, unframed mode is enabled. Select no-unframed to enable framing. Select unframed to return to the default mode.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices
- Feature Support Reference for SRX Series and J Series Devices

## update-server

**Syntax** update-server;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family inet dhcp]

**Release Information** Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** Propagate TCP/IP settings learned from an external DHCP server to the DHCP server running on the switch.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Configuring a DHCP Client (CLI Procedure)
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## update-server (dhcp-client)

**Syntax** update-server;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Propagate DHCP options to a local DHCP server.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration

## use-interface

**Syntax** use-interface-description {logical |device};

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client client-identifier]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** The description configured at the physical or logical interface level is used for client identification.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration

## user-id

**Syntax** user-id {ascii *ascii* hexadecimal *hexadecimal*};

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client client-identifier]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify an ASCII or hexadecimal user ID for the Dynamic Host Configuration Protocol (DHCP) client.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration

Copyright © 2013, Juniper Networks, Inc.

## vbr rate

**Syntax** vbr rate;

**Hierarchy Level** [edit interfaces interface-name atm-options vpi vpi-identifier shaping]

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** For ATM encapsulation only, define a variable bit rate bandwidth utilization in the traffic-shaping profile.

**Options**

- Burst Size–The maximum burst size that can be sent at the peak rate.
- Peak Rate–The maximum instantaneous rate at which the user will transmit.
- Sustained Rate–The average rate as measured over a long interval.
- CDVT–Cell Delay Variation Tolerance in microseconds (range: 1 – 9999).

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## vdsl-profile

**Syntax** vdsl-profile

**Hierarchy Level** [edit interfaces interface-name vdsl-options]

**Release Information** Command introduced in Release 10.1 of Junos OS.

**Description** Configure the type of VDSL2 profiles. A profile is a table that contains a list of preconfigured VDSL2 settings.

**Options**
- Auto (default)
- 8a
- 8b
- 8c
- 8d
- 12a
- 12b
- 17a

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

## vendor-id

**Syntax** vendor-id *vendor-id*;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Configure a vendor class ID for the Dynamic Host Configuration Protocol (DHCP) client.

**Options** **vendor-id**—Vendor class ID.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration

Copyright © 2013, Juniper Networks, Inc.

## vendor-id (Interfaces)

**Syntax** vendor-id *vendor-id* ;

**Hierarchy Level** [edit **interfaces** *interface-name* unit *logical-unit-number* family *family-name* dhcp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure a vendor class ID for the Dynamic Host Configuration Protocol (DHCP) client.

**Options** ***vendor-id*** —vendor class ID.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices

## vlan-tagging (Interfaces)

**Syntax** vlan-tagging native-vlan-id *vlan-id*;

**Hierarchy Level** [edit interfaces *interface* ]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure VLAN identifier for untagged packets received on the physical interface of a trunk mode interface.

**Options** **native-vlan-id**—Configures a VLAN identifier for untagged packets. Enter a number from 0 through 4094.

NOTE: **The native-vlan-id can be configured only when either flexible-vlan-tagging mode or interface-mode trunk is configured.**

**Required Privilege Level** **interface**—To view this statement in the configuration.
**interface-control**—To add this statement to the configuration.

**Related Documentation**
- Ethernet Port Switching for Security Devices
- Interfaces for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- Layer 2 Bridging and Switching for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## web-authentication (Interfaces)

**Syntax**

```
web-authentication {
  http;
  https;
  redirect-to-https;
}
```

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family *family-name* address *address* ]

**Release Information** Statement introduced in Junos OS Release 8.5. Support for **https** and **redirect-to-https** options added in Junos OS Release 12.1x44-D10.

**Description** Enable the Web authentication process for firewall user authentication.

**Options**

**http**—Enable HTTP service.

**https**—Enable authentication through HTTPS.

**redirect-to-https**—Redirect Web authentication to HTTPS.

**Required Privilege Level**

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 12

# Logical-Systems Hierarchy and Statement

This section includes the following topics:


- Logical-Systems Configuration Statement Hierarchy on page 223


## Logical-Systems Configuration Statement Hierarchy

To configure a logical system, use the configuration statements in the **logical-systems** configuration hierarchy. As indicated in the following hierarchy, you can include at this hierarchy level several of the hierarchies that can be included at the [**edit**] hierarchy level. However, some statements in a subhierarchy are not valid for logical systems. To learn which statements can be included on your device, issue the **set ?** command at the hierarchy level of interest.



NOTE: The **logical-systems** configuration hierarchy can only be used by the master administrator. Configuration statements in the other hierarchies can also be used by a user logical system administrator at the [edit] hierarchy level to configure their user logical system.

```
logical-systems {
  logical-system-name  {
    access{
      ...same statements as in several subhierarchies in [edit access] Hierarchy Level...
    }
    access-profile profile-name;
    applications {
      ...same statements as in [edit applications] Hierarchy Level...
    }
    firewall {
      ...same statements as in [edit firewall] Hierarchy Level...
    }
    policy-options {
      ...same statements as in [edit policy-options] Hierarchy Level...
    }
    routing-instance {
      ...most statements in [edit routing-instance] Hierarchy Level...
    }
    protocols {
      ...same statements as in [edit protocols] Hierarchy Level...
```

Copyright © 2013, Juniper Networks, Inc.

```
    }
    routing-options {
      ...most statements in [edit routing-options] Hierarchy Level...
    }
    schedulers {
      ...same statements as in the [edit schedulers] Hierarchy Level...
    }
    security {
      address-book {
        ... same statements as in [edit security address-book] Hierarchy Level...
      }
      application-firewall {
        ... same statements as in [edit security application-firewall] Hierarchy Level...
      }
      application-tracking {
        ... same statements as in [edit security application-tracking] Hierarchy Level...
      }
      firewall-authentication {
        ... same statements as in [edit security firewall-authentication] Hierarchy Level...
      }
      flow {
        ... same statements as in [edit security flow] Hierarchy Level...
      }
      nat {
        ... same statements as in [edit security nat] Hierarchy Level...
      }
      policies {
        ... same statements as in [edit security policies] Hierarchy Level...
      }
      screen {
        ... same statements as in [edit security screen] Hierarchy Level...
      }
      softwires {
        ... same statements as in [edit security softwires] Hierarchy Level...
      }
      zones {
        ... same statements as in [edit security zones] Hierarchy Level...
      }
    }
  }
}
```

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## logical-systems (All)

**Syntax**

```
logical-systems logical-system-name {
    ...
}
```

**Hierarchy Level** [edit]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Configure a logical system. Only the master administrator can configure a logical system at this hierarchy level.

At this hierarchy level, you can include several of the hierarchies that can be included at the [**edit**] hierarchy level. For descriptions of the applicable statements, see the appropriate hierarchies.



NOTE: The logical-systems configuration statement can only be used by the master administrator.

**Options** *logical-system-name*—Name of the logical system.

**Required Privilege Level** all—To view this statement in the configuration.
all—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 13

# Power Over Ethernet Hierarchy and Statements

This section contains the following topics:


- PoE Configuration Statement Hierarchy on page 227


## PoE Configuration Statement Hierarchy

To configure Power over Ethernet options, use the configuration statements in the **poe** configuration hierarchy. Statement descriptions that are exclusive to the J Series and SRX Series devices running Junos OS are described in this chapter.

```
poe {
   management type;
      guard-band watts;
      interface (all | interface-name) {
      disable ;
         maximum-power watts ;
         priority value;
         telemetries {
         disable;
            duration hours;
         interval minutes;
      }
   }
}
```

**Related Documentation**

- Ethernet Interfaces
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## disable (PoE)

**Syntax** disable

**Hierarchy Level** [edit poe interface (all | interface-name)],
[edit poe interface (all | interface-name) telemetries]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Disables the PoE capabilities of the port. If PoE capabilities are disabled for a port, the port operates as a standard network access port. If the disable statement is specified after the telemetries statement, logging of PoE power consumption for the port is disabled. To disable monitoring and retain the stored interval and duration values for possible future use, you can specify the disable sub statement in the sub stanza for telemetries. Similarly for retaining the port configuration but disabling the PoE feature on the port, disable can be used in sub stanza for interface.

**Default** The PoE capabilities are automatically enabled when a PoE interface is set. Specifying the telemetries statement enables monitoring of PoE per-port power consumption.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Ethernet Interfaces
- Interfaces for Security Devices

## duration (PoE)

**Syntax** duration hours;

**Hierarchy Level** [edit poe interface (all | interface-name) telemetries]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Modifies the duration for which telemetry records are stored. If telemetry logging continues beyond the specified duration, the older records are discarded one by one as new records are collected.

**Options** hours— Hours for which telemetry data should be retained.

**Range:** **Range** — 1 through 24 hours

**Default:** **Default**— 1 hour

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Ethernet Interfaces
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## guard-band (PoE)

**Syntax** guard-band watts;

**Hierarchy Level** [edit poe]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Reserves the specified amount of power for the SRX Series device in case of a spike in PoE consumption.

**Options** watts—Amount of power to be reserved for the SRX Series device in case of a spike in PoE consumption.

**Range:** **Range** — 0 through 19 W

**Default:** **Default**— 0 W

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Interfaces
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## interface (PoE)

**Syntax**

```
interface (all | interface-name) {
  disable;
    maximum-power watts;
    priority value;
    telemetries {
    disable;
      interval minutes;
    duration hours;
  }
}
```

**Hierarchy Level** [edit poe]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Enable a PoE interface for a PoE port. The PoE interface must be enabled in order for the port to provide power to a connected powered device.

**Default** The PoE interface is enabled by default

**Options**

- **all**— Apply the configuration to all interfaces on the SRX Series device that have not been explicitly configured otherwise.
- **interface-name**— Explicitly configure a specific interface.

**Required Privilege Level**

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
The remaining statements are explained separately.

**Related Documentation**

- Ethernet Interfaces
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## interval (PoE)

**Syntax** interval minutes;

**Hierarchy Level** [edit poe interface (all | interface-name) telemetries]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Modifies the interval for logging telemetries if you are monitoring the per-port power consumption for PoE interfaces.

**Options** minutes—Interval at which data is logged.

**Range:** **Range** —1 through 30 minutes

**Default:** **Default** — 5 minutes

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Interfaces
- Interfaces for Security Devices

## management (PoE)

**Syntax** management type;

**Hierarchy Level** [edit poe]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Designates how the SRX Series device allocates power to the PoE ports.

**Default** static

**Options**

- type—Management type:
- **static**—When a powered device is connected to a PoE port, the power allocated to it is equal to the maximum power configured for the port.
- **class**—When a powered device is connected to a PoE port, the power allocated to it is equal to the maximum power for the class as defined by the IEEE 802.3 AF standard.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Interfaces
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## maximum-power (PoE)

**Syntax** maximum-power watts;

**Hierarchy Level** [edit poe interface (all | interface-name)]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Maximum amount of power that can be supplied to the port

**Default** 15.4 W

**Options** **Watts**

**Range** —0 through 15.4

**Default**—15.4 W

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Interfaces
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## priority (PoE)

**Syntax** priority value;

**Hierarchy Level** [edit poe interface (all | interface-name)]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Sets the priority of individual ports. When it is not possible to maintain power to all connected ports, lower-priority ports are powered off before higher priority ports. When a new device is connected on a higher-priority port, a lower-priority port will be powered off automatically if available power is insufficient to power on the higher-priority port. Note that for ports with the same priority configuration, ports on the left are given higher priority than the ports on the right.

**Default** low

**Options** value—high or low:

- **high**—Specify that this port is to be treated as high priority in terms of power allocation
- **low**—Specify that this port is to be treated as low priority in terms of power allocation.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Interfaces
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## telemetries (PoE)

**Syntax**

```
telemetries {
  disable;
    duration hours;
  interval minutes;
}
```

**Hierarchy Level** [edit poe interface (all | interface-name)]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Allow logging of per-port PoE power consumption. The telemetries section must be explicitly specified to enable logging. If left unspecified, telemetries is disabled by default.

**Default** If the telemetries statement is specified, logging is enabled with the default values for interval and duration.

**Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- PoE Configuration Statement Hierarchy on page 227
- Ethernet Interfaces
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

CHAPTER 14

# Policy-Options Hierarchy and Statements

This section contains the following topics:


- Policy-Options Configuration Statement Hierarchy on page 235


## Policy-Options Configuration Statement Hierarchy

Use the statements in the **policy-options** configuration hierarchy to configure routing policies that control information from routing protocols that the device imports into its routing table and exports to its neighbors.

```
policy-options {
   as-path name regular-expression ;
   as-path-group group-name;
   community name {
      invert-match;
      members [ community-ids];
   }
   condition condition-name {
      if-route-exists address table table-name;
      route-active-on (node0 | node1);
   }
   damping name{
      disable;
      half-life minutes;
      max-suppress minutes;
      reuse number;
      suppress number;
   }
   policy-statement policy-name {
      term term-name {
         default-action (accept | reject);
         from {
            family family-name;
            match-conditions;
            multicast-scope (scope-value | global | link-local | node-local | organization-local
               | orhigher | orlower | site-local);
            policy subroutine- policy-name;
            prefix-list name;
            protocol {
               dvmrp;
               msdp;
```

Copyright © 2013, Juniper Networks, Inc.

```
            pim;
          }
          route-filter destination-prefix match-type < actions>;
          source-address-filter destination-prefix match-type <actions>;
        }
        to {
          match-conditions;
          policy subroutine- policy-name;
        }
        then actions;
      }
    }
    prefix-list name {
      ip-addresses;
    }
  }
```

**Related Documentation**

- Routing Policy Configuration Guide
- MPLS for Security Devices

## condition (Policy Options)

**Syntax**

```
condition condition-name {
  if-route-exists address table table-name ;
  route-active-on (node0 | node1);
}
```

**Hierarchy Level** [edit policy-options]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** For chassis cluster configurations, specify the match condition for use in routing to a redundant Ethernet (**reth**) interface.

**Options** *condition-name* —Name of the routing policy match condition.

The remaining statement is explained separately.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## load-balance (Security Devices)

**Syntax** load-balance per-packet

**Hierarchy Level** [edit policy-options policy-statement *policy-name* then]

**Release Information** Statement introduced before Release 12.1 of Junos OS.

**Description** Specify that multiple next hop entries in an equal-cost multipath (ECMP) set are installed in the forwarding table. On Juniper Networks security devices, source and destination IP addresses and protocols are examined to determine individual traffic flows. Packets for the same flow are forwarded on the same interface. The interface for a flow does not change when there are additions or changes to the ECMP set as long as the next hop associated with the interface remains in the ECMP set.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## multicast-scope

**Syntax** multicast-scope (*scope-value* | global | link-local | node-local | organization-local | orhigher | orlower | site-local);

**Hierarchy Level** [edit policy-options policy-statement *policy-name* from]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure multicast scoping to match the routing policy.

**Options**

- ***scope-value*** **<orhigher | orlower>**—The multicast-scope value is a number from 0 through 15.
- **global <orhigher | orlower>**—Global multicast scope
- **link-local <orhigher | orlower>**—Link-local scope
- **node-local <orhigher | orlower>**—Node-local scope
- **organization-local <orhigher | orlower>**—Organizational-local scope
- **orhigher**—Match on numerically higher scopes
- **orlower**—Match on numerically lower scopes
- **site-local <orhigher | orlower>**—Site-local values

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**

## route-active-on

**Syntax** route-active-on (node0 | node1);

**Hierarchy Level** [edit policy-options condition *condition-name* ]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** For chassis cluster configurations, identify the device (node) on which a route is active.

**Options** **node0** | **node1**—Node in a chassis cluster.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**

- Chassis Cluster for Security Devices


Copyright © 2013, Juniper Networks, Inc.

CHAPTER 15

# Protocols Hierarchy and Statements

This section contains the following topics:


- Protocols Configuration Statement Hierarchy on page 239


## Protocols Configuration Statement Hierarchy

Use the **protocols** configuration hierarchy statements to configure routing protocols, including End System-to-Intermediate System (ES-IS), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Routing Information Protocol Next Generation (RIPng), Border Gateway Protocol (BGP), and Layer 2 address learning and forwarding.

```
protocols {
  bfd {
    traceoptions {
      file filename <files number > <match regular-expression >
      <size maximum-file-size > <world-readable | no-world-readable>;
      flag flag ;
    }
  }
  bgp {
    accept-remote-nexthop;
    advertise-inactive;
    advertise-peer-as;
    authentication-algorithm algorithm ;
    authentication-key key ;
    authentication-key-chain key-chain ;
    bfd-liveness-detection {
      detection-time {
        threshold milliseconds ;
      }
      holddown-interval milliseconds;
      local-address ip-address ;
      minimum-interval milliseconds ;
      minimum-receive-interval milliseconds ;
      minimum-receive-ttl milliseconds ;
      multiplier number ;
      neighbor address ;
      transmit-interval {
        minimum-interval milliseconds ;
        threshold milliseconds ;
```

Copyright © 2013, Juniper Networks, Inc.

```
    }
    version (0 | 1);
  }
  cluster cluster-identifier;
  damping;
  description text-description ;
  disable;
  export [ policy-name ];
  family {
    (inet | inet-mvpn | inet-vpn | inet6 | inet6-mvpn | inet6-vpn | iso-vpn | l2-vpn) {
      (any | flow | multicast | unicast | signaling) {
        prefix-limit {
          maximum number ;
          teardown < percentage > <idle-timeout (forever | minutes )>;
        }
        rib-group group-name ;
      }
      labeled-unicast {
        aggregate-label {
          community community-name :
        }
        explicit-null {
          connected-only;
        }
        per-group-label;
        prefix-limit {
          maximum number ;
          teardown < percentage > <idle-timeout (forever | minutes )>;
        }
        resolve-vpn;
        rib inet.3;
        rib-group group-name ;
        traffic-statistics {
          file filename <files number > <match regular-expression >
          <size maximum-file-size > <world-readable | no-world-readable>;
          interval seconds ;
        }
      }
    }
    route-target {
      advertise-default;
      external-paths number ;
      prefix-limit {
        maximum number ;
        teardown < percentage > <idle-timeout (forever | minutes )>;
      }
    }
  }
  graceful-restart {
    disable;
    restart-time seconds ;
    stale-routes-time seconds ;
  }
  group group-name {
    bgp-options ;
    peer-as autonomous-system ;
```


Copyright © 2013, Juniper Networks, Inc.

```
    type type ;
    neighbor address ;
  }
  hold-time seconds ;
  import [ policy-name ];
  include-mp-next-hop;
  keep (all | none);
  local-address address ;
  local-as autonomous-system <private> <loops loops >;
  local-preference local-preference ;
  log-updown;
  metric-out ( metric | minimum-igp < offset > | igp < offset >);
  multihop < ttl-value >;
  no-advertise-peer-as;
  no-aggregator-id;
  no-client-reflect;
  out-delay seconds ;
  passive;
  path-selection {
    (always-compare-med | cisco-non-deterministic | external-router-id);
    med-plus-igp {
      igp-multiplier number ;
      med-multiplier number ;
    }
  }
  peer-as autonomous-system ;
  preference preference ;
  remove-private;
  tcp-mss segment-size ;
  traceoptions {
    file filename <files number >
    <size maximum-file-size > <world-readable | no-world-readable>;
    flag flag < flag-modifier > <disable>;
  }
  vpn-apply-export;
}
connections {
  interface-switch interface-switch-name {
    interface interface-name ;
  }
  lsp-switch lsp-switch-name {
    receive-lsp path-name ;
    transmit-lsp path-name ;
  }
  remote-interface-switch {
    interface interface-name ;
    receive-lsp path-name ;
    transmit-lsp path-name ;
  }
}
dot1x {
  authenticator {
    authentication-profile-name profile-name ;
    interface interface-name {
      guest-vlan vlan-name;
      mac-radius;
```

```
        maximum-requests request-number ;
        quiet-period seconds ;
        (reauthentication seconds | no-reauthentication);
        retries number ;
        server-fail deny | permit | use-cache | vlan vlan-name | vlan vlan-id;
        server-timeout seconds ;
        supplicant (multiple | single | single-secure);
        supplicant-timeout seconds ;
        transmit-period seconds ;
      }
      server-reject-vlan vlan-name | vlan-id;
      static mac-address {
        interface interface-name;
        vlan-assignment ( vlan-id | vlan-name);
      }
    }
    traceoptions {
      file filename <files number >
      <size maximum-file-size > <world-readable | no-world-readable>;
      flag flag <disable>;
    }
  }
  dvmrp {
    disable;
    export [ policy-name ];
    import [ policy-name ];
    interface interface-name {
      disable;
      hold-time seconds ;
      metric value ;
      mode (forwarding | unicast-routing);
    }
    rib-group group-name ;
    traceoptions {
      file filename <files number >
      <size maximum-file-size > <world-readable | no-world-readable>;
      flag flag < flag-modifier > <disable>;
    }
  }
  gvrp {
    disable;
    interface interface-name {
      disable;
    }
    join-timer milliseconds ;
    leave-timer milliseconds ;
    leaveall-timer milliseconds ;
  }
  igmp {
    accounting;
    interface interface-name {
      (accounting | no-accounting);
      disable;
      immediate-leave;
      promiscuous-mode;
      ssm-map ssm-map ;
```


Copyright © 2013, Juniper Networks, Inc.

```
    static {
      group group-address {
        source source-address ;
      }
    }
    version number ;
  }
  query-interval seconds ;
  query-last-member-interval seconds ;
  query-response-interval seconds ;
  robust-count robust-count ;
  traceoptions {
    file filename <files number > <size maximum-file-size >
    <world-readable | no-world-readable>;
    flag flag < flag-modifier > <disable>;
  }
}
igmp-snooping {
  traceoptions {
    file filename <files number > <size maximum-file-size >
    <world-readable | no-world-readable> <match regex>;
    flag flag ;
  }
  vlan ( vlan-id | vlan-number {
    disable;
    immediate-leave;
    interface interface-name {
      multicast-router-interface;
      static {
        group ip-address ;
      }
    }
    query-interval seconds ;
    query-last-member-interval seconds ;
    query-response-interval seconds ;
    robust-count number ;
  }
}
isis {
  clns-routing;
  disable;
  export [ policy-names ];
  graceful-restart {
    disable;
    helper-disable;
    restart-duration seconds ;
  }
  ignore-attached-bit;
  interface (all | interface-name ) {
    bfd-liveness-detection {
      detection-time {
        threshold milliseconds ;
      }
      minimum-interval milliseconds ;
      minimum-receive-interval milliseconds ;
      transmit-interval {
```

Copyright © 2013, Juniper Networks, Inc.

```
            minimum-interval milliseconds ;
            threshold milliseconds ;
          }
          multiplier number ;
          version (1 | automatic);
        }
        checksum;
        csnp-interval ( seconds | disable);
        disable;
        hello-padding (adaptive | loose | strict);
        ldp-synchronization {
          disable;
          hold-time seconds ;
        }
        level level-number {
          disable;
          hello-authentication-key key;
          hello-authentication-type authentication ;
          hello-interval seconds ;
          hold-time seconds ;
          ipv4-multicast-metric number ;
          ipv6-multicast-metric number ;
          ipv6-unicast-metric number ;
          metric metric ;
          passive;
          priority number ;
          te-metric metric ;
        }
        lsp-interval milliseconds ;
        mesh-group ( value | blocked);
        no-adjacency-down-notification;
        no-ipv4-multicast;
        no-ipv6-multicast;
        no-ipv6-unicast;
        no-unicast-topology;
        passive;
        point-to-point;
      }
      label-switched-path name level level metric metric ;
      level level-number {
        authentication-key key ;
        authentication-type authentication ;
        disable;
        external-preference preference ;
        no-csnp-authentication;
        no-hello-authentication;
        no-psnp-authentication;
        preference preference ;
        prefix-export-limit number ;
        wide-metrics-only;
      }
      loose-authentication-check;
      lsp-lifetime seconds ;
      no-adjacency-holddown;
      no-authentication-check;
      no-ipv4-routing;
```


Copyright © 2013, Juniper Networks, Inc.

```
    no-ipv6-routing;
    overload {
      advertise-high-metrics;
      timeout seconds ;
    }
    reference-bandwidth reference-bandwidth ;
    rib-group {
      inet group--name ;
      inet6 group--name ;
    }
    spf-options {
      delay milliseconds ;
      holddown milliseconds ;
      rapid-runs number ;
    }
    topologies {
      ipv4-multicast;
      ipv6-unicast;
    }
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
      flag flag < flag-modifier > <disable>;
    }
    traffic-engineering {
      disable;
      ipv4-multicast-rpf-routes;
      shortcuts <ignore-lsp-metrics>;
    }
  }
  l2-learning {
    global-mac-limit limit {
    packet-action-drop
    }
    global-mac-table-aging-time seconds;
    global-no-mac-learning;
  }
  l2circuit {
    local-switching {
      interface interface-name {
        description text-description ;
        end-interface {
          interface interface-name ;
          protect-interface interface-name ;
        }
        ignore-mtu-mismatch;
        protect-interface interface-name ;
      }
    }
    neighbor address {
      interface interface-name {
        bandwidth (ct0 class0 | ct1 class1 | ct2 class2 | ct3 class3 );
        community community ;
        (control-word | no-control-word);
        description text-description ;
        ignore-encapsulation-mismatch;
```

```
        mtu mtu ;
        protect-interface interface-name ;
        psn-tunnel-endpoint psn-tunnel-endpoint ;
        virtual-circuit-id circuit-id ;
      }
    }
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
      flag flag < flag-modifier > <disable>;
    }
  }
  lacp {
    traceoptions {
      file filename <files number > <match regular-expression >
      <size maximum-file-size > <world-readable | no-world-readable>;
      flag flag ;
    }
  }
  layer2-control {
    mac-rewrite {
      interface interface-name {
        protocol protocol-name ;
      }
    }
    nonstop-bridging {
      mac-rewrite {
        interface interface-name {
          protocol protocol-name ;
        }
      }
      traceoptions {
        file filename <files number >
        <size maximum-file-size > <world-readable | no-world-readable>;
        flag flag ;
      }
    }
    traceoptions {
      file filename <files number >
      <size maximum-file-size > <world-readable | no-world-readable>;
      flag flag ;
    }
  }
  ldp {
    (deaggregate | no-deaggregate);
    egress-policy [ policy-name ];
    explicit-null;
    export [ policy-name ];
    graceful-restart {
      disable;
      helper-disable;
      maximum-recovery-time seconds ;
      recovery-time seconds ;
    }
    import [ policy-name ];
    interface interface-name {
```


Copyright © 2013, Juniper Networks, Inc.

```
    disable;
    hello-interval seconds ;
    hold-time seconds ;
    transport-address (interface | router-id);
  }
  keepalive-interval seconds ;
  keepalive-timeout seconds ;
  l2-smart-policy;
  log-updown {
    trap {
      disable;
    }
  }
  next-hop {
    merged {
      policy [ policy-name ];
    }
  }
  no-forwarding;
  oam {
    bfd-liveness-detection {
      detection-time {
        threshold milliseconds ;
      }
      minimum-interval milliseconds ;
      minimum-receive-interval milliseconds ;
      multiplier number ;
      transmit-interval {
        minimum-interval milliseconds ;
        threshold milliseconds ;
      }
      version (0 | 1 | automatic);
    }
    fec class-address {
      (bfd-liveness-detection | no-bfd-liveness-detection);
      periodic-traceroute flags ;
    }
  }
  policing {
    fec class-address {
      ingress-traffic filter-name ;
      transit-traffic filter-name ;
    }
  }
  preference preference ;
  session session-address {
    authentication-algorithm algorithm ;
    authentication-key key ;
    authentication-key-chain key-chain ;
  }
  strict-targeted-hellos;
  traceoptions {
    file filename <files number > <size maximum-file-size >
    <world-readable | no-world-readable>;
    flag flag < flag-modifier > <disable>;
  }
```

Copyright © 2013, Juniper Networks, Inc.

```
    track-igp-metric;
    traffic-statistics {
      file filename <files number > < match regular-expression >
      <size maximum-file-size > <world-readable | no-world-readable>;
      interval seconds ;
      no-penultimate-hop;
    }
    transport-address (interface | router-id);
  }
  link-management {
    peer peer-name {
      address address ;
      control-channel [ control-channel-interfaces ];
      lmp-control-channel interface-name {
        remote-address address ;
      }
      lmp-protocol {
        hello-dead-interval milliseconds ;
        hello-interval milliseconds ;
        passive;
        retransmission-interval milliseconds ;
        retry-limit number ;
      }
      te-link [ te-link-names ];
    }
    te-link te-link-name {
      disable;
      interface interface-name {
        disable;
        local-address address ;
        remote-address address ;
        remote-id id-number ;
      }
      local-address address ;
      remote-address address ;
      remote-id id-number ;
      te-metric te-metric ;
    }
    traceoptions {
      file filename <files number> <size maximum-file-size>
      <world-readable | no-world-readable>;
      flag flag < flag-modifier > <disable>;
    }
  }
  mld {
    interface interface-name {
      disable;
      immediate-leave;
      ssm-map ssm-map ;
      static {
        group group-address {
          source source-address ;
        }
      }
      version number ;
    }
```


Copyright © 2013, Juniper Networks, Inc.

```
    query-interval seconds;
    query-last-member-interval seconds;
    query-response-interval seconds;
    robust-count robust-count;
    traceoptions {
      file filename <files number>
      <size maximum-file-size> <world-readable | no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
  }
  mpls {
    disable;
    admin-down;
    admin-group {
      exclude [ group-names ];
      include-all [ group-names ];
      include-any [ group-names ];
    }
    admin-groups {
      group-name group-value;
    }
    advertise-hold-time seconds;
    auto-policing {
      class all policer-action;
      class ctnumber (drop | loss-priority-high | loss-priority-low);
    }
    bandwidth bps;
    class-of-service cos-value;
    diffserv-te {
      bandwidth-model {
        extended-mam;
        mam;
        rdm;
      }
      te-class-matrix {
        tenumber {
          priority priority;
          traffic-class {
            ctnumber priority priority;
          }
        }
      }
    }
    expand-loose-hop;
    explicit-null;
    hop-limit number;
    icmp-tunneling;
    interface ( interface-name | all) {
      disable;
      admin-group {
        group-name;
      }
      label-map ( in-label | default-route) {
        class-of-service value;
        (discard | next-hop ( address | hostname | interface-name ) | reject);
        (pop | swap out-label );
```

```
      preference preference ;
      swap-push swap-label  push-label ;
    }
  }
  ipv6-tunneling;
  label-switched-path lsp-name {
    disable;
    adaptive;
    admin-down;
    admin-group {
      exclude [ group-names ];
      include-all [ group-names ];
      include-any [ group-names ];
    }
    associate-backup-pe-groups;
    auto-bandwidth {
      adjust-interval seconds ;
      adjust-threshold percent ;
      adjust-threshold-overflow-limit number ;
      maximum-bandwidth bps ;
      minimum-bandwidth bps ;
      monitor-bandwidth;
    }
    bandwidth bps ;
    class-of-service cos-value ;
    description;
    fast-reroute {
      bandwidth bps ;
      bandwidth-percent percent ;
      (exclude group-names | no-exclude);
      hop-limit number ;
      (include-all group-names | no-include-all);
      (include-any group-names | no-include-any);
    }
    from address ;
    hop-limit number ;
    install {
      destination-prefix / prefix-length <active>;
    }
    ldp-tunneling;
    link-protection;
    metric number ;
    no-cspf;
    no-decrement-ttl;
    no-install-to-address;
    node-link-protection;
    oam {
      bfd-liveness-detection {
        detection-time threshold milliseconds ;
        failure-action teardown;
        minimum-interval milliseconds ;
        minimum-receive-interval milliseconds ;
        multiplier detection-time-multiplier ;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds ;
```


Copyright © 2013, Juniper Networks, Inc.

```
        threshold milliseconds ;
      }
      version bfd-version ;
    }
    traceoptions {
      file filename <files number > <match regular-expression >
      <size maximum-file-size > <world-readable | no-world-readable>;
      flag flag ;
    }
  }
  optimize-timer seconds ;
  p2mp {
    path-name ;
  }
  policing {
    filter filter-name ;
    no-auto-policing;
  }
  preference preference ;
  primary path-name {
    adaptive;
    admin-down;
    admin-group {
      exclude [ group-names ];
      include-all [ group-names ];
      include-any [ group-names ];
    }
    bandwidth bps ;
    class-of-service cos-value ;
    hop-limit number ;
    no-cspf;
    no-decrement-ttl;
    oam {
      bfd-liveness-detection {
        detection-time threshold milliseconds ;
        failure-action teardown;
        minimum-interval milliseconds ;
        minimum-receive-interval milliseconds ;
        multiplier detection-time-multiplier ;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds ;
          threshold milliseconds ;
        }
        version bfd-version ;
      }
      traceoptions {
        file filename <files number > <match regular-expression >
        <size maximum-file-size > <world-readable | no-world-readable>;
        flag flag ;
      }
    }
    optimize-timer seconds ;
    preference preference ;
    priority setup-priority hold-priority ;
    (record | no-record);
```

```
    select {
      manual;
      unconditional;
    }
    standby;
  }
  priority setup-priority hold-priority ;
  (random | least-fill | most-fill);
  (record | no-record);
  retry-limit number ;
  retry-timer seconds ;
  revert-timer seconds ;
  secondary path-name {
    adaptive;
    admin-down;
    admin-group {
      exclude [ group-names ];
      include-all [ group-names ];
      include-any [ group-names ];
    }
    bandwidth bps ;
    class-of-service cos-value ;
    hop-limit number ;
    no-cspf;
    no-decrement-ttl;
    oam {
      bfd-liveness-detection {
        detection-time threshold milliseconds ;
        failure-action teardown;
        minimum-interval milliseconds ;
        minimum-receive-interval milliseconds ;
        multiplier detection-time-multiplier ;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds ;
          threshold milliseconds ;
        }
        version bfd-version ;
      }
      traceoptions {
        file filename <files number > <match regular-expression >
        <size maximum-file-size > <world-readable | no-world-readable>;
        flag flag ;
      }
    }
    optimize-timer seconds ;
    preference preference ;
    priority setup-priority hold-priority ;
    (record | no-record);
    select {
      manual;
      unconditional;
    }
    standby;
  }
  soft-preemption;
```


Copyright © 2013, Juniper Networks, Inc.

```
    standby;
    template;
    to address ;
    traceoptions {
      file filename <files number >
      <size maximum-file-size > <world-readable | no-world-readable>;
      flag flag ;
    }
  }
  log-updown {
    (syslog | no-syslog);
    (trap | no-trap (mpls-lsp-traps | rfc3812-traps) );
    trap-path-down;
    trap-path-up;
  }
  no-cspf;
  no-decrement-ttl;
  no-propagate-ttl;
  oam {
    bfd-liveness-detection {
      detection-time threshold milliseconds ;
      failure-action teardown;
      minimum-interval milliseconds ;
      minimum-receive-interval milliseconds ;
      multiplier detection-time-multiplier ;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds ;
        threshold milliseconds ;
      }
      version bfd-version ;
    }
    traceoptions {
      file filename <files number > <match regular-expression >
      <size maximum-file-size > <world-readable | no-world-readable>;
      flag flag ;
    }
  }
  optimize-aggressive;
  optimize-timer;
  path path-name {
    address <loose | strict>;
  }
  path-mtu {
    allow-fragmentation;
    rsvp {
      mtu-signaling;
    }
  }
  preference preference ;
  priority setup-priority hold-priority ;
  (record | no-record);
  revert-timer seconds ;
  rsvp-error-hold-time seconds ;
  smart-optimize-timer seconds ;
  standby;
```

Copyright © 2013, Juniper Networks, Inc.

```
    static-path inet {
      prefix {
        class-of-service value ;
        double-push bottom-value top-value ;
        next-hop ( address | interface-name );
        preference preference ;
        push out-label ;
        triple-push bottom-value middle-value top-value ;
      }
    }
    statistics {
      auto-bandwidth;
      file filename <files number> <size maximum-file-size >
      <world-readable | no-world-readable>;
      interval seconds ;
    }
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
      flag flag ;
    }
    traffic-engineering (bgp | bgp-igp | bgp-igp-both-ribs | mpls-forwarding);
  }
  msdp {
    msdp-options ;
  }
  mstp {
    bpdu-block-on-edge;
    bridge-priority priority ;
    configuration-name name ;
    disable;
    forward-delay seconds ;
    hello-time seconds ;
    interface interface-name {
      bpdu-timeout-action {
        alarm;
        block;
      }
      cost interface-cost ;
      disable;
      edge;
      mode (point-to-point | shared);
      no-root-port;
      priority interface-priority ;
    }
    max-age seconds ;
    max-hops number ;
    msti msti-id {
      bridge-priority priority ;
      interface interface-name {
        cost interface-cost ;
        disable;
        priority interface-priority ;
      }
      vlan [vlan-id];
    }
```


Copyright © 2013, Juniper Networks, Inc.

```
    revision-level number ;
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
      flag flag < flag-modifier > <disable>;
    }
  }
  neighbor-discovery {
    onlink-subnet-only ;
  }
  oam {
    ethernet {
      connectivity-fault-management {
        action-profile profile-name {
          default-actions {
            interface-down;
          }
        }
        linktrace {
          age (10s | 30s | 1m | 10m | 30m);
          path-database-size number ;
        }
        maintenance-domain domain-name {
          level number;
          name-format (character-string | dns | mac+2oct | none);
          maintenance-association association-name {
            continuity-check {
              hold-interval minutes ;
              interval (10m | 10s | 1m | 1s | 100ms);
              loss-threshold number ;
            }
            mep mep-id {
              auto-discovery;
              direction (up | down);
              interface interface-name ;
              priority number ;
              remote-mep mep-id {
                action-profile profile-name ;
              }
            }
            short-name-format (2octet | character-string | rfc-2685-vpn-id | vlan);
          }
        }
        traceoptions {
          file filename <files number > <match regular-expression >
          <size maximum-file-size > <world-readable | no-world-readable>;
          flag flag ;
        }
      }
      link-fault-management {
        action-profile profile-name {
          action {
            link-down;
            send-critical-event;
            syslog;
          }
```

```
            event {
              link-adjacency-loss;
              link-event-rate {
                frame-error count ;
                frame-period count ;
                frame-period-summary count ;
                symbol-period count ;
              }
              protocol-down;
            }
          }
          interface interface-name {
            apply-action-profile profile-name ;
            event-thresholds {
              frame-error count ;
              frame-period count ;
              frame-period-summary count ;
              symbol-period count ;
            }
            link-discovery (active | passive);
            negotiation-options {
              allow-remote-loopback;
              no-allow-link-events;
            }
            pdu-interval interval ;
            pdu-threshold threshold-value ;
          }
          traceoptions {
            file filename <files number > <match regular-expression >
            <size maximum-file-size > <world-readable | no-world-readable>;
            flag flag ;
          }
        }
      }
    }
    ospf {
      ospf-options ;
    }
    ospf3 {
      area area-id {
        area-range network/mask-length <restrict> <exact> <override-metric metric >;
        interface interface-name {
          disable;
          dead-interval seconds ;
          hello-interval seconds ;
          metric metric ;
          neighbor address <eligible>;
          passive;
          priority number ;
          retransmit-interval seconds ;
          transit-delay seconds ;
        }
        nssa {
          area-range network/mask-length <restrict> <exact>
          <override-metric metric >;
          default-lsa {
```


Copyright © 2013, Juniper Networks, Inc.

```
            default-metric metric ;
            metric-type type ;
            type-7;
          }
          (no-summaries | summaries);
        }
        stub <default-metric metric > <(no-summaries | summaries)>;
      }
      disable;
      export [ policy-names ];
      external-preference preference ;
      import [ policy-names ];
      overload {
        <timeout seconds >;
      }
      preference preference ;
      prefix-export-limit number ;
      reference-bandwidth reference-bandwidth ;
      rib-group group-name ;
      spf-options {
        delay milliseconds ;
        holddown milliseconds ;
        rapid-runs number ;
      }
      traceoptions {
        file filename <files number > <size maximum-file-size >
        <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
      }
    }
    pgm {
      pgm-options ;
    }
    pim {
      pim-options ;
    }
    ppp {
      ppp-options ;
    }
    rip {
      authentication-key password ;
      authentication-type type ;
      (check-zero | no-check-zero);
      graceful-restart {
        disable;
        restart-time seconds ;
      }
      group group-name {
        bfd-liveness-detection {
          detection-time {
            threshold milliseconds ;
          }
          minimum-interval milliseconds ;
          minimum-receive-interval milliseconds ;
          transmit-interval {
            minimum-interval milliseconds ;
```

```
            threshold milliseconds ;
          }
          multiplier number ;
          version (0 | 1 | automatic);
        }
        export [ policy-names ];
        metric-out metric ;
        preference preference ;
        route-timeout seconds ;
        update-interval seconds ;
        neighbor neighbor-name {
          authentication-key password ;
          authentication-type type ;
          bfd-liveness-detection {
            detection-time {
              threshold milliseconds ;
            }
            minimum-interval milliseconds ;
            minimum-receive-interval milliseconds ;
            transmit-interval {
              minimum-interval milliseconds ;
              threshold milliseconds ;
            }
            multiplier number ;
            version (0 | 1 | automatic);
          }
          (check-zero | no-check-zero);
          import [ policy-names ];
          message-size number ;
          metric-in metric ;
          receive receive-options ;
          route-timeout seconds ;
          send send-options ;
          update-interval seconds ;
        }
      }
      holddown seconds ;
      import [ policy-names ];
      message-size number ;
      metric-in metric ;
      receive receive-options ;
      rib-group group-name ;
      route-timeout seconds ;
      send send-options ;
      update-interval seconds ;
      traceoptions {
        file filename <files number > <size maximum-file-size >
        <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
      }
    }
    ripng {
      ripng-options ;
    }
    router-advertisement {
      router-advertisement-configuration ;
```


Copyright © 2013, Juniper Networks, Inc.

```
}
router-discovery {
  address address {
    (advertise | ignore);
    (broadcast | multicast);
    (priority number | ineligible);
  }
  disable;
  interface interface-name {
    lifetime seconds ;
    max-advertisement-interval seconds ;
    min-advertisement-interval seconds ;
  }
  traceoptions {
    file filename <files number > <size maximum-file-size >
    <world-readable | no-world-readable>;
    flag flag < flag-modifier > <disable>;
  }
}
rstp {
  bpdu-block-on-edge;
  bridge-priority priority ;
  disable;
  forward-delay seconds ;
  hello-time seconds ;
  interface interface-name {
    bpdu-timeout-action {
      alarm;
      block;
    }
    cost interface-cost ;
    disable;
    edge;
    mode (point-to-point | shared);
    no-root-port;
    priority interface-priority ;
  }
  max-age seconds ;
  traceoptions {
    file filename <files number > <size maximum-file-size >
    <world-readable | no-world-readable>;
    flag flag < flag-modifier > <disable>;
  }
}
rsvp {
  rsvp-options ;
}
sap {
  sap-options ;
}
stp {
  bpdu-block-on-edge;
  bridge-priority priority ;
  disable;
  forward-delay seconds ;
  hello-time seconds ;
```

```
    interface interface-name {
      bpdu-timeout-action {
        alarm;
        block;
      }
      cost interface-cost ;
      disable;
      edge;
      mode (point-to-point | shared);
      no-root-port;
      priority interface-priority ;
    }
    max-age seconds ;
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
      flag flag < flag-modifier > <disable>;
    }
  }
  vrrp {
    vrrp-options ;
  }
  vstp {
    disable;
    force-version stp;
    interface interface-name {
      bpdu-timeout-action {
        alarm;
        block;
      }
      cost cost ;
      edge;
      mode (p2p | shared);
      no-root-port;
      priority interface-priority ;
    }
    vlan vlan-id {
      bridge-priority priority ;
      forward-delay seconds ;
      hello-time seconds ;
      interface interface-name {
        bpdu-timeout-action {
          alarm;
          block;
        }
        cost cost ;
        edge;
        mode (p2p | shared);
        no-root-port;
        priority interface-priority ;
      }
      max-age seconds ;
      traceoptions {
        file filename <files number >
        <size maximum-file-size > <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
```


Copyright © 2013, Juniper Networks, Inc.

```
        }
      }
    }
  }
```

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- MPLS for Security Devices
- Junos OS Routing Protocols Configuration Guide
- Junos OS Services Interfaces Configuration Guide

## demand-circuit (Protocols RIP)

**Syntax** demand-circuit;

**Hierarchy Level**
[edit logical-systems *logical-system-name* protocols rip group *group-name*],
[edit logical-systems *logical-system-name* protocols rip group *group-name* neighbor *neighbor-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols rip group *group-name* neighbor *neighbor-name*],
[edit protocols rip group *group-name*],
[edit protocols rip group *group-name* neighbor *neighbor-name*],
[edit routing-instances *routing-instance-name* protocols rip group *group-name*],
[edit routing-instances *routing-instance-name* protocols rip group *group-name* neighbor *neighbor-name*]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Configure a neighboring interface to act as a RIP demand circuit. To complete the demand circuit, you must configure both ends of the pair as demand circuits. When configured, the device sends RIP information only when changes occur in the routing database.

**Default** Disabled. You must explicitly configure two neighboring interfaces to act as a RIP demand circuit.

**Required Privilege Level**
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring RIP Demand Circuits
- RIP Demand Circuits Overview
- max-retrans-time on page 265

Copyright © 2013, Juniper Networks, Inc.

## disable (Protocols R2CP)

**Syntax** disable;

**Hierarchy Level** [edit protocols r2cp]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Disable R2CP on the system.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- Interface Encapsulation

## global-mac-limit (Protocols)

**Syntax**
```
global-mac-limit limit {
  packet-action drop;
}
```

**Hierarchy Level** [edit protocols l2-learning]

**Release Information** Statement modified in Release 9.5 of Junos OS.

**Description** Limit the number of media access control (MAC) addresses learned from the logical interfaces on the router.

**Default** 131071 MAC addresses

**Options** ***limit***—Number of MAC addresses that can be learned on the device.

**Range:** 20 through 131071 addresses

The remaining statement is explained separately.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- Layer 2 Bridging and Transparent Mode for Security Devices
- Layer 2 Bridging and Switching for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## global-mac-table-aging-time (Protocols)

**Syntax** global-mac-table-aging-time *seconds*;

**Hierarchy Level** [edit protocols l2-learning]

**Release Information** Statement modified in Release 9.5 of Junos OS.

**Description** Configure the timeout interval for entries in the MAC table.

**Default** 300 seconds

**Options** ***seconds***—Time elapsed before MAC table entries are timed out and entries are deleted from the table.

**Range:** 10 through 64000 seconds

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- Layer 2 Bridging and Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices

## global-no-mac-learning (Protocols)

**Syntax** global-no-mac-learning;

**Hierarchy Level** [edit protocols l2-learning]

**Release Information** Statement modified in Release 9.5 of Junos OS.

**Description** Disable MAC learning for the entire device.

**Default** MAC learning is enabled.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- Layer 2 Bridging and Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## interface (Protocols R2CP)

**Syntax** interface *interface-name* unit *unit*

**Hierarchy Level** [edit protocols r2cp radio *radio-name*]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the interface that receives R2CP messages.

**Options** ***interface-name***—Name of the radio interface.

***unit***—Radio unit number.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- R2CP Radio-to-Router Protocol Overview
- Interfaces for Security Devices

## l2-learning (Protocols)

**Syntax**
```
l2-learning {
  global-mac-limit limit {
  packet-action-drop
  }
  global-mac-table-aging-time seconds;
  global-no-mac-learning;
}
```

**Hierarchy Level** [edit protocols]

**Release Information** Statement modified in Release 9.5 of Junos OS.

**Description** Configure Layer 2 address learning and forwarding properties globally.

The statements are explained separately.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- Layer 2 Bridging and Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## max-retrans-time

**Syntax** max-retrans-time *seconds*;

**Hierarchy Level**
[edit logical-systems *logical-system-name* protocols rip group *group-name*],
[edit logical-systems *logical-system-name* protocols rip group *group-name* neighbor *neighbor-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols rip group *group-name* neighbor *neighbor-name*],
[edit protocols rip group *group-name*],
[edit protocols rip group *group-name* neighbor *neighbor-name*],
[edit routing-instances *routing-instance-name* protocols rip group *group-name*],
[edit routing-instances *routing-instance-name* protocols rip group *group-name* neighbor *neighbor-name*]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** RIP demand circuits send update messages every 5 seconds to an unresponsive peer. Configure the retransmission timer to limit the number of times the demand circuit resends update messages to an unresponsive peer. If the configured retransmission threshold is reached, routes from the next hop router are marked as unreachable and the hold-down timer starts. You must configure a pair of RIP demand circuits for this timer to take effect.

To determine the number of times to resend the update message, use the following calculation:

5 seconds * number of retransmissions = retransmission seconds

**Options** *seconds*—The total amount of time the demand circuit resends update messages to an unresponsive peer. The seconds range corresponds to sending an update message a minimum of 1 time (5 seconds) and a maximum of 36 times (180 seconds).

**Range:** 5 through 180 seconds

**Default:** 5 seconds

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring RIP Demand Circuits
- RIP Demand Circuits Overview
- demand-circuit on page 261

Copyright © 2013, Juniper Networks, Inc.

## neighbor-discovery

**Syntax**

```
neighbor-discovery {
  onlink-subnet-only;
}
```

**Hierarchy Level** [edit protocols]

**Release Information** Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 11.3 for SRX Series devices.

**Description** Configures neighbor discovery to be set up between nodes that fall under same IPv6 subnet.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

## node-terminate-count

**Syntax** node-terminate-count *count*;

**Hierarchy Level** [edit protocols r2cp]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the number of node terminate retransmits attempted when a node terminate ACK has not been received before radio/router adjacency is terminated.

**Options** ***count***—Number of node terminate retransmits

**Range:** 1 through 5

**Default:** 3

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**

- R2CP Radio-to-Router Protocol Overview
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## node-terminate-interval

**Syntax** node-terminate-interval *interval*;

**Hierarchy Level** [edit protocols r2cp]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the interval between node terminate retransmits.

**Options** ***interval***—Interval in milliseconds.
**Range:** 100 through 5000
**Default:** 1000

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- R2CP Radio-to-Router Protocol Overview

## onlink-subnet-only

**Syntax** onlink-subnet-only

**Hierarchy Level** [edit protocols neighbor-discovery]

**Release Information** Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 11.3 for SRX Series devices.

**Description** Enable this option to prevent the device from responding to a Neighbor Solicitation (NS) from a prefix which was not included as one of the device interface prefixes.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Copyright © 2013, Juniper Networks, Inc.

## packet-action (Protocols)

**Syntax** packet-action drop;

**Hierarchy Level** [edit protocols l2-learning global-mac-limit *limit*]

**Release Information** Statement modified in Release 9.5 of Junos OS.

**Description** Specify that packets for new source MAC addresses be dropped after the MAC address limit is reached.

**Default** Disabled. The default is for packets for new source MAC addresses to be forwarded after the MAC address limit is reached.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- Layer 2 Bridging and Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices

## preference (Protocols ES-IS)

**Syntax** preference *preference*;

**Hierarchy Level** [edit protocols esis],
[edit routing-instances *routing-instance-name* protocols esis]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the ES-IS preference value.

**Options** ***preference***—Preference value.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- Layer 2 Bridging and Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## r2cp

**Syntax**

```
r2cp {
    {enable | disable};
    traceoptions {
        flag flags;
        file filename;
    }
    server-port port-number;
    node-terminate-count count;
    node-terminate-interval interval;
    session-terminate-count count;
    session-terminate-interval interval;
    radio radio-name {
        interface interface unit unit-number;
        radio-interface interface unit number;
        virtual-channel-group vc-group;
    }
}
```

**Hierarchy Level** [edit protocols]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the network interfaces that are used for protocol updates. By default, the protocol is disabled on all interfaces.

**Options** The statements are explained separately.

**Required Privilege Level**
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- R2CP Radio-to-Router Protocol Overview

Copyright © 2013, Juniper Networks, Inc.

## radio

**Syntax**

```
radio radio-name {
  interface interface unit unit-number;
  virtual-channel-group vc-group-name;
  radio-interface interface unit number;
}
```

**Hierarchy Level** [edit protocols r2cp]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the arbitrary name that describes the R2CP radio that exchanges messages and listens for acknowledgements. The interfaces and radio interfaces must reference the same Ethernet port for a particular radio. In addition, the logical interface configured by the radio interface can only be referenced by a single radio.

**Options** ***radio-name***—Name of the R2CP radio.

The remaining statements are explained separately.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**

- R2CP Radio-to-Router Protocol Overview

## radio-interface

**Syntax** radio-interface *interface* unit *unit*;

**Hierarchy Level** [edit protocols r2cp radio *radio-name*]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the attributes that identify the VLANs managed through the R2CP protocol.

**Options** ***interface***—Name of the interface.

***unit***—Unit number.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**

- R2CP Radio-to-Router Protocol Overview
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## server-port

**Syntax** server-port *port-number*;

**Hierarchy Level** [edit protocols r2cp]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the R2CP server that exchanges messages and listens for acknowledgements.

**Options** ***port-number***—Number of the server port.
**Default:** UDP port 28762

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- R2CP Radio-to-Router Protocol Overview
- Interfaces for Security Devices

## session-terminate-count

**Syntax** session-terminate-count *count*;

**Hierarchy Level** [edit protocols r2cp radio]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the number of Session Terminate retransmits to be attempted when a Session Terminate ACK has not been received before the session terminated.

**Options** ***count***—Number of session terminate retransmits
**Range:** 1 through 5
**Default:** 3

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- R2CP Radio-to-Router Protocol Overview
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## session-terminate-interval

**Syntax** session-terminate-interval *interval*;

**Hierarchy Level** [edit protocols r2cp]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the interval between Session Terminate retransmits.

**Options** ***interval***—Interval in milliseconds
**Range:** 100 through 5000
**Default:** 1000

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- R2CP Radio-to-Router Protocol Overview
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Protocols ES-IS)

**Syntax**

```
traceoptions {
  file filename <files number> <size maximum-file-size> <world-readable |
    no-world-readable>;
  flag flag <flag-modifier> <disable>;
}
```

**Hierarchy Level**

[edit protocols esis],
[edit routing-instances *routing-instance-name* protocols esis]

**Release Information**

Statement introduced in Release 8.5 of Junos OS.

**Description**

Configure ES-IS protocol-level tracing options.

To specify more than one tracing operation, include multiple flag statements.

**Default**

The default ES-IS protocol-level tracing options are those inherited from the routing protocols **traceoptions** statement included at the **[edit routing-options]** hierarchy level.

**Options**

- **disable**—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as **all**.
- **file *filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. We recommend that you place ES-IS tracing output in the file **esis-log**.
- **files *number***—(Optional) Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
- If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

  **Range:** 2 through 1000 files
  **Default:** 2 files

- ***flag***—Tracing operation to perform. To specify more than one flag, include multiple **flag** statements.

  **ES-IS Tracing Flags**

  - **error**—Errored ES-IS packets
  - **esh**—End-System hello packets
  - **graceful-restart**—Graceful restart events
  - **ish**—Intermediate-System hello packets

  **Global Tracing Flags**

Copyright © 2013, Juniper Networks, Inc.

- **all**—All tracing operations
- **general**—A combination of the **normal** and **route** trace operations
- **normal**—All normal operations, including adjacency changes

**Default:** If you do not specify this option, only unusual or abnormal operations are traced.

- **policy**—Policy operations and actions
- **route**—Routing table changes
- **state**—State transitions
- **task**—Interface transactions and processing
- **timer**—Timer usage
- ***flag-modifier***—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:
  - **detail**—Detailed trace information
  - **receive**—Packets being received
  - **send**—Packets being transmitted
- **no-world-readable**—(Optional) Prevent any user from reading the log file.
- **size *maximum-file-size***—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the ***trace-file*** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
- If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**Syntax:** ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB
**Range:** 10 KB through the maximum file size supported on your system
**Default:** Default: 1 MB

- **world-readable**—(Optional) Allow any user to read the log file.

**Required Privilege Level**
routing and trace—To view this statement in the configuration.
routing-control and trace-control—To add this statement to the configuration.

**Related Documentation**
- Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Protocols R2CP)

**Syntax**

```
traceoptions {
    file filename;
    flag flag;
}
```

**Hierarchy Level** [edit protocols r2cp]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the trace options for R2CP.

**Options** **file *filename***—Name of the file to receive the output of the tracing operation.

**flag *flag***—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—All tracing operations
- **configuration**—Configuration operations
- **event**—All tracing events
- **interface**—Interface operations
- **node**—Node events
- **packet**—Packet events
- **rtsock** —Routing socket operations
- **session**—Session events
- **socket**—Socket events
- **timer**—Timer events
- **virtual-channel**—Virtual channel events

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**

- R2CP Radio-to-Router Protocol Overview
- Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## virtual-channel-group

**Syntax** virtual-channel-group *vc-group*;

**Hierarchy Level** [edit protocols r2cp radio *radio-name*]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the virtual channel group that is used when allocating a virtual circuit for each learned MAC address.

**Options** ***vc-group***—Name of virtual channel group.

**Required Privilege Level** routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- R2CP Radio-to-Router Protocol Overview


Copyright © 2013, Juniper Networks, Inc.

CHAPTER 16

# Routing-Instances Hierarchy

This section contains the following topics:


- Routing-Instances Configuration Statement Hierarchy on page 277


## Routing-Instances Configuration Statement Hierarchy

Use the statements in the **routing-instances** configuration hierarchy to configure routing instances.

```
routing-instances {
  routing-instance-name {
    description text ;
    forwarding-options{
      accounting group-name {
        output {
          aggregate-export-interval seconds ;
          cflowd hostname {
            aggregation {
              autonomous-system;
              destination-prefix;
              protocol-port;
              source-destination-prefix {
                caida-compliant;
              }
              source-prefix;
            }
            autonomous-system-type (origin | peer);
            port port-number ;
            version number ;
          }
        }
      }
      family {
        inet filter (input filter-name | output filter-name);
        inet6 filter (input filter-name | output filter-name);
        mpls filter (input filter-name | output filter-name);
        vpls (filter input filter-name | flood input filter-name);
      }
      helpers {
        bootp {
          client-response-ttl value ;
```

Copyright © 2013, Juniper Networks, Inc.

```
    description text ;
    interface interface-name {
      client-response-ttl value ;
      description text ;
      maximum-hop-count number ;
      minimum-wait-time seconds ;
      no-listen;
      server address {
        routing-instance [ value ];
      }
      vpn;
    }
    maximum-hop-count number ;
    minimum-wait-time seconds ;
    relay-agent-option;
    server address {
      routing-instance [ value ];
    }
    vpn;
  }
  domain {
    description text ;
    interface interface-name {
      description text ;
      no-listen;
      server address {
        routing-instance [ value ];
      }
    }
    server address {
      routing-instance [ value ];
    }
  }
  port port-number {
    description text ;
    interface interface-name {
      description text ;
      no-listen;
      server address {
        routing-instance [ value ];
      }
    }
    server address {
      routing-instance [ value ];
    }
  }
  tftp {
    description text ;
    interface interface-name {
      description text ;
      no-listen;
      server address {
        routing-instance [ value ];
      }
    }
    server address {
```


Copyright © 2013, Juniper Networks, Inc.

```
        routing-instance [ value ];
      }
    }
    traceoptions {
      file filename <files number > <match regular-expression >
      <size maximum-file-size >
      <world-readable | no-world-readable>;
      flag {
        address;
        all;
        bootp;
        config;
        domain;
        ifdb;
        io;
        main;
        port;
        rtsock;
        tftp;
        trace;
        ui;
        util;
      }
      level match-level ;
    }
  }
  packet-capture {
    disable;
    file filename <files number > <size maximum-file-size >
    <world-readable | no-world-readable>;
    maximum-capture-size size ;
  }
  sampling {
    disable;
    family (inet | inet6 | mpls ) {
      disable;
      output {
        extension-service name;
        file;
        flow-server name {
          aggregation {
            source-destination;
          }
        }
      }
    }
    input {
      max-packets-per-second number;
      rate number ;
      run-length number ;
    }
    traceoptions {
      file filename <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
    }
  }
```

Copyright © 2013, Juniper Networks, Inc.

```
instance-type (forwarding | l2vpn | no-forwarding | virtual-router | vpls | vrf);
interface interface-name ;
multicast-snooping-options {
  flood-groups [ value ];
  forwarding-cache {
    threshold (suppress | reuse) value value ;
    timeout minutes ;
  }
  options {
    syslog {
      level level | upto level ;
      mark seconds;
    }
  }
}
no-local-switching;
no-vrf-advertise;
protocols {
  bgp {
    bgp-configuration ;
  }
  esis {
    esis-configuration ;
  }
  isis {
    isis-configuration ;
  }
  l2vpn {
    l2vpn-configuration ;
  }
  ldp {
    ldp-configuration ;
  }
  msdp {
    msdp-configuration;
  }
  ospf {
    domain-id domain-id ;
    domain-vpn-tag number ;
    route-type-community (vendor | iana);
    ospf-configuration ;
  }
  ospf3 {
    domain-id domain-id ;
    domain-vpn-tag number ;
    route-type-community (vendor | iana);
    ospf3-configuration ;
  }
  pim {
    mdt {
      group-range multicast-prefix ;
      threshold {
        group group-address {
          source source-address {
            rate threshold-rate ;
          }
```


Copyright © 2013, Juniper Networks, Inc.

```
            }
          }
          tunnel-limit limit ;
        }
        pim-configuration ;
      }
      rip {
        rip-configuration ;
      }
      ripng {
        ripng-configuration;
      }
      router-discovery {
        router-discovery-configuration ;
      }
      vpls
        mesh-group mesh-group-name {
          associate-profile {
            profile-variable-set variable-set;
          }
          local-switching;
          mac-flush {
            (any-interface | any-spoke);
            propagate;
          }
          neighbor {
            associate-profile profile-name {
              profile-variable-set variable-set;
            }
            backup-neighbor neighbor-id;
            community;
            connection-protection;
            encapsulation-type;
            ignore-encapsulation-mismatch;
            pseudowire-status-tlv;
            psn-tunnel-endpoint;
            revert-time;
            static (incoming-label | Outgoing-label);
            switchover-delay;
          }
          peer-as {
            all;
          }
          route-distinguisher rd-type;
          vpls-id rd-type;
      }
    }
    provider-tunnel {
      pim-asm {
        group-address group-address ;
      }
      rsvp-te {
        label-switched-path-template (default | lsp-template-name );
        static-lsp p2mp-lps-name ;
      }
      selective {
```

```
    group group-prefix ;
    tunnel-limit number ;
  }
}
route-distinguisher ( as-number : number | ip-address : number );
routing-options {
  aggregate {
    defaults {
      aggregate-options ;
    }
    route destination-prefix {
      aggregate-options ;
      policy policy-name ;
    }
  }
  auto-export {
    (disable | enable);
    family {
      inet {
        disable;
        flow {
          (disable | enable);
          rib-group rib-group ;
        }
        multicast {
          (disable | enable);
          rib-group rib-group ;
        }
        unicast {
          (disable | enable);
          rib-group rib-group ;
        }
      }
      inet6 {
        disable;
        multicast {
          (disable | enable);
          rib-group rib-group ;
        }
        unicast {
          (disable | enable);
          rib-group rib-group ;
        }
      }
      iso {
        disable;
        unicast {
          (disable | enable);
          rib-group rib-group ;
        }
      }
    }
    traceoptions {
      file filename <files number >
      <size maximum-file-size >
      <world-readable | no-world-readable>;
```


Copyright © 2013, Juniper Networks, Inc.

```
      flag flag < flag-modifier > <disable>;
    }
  }
  autonomous-system autonomous-system <loops number > {
    independent-domain;
  }
  fate-sharing {
    group group-name {
      cost value ;
      from address {
        to address ;
      }
    }
  }
  flow {
    route name {
      match {
        match-conditions ;
      }
      then {
        actions ;
      }
    }
    validation {
      traceoptions {
        file filename <files number >
        <size maximum-file-size >
        <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
      }
    }
  }
  forwarding-table {
    unicast-reverse-paths (active-paths | feasible-paths);
  }
  generate {
    defaults {
      generate-options ;
    }
    route destination-prefix {
      generate-options ;
      policy policy-name ;
    }
  }
  graceful-restart {
    disable;
    restart-duration duration ;
  }
  instance-export [ policy-names ];
  instance-import [ policy-names ];
  interface-routes {
    family (inet | inet6) {
      import [ import-policies ];
      export {
        lan;
        point-to-point;
```

```
    }
  }
  rib-group {
    inet group-name ;
    inet6 group-name ;
  }
}
martians {
  destination-prefix  match-type  <allow>;
}
maximum-paths path-limit  <log-only | threshold value  log-interval seconds >;
maximum-prefixes prefix-limit  <log-only | threshold value  log-interval seconds
  >;
multicast {
  flow-map map-name  {
    bandwidth value  {
      adaptive;
    }
    forwarding-cache {
      timeout minutes  {
        never;
      }
    }
    policy [ policy-name ];
    redundant-sources [ source-address ];
  }
  forwarding-cache {
    threshold (suppress | reuse) value value ;
    timeout minutes ;
  }
  interface interface-name  {
    maximum-bandwidth limit ;
  }
  rpf-check-policy [ value ];
  scope scope-name  {
    interface [ interface-name  ];
    prefix destination-prefix ;
  }
  scope-policy [ policy-name  ];
  ssm-groups [ addresses  ];
  ssm-map map-name  {
    policy [ policy-name ];
    source [ source-address ];
  }
}
multipath {
  vpn-unequal-cost {
    equal-external-internal;
  }
}
options {
  mark seconds ;
  syslog (level level  | upto level );
}
resolution {
  rib routing-table-name  {
```


Copyright © 2013, Juniper Networks, Inc.

```
    import [ policy-names ];
    resolution-ribs [ routing-table-names ];
  }
}
rib routing-table-name {
  aggregate {
    defaults {
      aggregate-options ;
    }
    route destination-prefix {
      aggregate-options ;
      policy policy-name ;
    }
  }
  generate {
    defaults {
      generate-options ;
    }
    route destination-prefix {
      generate-options ;
      policy policy-name ;
    }
  }
  martians {
    destination-prefix match-type <allow>;
  }
  maximum-paths path-limit <log-only | threshold value log-interval seconds
    >;
  maximum-prefixes prefix-limit <log-only | threshold value log-interval
  seconds >;
  multipath {
    vpn-unequal-cost {
      equal-external-internal;
    }
  }
  static {
    defaults {
      static-options ;
    }
    rib-group group-name ;
    route destination-prefix {
      bfd-liveness-detection {
        detection-time {
          threshold milliseconds ;
        }
        holddown-interval milliseconds;
        local-address ip-address ;
        minimum-interval milliseconds ;
        minimum-receive-interval milliseconds ;
        minimum-receive-ttl milliseconds ;
        multiplier number ;
        neighbor address ;
        transmit-interval {
          minimum-interval milliseconds ;
          threshold milliseconds ;
        }
```

```
            version (0 | 1);
          }
          lsp-next-hop nexthop {
            metric metric ;
            preference preference ;
          }
          next-hop [ nexthop ];
          qualified-next-hop ( address | interface-name ) {
            interface interface-name ;
            metric metric ;
            preference preference ;
          }
          static-options ;
        }
      }
    }
    router-id address ;
    static {
      defaults {
        static-options ;
      }
      rib-group group-name ;
      route destination-prefix {
        bfd-liveness-detection {
          detection-time {
            threshold milliseconds ;
          }
          holddown-interval milliseconds;
          local-address ip-address ;
          minimum-interval milliseconds ;
          minimum-receive-interval milliseconds ;
          minimum-receive-ttl milliseconds ;
          multiplier number ;
          neighbor address ;
          transmit-interval {
            minimum-interval milliseconds ;
            threshold milliseconds ;
          }
          version (0 | 1);
        }
        lsp-next-hop nexthop {
          metric metric ;
          preference preference ;
        }
        next-hop [ nexthop ];
        qualified-next-hop ( address | interface-name ) {
          interface interface-name ;
          metric metric ;
          preference preference ;
        }
        static-options ;
      }
    }
  }
  vlan-id (all | none | vlan-id );
  vlan-tags {
```


Copyright © 2013, Juniper Networks, Inc.

```
            inner vlan-id ;
            outer vlan-id ;
          }
          vrf-export [ policy-names ];
          vrf-import [ policy-names ];
          vrf-table-label;
          vrf-target {
            export community-name ;
            import community-name ;
          }
        }
      }
    }
```

**Related Documentation**

- MPLS for Security Devices
- Junos OS Services Interfaces Configuration Guide
- Multicast Protocols Configuration Guide

Copyright © 2013, Juniper Networks, Inc.

## mesh-group

**Syntax**

```
mesh-group mesh-group-name {
  associate-profile {
    profile-variable-set variable-set;
  }
  local-switching;
  mac-flush {
    (any-interface | any-spoke);
    propagate;
  }
  neighbor {
    associate-profile profile-name {
      profile-variable-set variable-set}
      }
    }
    backup-neighbor neighbor-id;
    community;
    connection-protection;
    encapsulation-type;
    ignore-encapsulation-mismatch;
    pseudowire-status-tlv;
    psn-tunnel-endpoint;
    revert-time;
    static (incoming-label | Outgoing-label);
    switchover-delay;
  }
  peer-as {
    all;
  }
  route-distinguisher rd-type;
  vpls-id rd-type;
```

**Hierarchy Level** [edit routing-instances *routing-instance-name* protocols vpls]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Blocks flooding of broadcast, unicast, and multicast packets within the customer edge (CE) devices.



NOTE: The configuration-statement is not applicable for packets that come from or go out of a provide edge (PE) device.

**Options**

- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Do not inherit configuration data from these groups.
- **associate-profile**—Associate profiles for dynamic IFL.
- **local-switching**—Allows local switching within CE device interfaces.
- **mac-flush**—Enables mac-flush processing.


Copyright © 2013, Juniper Networks, Inc.

- **neighbour**—Neighboring interface belonging to the mesh group.
- **peer-as**—Device that can be a peer.
- **route-distinguisher**—Route distinguisher for the mesh group.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- MPLS for Security Devices

## local-switching

**Syntax**
local-switching

**Hierarchy Level**
[edit routing-instances *routing-instance-name* protocols vpls mesh-group *mesh-group-name*]

**Release Information**
Statement introduced in Release 10.4 of Junos OS.

**Description**
The broadcast, unicast, and multicast packets are allowed to pass between two CE devices, when you enable the local switching configuration within the mesh group configuration.

**Options**
- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Do not inherit configuration data from these groups.
- **associate-profile**—Associate profiles for dynamic IFL.
- **local-switching**—Allows local switching within CE device interfaces.
- **mac-flush**—Enables mac-flush processing.
- **neighbour**—Neighboring interface belonging to the mesh group.
- **peer-as**—Device that can be a peer.
- **route-distinguisher**—Route distinguisher for the mesh group.
- **vpls-id**—LDP VPLS identifier for the mesh group.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- MPLS for Security Devices

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 17

# Routing-Options Hierarchy

This section contains the following topics:


- Routing-Options Configuration Statement Hierarchy on page 291


## Routing-Options Configuration Statement Hierarchy

Use the statements in the **routing-options** configuration hierarchy to configure protocol-independent routing properties.

```
routing-options {
  aggregate {
    defaults {
      aggregate-options ;
    }
    route destination-prefix {
      policy policy-name ;
      aggregate-options ;
    }
  }
  auto-export {
    (disable | enable);
    family {
      inet {
        disable;
        flow {
          (disable | enable);
          rib-group rib-group ;
        }
        multicast {
          (disable | enable);
          rib-group rib-group ;
        }
        unicast {
          (disable | enable);
          rib-group rib-group ;
        }
      }
      inet6 {
        disable;
        multicast {
          (disable | enable);
```

Copyright © 2013, Juniper Networks, Inc.

```
            rib-group rib-group ;
          }
          unicast {
            (disable | enable);
            rib-group rib-group ;
          }
        }
        iso {
          disable;
          unicast {
            (disable | enable);
            rib-group rib-group ;
          }
        }
      }
      traceoptions {
        file filename <files number > <size maximum-file-size >
        <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
      }
    }
    autonomous-system autonomous-system <loops number >;
    bgp-orf-cisco-mode;
    confederation confederation-autonomous-systems {
      members [ autonomous-system ] ;
    }
    dynamic-tunnels {
      tunnel-name {
        destination-networks prefix ;
        source-address address ;
        tunnel-type type-of-tunnel ;
      }
      traceoptions {
        file filename <files number > <size maximum-file-size >
        <world-readable | no-world-readable>;
        flag flag < flag-modifier > <disable>;
      }
    }
    fate-sharing {
      group group-name {
        cost value ;
        from address {
          to address ;
        }
      }
    }
    flow {
      route name {
        match {
          match-conditions ;
        }
        then {
          actions ;
        }
      }
      validation {
```


Copyright © 2013, Juniper Networks, Inc.

```
    traceoptions {
      file filename <files number >
      <size maximum-file-size > <world-readable | no-world-readable>;
      flag flag < flag-modifier > <disable>;
    }
  }
}
forwarding-table {
  export [ policy-names ];
  (indirect-next-hop | no-indirect-next-hop);
  unicast-reverse-paths (active-paths | feasible-paths);
}
generate {
  defaults {
    generate-options ;
  }
  route destination-prefix {
    policy policy-name ;
    generate-options ;
  }
}
graceful-restart {
  disable;
  restart-duration duration ;
}
instance-export [ policy-names ];
instance-import [ policy-names ];
interface-routes {
  family (inet | inet6) {
    import [ import-policies ];
    export {
      lan;
      point-to-point;
    }
  }
  rib-group {
    inet group-name ;
    inet6 group-name ;
  }
}
martians {
  destination-prefix match-type <allow>;
}
maximum-paths path-limit <log-only | threshold value log-interval seconds >;
maximum-prefixes prefix-limit <log-only | threshold value log-interval seconds >;
multicast {
  flow-map map-name {
    bandwidth value {
      adaptive;
    }
    forwarding-cache {
      timeout minutes {
        never;
      }
    }
    policy [ policy-name ];
```

Copyright © 2013, Juniper Networks, Inc.

```
    redundant-sources [ source-address ];
  }
  forwarding-cache {
    threshold (suppress | reuse) value value ;
    timeout minutes ;
  }
  interface interface-name {
    maximum-bandwidth limit ;
  }
  rpf-check-policy [ value ];
  scope scope-name {
    interface [ interface-name ];
    prefix destination-prefix ;
  }
  scope-policy [ policy-name ];
  ssm-groups [ addresses ];
  ssm-map map-name {
    policy [ policy-name ];
    source [ source-address ];
  }
  traceoptions {
    file filename <files number > <size maximum-file-size >
    <world-readable | no-world-readable>;
    flag flag < flag-modifier > <disable>;
  }
}
options {
  mark seconds ;
  syslog (level level | upto level );
}
resolution {
  rib routing-table-name {
    import [ policy-names ];
    resolution-ribs [ routing-table-names ];
  }
  tracefilter [ policy-name ];
  traceoptions {
    file filename <files number > <size maximum-file-size >
    <world-readable | no-world-readable>;
    flag flag < flag-modifier > <disable>;
  }
}
rib routing-table-name {
  aggregate {
    defaults {
      aggregate-options ;
    }
    route destination-prefix {
      policy policy-name ;
      aggregate-options ;
    }
  }
  generate {
    defaults {
      generate-options ;
    }
```


Copyright © 2013, Juniper Networks, Inc.

```
    route destination-prefix {
      policy policy-name ;
      generate-options ;
    }
  }
  martians {
    destination-prefix match-type <allow>;
  }
  maximum-paths path-limit <log-only | threshold value log-interval seconds >;
  maximum-prefixes prefix-limit <log-only | threshold value log-interval
  seconds >;
  static {
    defaults {
      static-options ;
    }
    rib-group group-name ;
    route destination-prefix {
      bfd-liveness-detection {
        detection-time {
          threshold milliseconds ;
        }
        holddown-interval milliseconds;
        local-address ip-address ;
        minimum-interval milliseconds ;
        minimum-receive-interval milliseconds ;
        minimum-receive-ttl milliseconds ;
        multiplier number ;
        neighbor address ;
        transmit-interval {
          minimum-interval milliseconds ;
          threshold milliseconds ;
        }
        version (0 | 1);
      }
      lsp-next-hop nexthop '{
        metric metric ;
        preference preference ;
      }
      next-hop [ next-hop ];
      qualified-next-hop ( address | interface-name ) {
        interface interface-name ;
        metric metric ;
        preference preference ;
      }
      static-options ;
    }
  }
}
rib-groups {
  group-name {
    export-rib [ group-names ];
    import-policy [ policy-names ];
    import-rib [ group-names ];
  }
}
route-distinguished-id address ;
```

Copyright © 2013, Juniper Networks, Inc.

```
    route-record;
    router-id address ;
    source-routing (ip | ipv6);
    static {
      defaults {
        static-options ;
      }
      rib-group group-name ;
      route destination-prefix {
        bfd-liveness-detection {
          detection-time {
            threshold milliseconds ;
          }
          holddown-interval milliseconds;
          local-address ip-address ;
          minimum-interval milliseconds ;
          minimum-receive-interval milliseconds ;
          minimum-receive-ttl milliseconds ;
          multiplier number ;
          neighbor address ;
          transmit-interval {
            minimum-interval milliseconds ;
            threshold milliseconds ;
          }
          version (0 | 1);
        }
        lsp-next-hop nexthop '{
          metric metric ;
          preference preference ;
        }
        next-hop [ next-hop ];
        qualified-next-hop ( address | interface-name ) {
          interface interface-name ;
          metric metric ;
          preference preference ;
        }
        static-options ;
      }
    }
    topologies {
      family (inet | inet6) {
        topology topology-name;
      }
    }
    traceoptions {
      file name <files number > <size maximum-file-size >
      <world-readable | no-world-readable>;
      flag flag < flag-modifier > <disable>;
    }
  }
```

**Related Documentation**

- MPLS for Security Devices
- Junos OS Services Interfaces Configuration Guide
- Multicast Protocols Configuration Guide


Copyright © 2013, Juniper Networks, Inc.

CHAPTER 18

# Schedulers Hierarchy and Statements

This section contains the following topics:


- Schedulers Configuration Statement Hierarchy on page 297


## Schedulers Configuration Statement Hierarchy

Use the statements in the **schedulers** configuration hierarchy to determine the day and time when security policies are in effect.

```
schedulers {
  scheduler scheduler-name {
    daily (all-day | exclude | start-time time stop-time time);
    description text;
    friday {
      (all-day | exclude | start-time time stop-time time);
    }
    monday {
      (all-day | exclude | start-time time stop-time time);
    }
    saturday {
      (all-day | exclude | start-time time stop-time time);
    }
    start-date date-time stop-date date-time;
    sunday {
      (all-day | exclude | start-time time stop-time time);
    }
    thursday {
      (all-day | exclude | start-time time stop-time time);
    }
    tuesday {
      (all-day | exclude | start-time time stop-time time);
    }
    wednesday {
      (all-day | exclude | start-time time stop-time time);
    }
  }
}
```

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## all-day

**Syntax** all-day;

**Hierarchy Level**
[edit schedulers scheduler *scheduler-name* daily],
[edit schedulers scheduler *scheduler-name* friday],
[edit schedulers scheduler *scheduler-name* monday],
[edit schedulers scheduler *scheduler-name* saturday],
[edit schedulers scheduler *scheduler-name* sunday],
[edit schedulers scheduler *scheduler-name* tuesday],
[edit schedulers scheduler *scheduler-name* thursday],
[edit schedulers scheduler *scheduler-name* wednesday]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Schedule the security policy to be in effect for an entire day.

NOTE: A schedule set for a specific time overrides a schedule set with the all-day statement. Use the all-day statement to specify that a security policy be in effect for the whole day

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## daily

**Syntax**

```
daily {
  (all-day | exclude | start-time time stop-time time );
}
```

**Hierarchy Level** [edit schedulers scheduler *scheduler-name* ]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Schedule the security policy to be in effect every day of the week.

If you create a daily schedule with the **daily** statement and also use the **friday**, **monday**, **saturday**, **sunday**, **tuesday**, **thursday**, and **wednesday** statement in the schedule, the parameters specified for a specific day (for example, Friday using the **friday** statement) override the schedule set with the **daily** statement.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## description (Schedulers)

**Syntax** description *text*;

**Hierarchy Level** [edit schedulers scheduler *scheduler-name*]

**Release Information** Statement introduced in Junos OS Release 12.1.

**Description** Specify descriptive text for a scheduler.



NOTE: The descriptive text should not include characters, such as “<”, “>”, “&”, or “\n”.

**Options** ***text***—Descriptive text about a scheduler.

**Range:** 1 through 300 characters



NOTE: The upper limit of the description text range is related to character encoding, and is therefore dynamic. However, if you configure the descriptive text length beyond 300 characters, the configuration might fail to take effect.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## exclude (Schedulers)

**Syntax** **exclude;**

**Hierarchy Level**
**[edit schedulers scheduler *scheduler-name* daily],**
**[edit schedulers scheduler *scheduler-name* friday],**
**[edit schedulers scheduler *scheduler-name* monday],**
**[edit schedulers scheduler *scheduler-name* saturday],**
**[edit schedulers scheduler *scheduler-name* sunday],**
**[edit schedulers scheduler *scheduler-name* tuesday],**
**[edit schedulers scheduler *scheduler-name* thursday],**
**[edit schedulers scheduler *scheduler-name* wednesday]**

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Exclude a specified day from the schedule.

Use the **exclude** statement to exclude a day from a daily schedule created with the **daily** statement. You cannot use the **exclude** statement for a particular day unless it is in conjunction with the **daily** statement in a schedule.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## friday

**Syntax**

```
friday {
  (all-day | exclude | start-time time stop-time time );
}
```

**Hierarchy Level** [edit schedulers scheduler *scheduler-name* ]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify a schedule for every Friday.

If you use the **friday** statement in conjunction with the **daily** statement for a schedule, the parameters set for the **friday** statement override the parameters set for the **daily** statement.

Use the **exclude** option to exclude Friday from a daily schedule configured with the **daily** statement.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## monday

**Syntax**

```
monday {
  (all-day | exclude | start-time time stop-time time );
}
```

**Hierarchy Level** [edit schedulers scheduler *scheduler-name* ]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify a schedule for every Monday.

If you use the **monday** statement in conjunction with the **daily** statement for a schedule, the parameters set for the **monday** statement override the parameters set for the **daily** statement.

Use the **exclude** option to exclude Monday from a daily schedule configured with the **daily** statement.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## saturday

**Syntax**

```
saturday {
  (all-day | exclude | start-time time stop-time time );
}
```

**Hierarchy Level** [edit schedulers scheduler *scheduler-name* ]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify a schedule for every Saturday.

If you use the **saturday** statement in conjunction with the **daily** statement for a schedule, the parameters set for the **saturday** statement override the parameters set for the **daily** statement.

Use the **exclude** option to exclude Saturday from a daily schedule configured with the **daily** statement.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## scheduler (Security Policies)

**Syntax**

```
scheduler scheduler-name {
  daily (all-day | exclude | start-time time stop-time time );
  description text;
  friday {
    (all-day | exclude | start-time time stop-time time );
  }
  monday {
    (all-day | exclude | start-time time stop-time time );
  }
  saturday {
    (all-day | exclude | start-time time stop-time time );
  }
  start-date date-time stop-date date-time ;
  sunday {
    (all-day | exclude | start-time time stop-time time );
  }
  thursday {
    (all-day | exclude | start-time time stop-time time );
  }
  tuesday {
    (all-day | exclude | start-time time stop-time time );
  }
  wednesday {
    (all-day | exclude | start-time time stop-time time );
  }
}
```

**Hierarchy Level** [edit schedulers]

**Release Information** Statement introduced in Junos OS Release 8.5. The **description** option added in Junos OS Release 12.1.

**Description** Create or modify a scheduler that defines when security policies are in effect.

You configure a scheduler to start at a specific date and time or start on a recurrent basis.

**Options** *scheduler-name* —Name of the scheduler. The scheduler name must consist of 1 to 63 characters that can be letters, numbers, dashes, and underscores and can begin with a number or letter.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## schedulers (Security Policies)

**Syntax** **schedulers { ... }**

**Hierarchy Level** **[edit]**

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Configure schedules for security policies that allow you to control network traffic flow and enforce network security.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## start-date

**Syntax** **start-date** *date-time*;

**Hierarchy Level** **[edit schedulers],**
**[edit schedulers scheduler** *scheduler-name* **]**

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the time, day, month, and year that the schedule starts.

Specifying the year is optional. If no year is specified, the schedule applies to the current year and all subsequent years. If the year is specified in either the **start-date** or **stop-date** statement, that year is used for both statements.

**Options** *date-time* —Use the format **[** *yyyy* **-]** *mm* **-** *dd* **.** *hh* **.** *mm* to specify the year, month, day, hour, and minutes.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## start-time (Schedulers)

**Syntax** **start-time** *time*;

**Hierarchy Level**
**[edit schedulers scheduler** *scheduler-name* **daily],**
**[edit schedulers scheduler** *scheduler-name* **friday],**
**[edit schedulers scheduler** *scheduler-name* **monday],**
**[edit schedulers scheduler** *scheduler-name* **saturday],**
**[edit schedulers scheduler** *scheduler-name* **sunday],**
**[edit schedulers scheduler** *scheduler-name* **tuesday],**
**[edit schedulers scheduler** *scheduler-name* **thursday],**
**[edit schedulers scheduler** *scheduler-name* **wednesday]**

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the time that a schedule starts for a specified day.

If you specify a starting time for a daily schedule with the **daily** statement and also include the **friday**, **monday**, **saturday**, **sunday**, **tuesday**, **thursday**, and **wednesday** statements in the schedule, the starting time specified for a specific day (for example, Friday using the **friday** statement) overrides the starting time set with the **daily** statement.

**Options** ***time*** —Use the 24-hour format ( ***hh*** : ***mm*** : ***ss*** ) to specify the hours, minutes, and seconds.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## stop-date

**Syntax** **stop-date** *date-time* **;**

**Hierarchy Level** **[edit schedulers],**
**[edit schedulers scheduler** *scheduler-name* **]**

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the time, day, month, and year that the schedule ends.

Specifying the year is optional. If no year is specified, the schedule applies to the current year and all subsequent years. If the year is specified in either the **start-date** or **stop-date** statement, that year is used for both statements.

**Options** *date-time* —Use the format **[** *yyyy* **-]** *mm* **-** *dd* **.** *hh* **.** *mm* to specify the year, month, day, hour, and minutes.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## stop-time

**Syntax** **stop-time** *time*;

**Hierarchy Level**
[edit schedulers scheduler *scheduler-name* daily],
[edit schedulers scheduler *scheduler-name* friday],
[edit schedulers scheduler *scheduler-name* monday],
[edit schedulers scheduler *scheduler-name* saturday],
[edit schedulers scheduler *scheduler-name* sunday],
[edit schedulers scheduler *scheduler-name* tuesday],
[edit schedulers scheduler *scheduler-name* thursday],
[edit schedulers scheduler *scheduler-name* wednesday]

**Release Information** Statement introduced in Junos OS Release.

**Description** Specify the time that a schedule stops for a specified day.

If you specify a stop time for a daily schedule with the **daily** statement and also include the the **friday**, **monday**, **saturday**, **sunday**, **tuesday**, **thursday**, and **wednesday** statements in the schedule, the stop time specified for a specific day (for example, Friday using the **friday** statement) overrides the stop time set with the **daily** statement.

**Options** *time*—Use the 24-hour format ( ***hh*** : ***mm*** : ***ss*** ) to specify the hours, minutes, and seconds.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## sunday

**Syntax** **sunday (all-day | exclude | start-time** ***time*** **stop-time** ***time*** **);**

**Hierarchy Level** **[edit schedulers scheduler** ***scheduler-name*** **]**

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify a schedule for every Sunday.

If you use the **sunday** statement in conjunction with the **daily** statement for a schedule, the parameters set for the **sunday** statement override the parameters set for the **daily** statement.

Use the **exclude** option to exclude Sunday from a daily schedule configured with the **daily** statement.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## thursday

**Syntax**

```
thursday {
  (all-day | exclude | start-time time stop-time time );
}
```

**Hierarchy Level** [edit schedulers scheduler *scheduler-name* ]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify a schedule for every Thursday.

If you use the **thursday** statement in conjunction with the **daily** statement for a schedule, the parameters set for the **thursday** statement override the parameters set for the **daily** statement.

Use the **exclude** option to exclude Thursday from a daily schedule configured with the **daily** statement.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## tuesday

**Syntax**

```
tuesday {
    (all-day | exclude | start-time time stop-time time );
}
```

**Hierarchy Level** [edit schedulers scheduler *scheduler-name* ]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify a schedule for every Tuesday.

If you use the **tuesday** statement in conjunction with the **daily** statement for a schedule, the parameters set for the **tuesday** statement override the parameters set for the **daily** statement.

Use the **exclude** option to exclude Tuesday from a daily schedule configured with the **daily** statement.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## wednesday

**Syntax**

```
wednesday {
  (all-day | exclude | start-time time stop-time time );
}
```

**Hierarchy Level** [edit schedulers scheduler *scheduler-name* ]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify a schedule for every Wednesday.

If you use the **wednesday** statement in conjunction with the **daily** statement for a schedule, the parameters set for the **wednesday** statement override the parameters set for the **daily** statement.

Use the **exclude** option to exclude Wednesday from a daily schedule configured with the **daily** statement.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 19

# Security Hierarchy and Statements

This section contains the following topics:


- [edit security] Hierarchy Level on page 315


## [edit security] Hierarchy Level


- [edit security address-book] Hierarchy Level on page 316
- [edit security alarms] Hierarchy Level on page 316
- [edit security alg] Hierarchy Level on page 317
- [edit security analysis] Hierarchy Level on page 322
- [edit security application-firewall] Hierarchy Level on page 322
- [edit security application-tracking] Hierarchy Level on page 322
- [edit security certificates] Hierarchy Level on page 323
- [edit security datapath-debug] Hierarchy Level on page 323
- [edit security dynamic-vpn] Hierarchy Level on page 324
- [edit security firewall-authentication] Hierarchy Level on page 325
- [edit security flow] Hierarchy Level on page 325
- [edit security forwarding-options] Hierarchy Level on page 326
- [edit security forwarding-process] Hierarchy Level on page 327
- [edit security gprs] Hierarchy Level on page 327
- [edit security group-vpn] Hierarchy Level on page 330
- [edit security idp] Hierarchy Level on page 333
- [edit security ike] Hierarchy Level on page 342
- [edit security ipsec] Hierarchy Level on page 344
- [edit security log] Hierarchy Level on page 345
- [edit security nat] Hierarchy Level on page 346
- [edit security pki] Hierarchy Level on page 349
- [edit security policies] Hierarchy Level on page 350
- [edit security resource-manager] Hierarchy Level on page 354
- [edit security screen] Hierarchy Level on page 354


Copyright © 2013, Juniper Networks, Inc.

- [edit security softwires] Hierarchy Level on page 356
- [edit security ssh-known-hosts] Hierarchy Level on page 356
- [edit security traceoptions] Hierarchy Level on page 357
- [edit security user-identification] Hierarchy Level on page 357
- [edit security utm] Hierarchy Level on page 357
- [edit security zones] Hierarchy Level on page 365

## [edit security address-book] Hierarchy Level

```
security {
  address-book (book-name | global) {
    address address-name {
      ip-prefix {
        description text;
      }
      description text;
      dns-name domain-name {
        ipv4-only;
        ipv6-only;
      }
      range-address lower-limit to upper-limit;
      wildcard-address ipv4-address/wildcard-mask;
    }
    address-set address-set-name {
      address address-name;
      address-set address-set-name;
      description text;
    }
    attach {
      zone zone-name;
    }
    description text;
  }
}
```

**Related Documentation**

- MPLS for Security Devices
- Address Books and Address Sets for Security Devices
- Security Policy Applications for Security Devices
- Logical Systems for Security Devices

## [edit security alarms] Hierarchy Level

```
security {
  alarms {
    audible {
      continuous;
    }
    potential-violation {
      authentication failures;
      cryptographic-self-test;
      decryption-failures {
```


Copyright © 2013, Juniper Networks, Inc.

```
        threshold value;
      }
      encryption-failures {
        threshold value;
      }
      idp;
      ike-phase1-failures {
        threshold value;
      }
      ike-phase2-failures {
        threshold value;
      }
      key-generation-self-test;
      non-cryptographic-self-test;
      policy {
        application {
          duration interval;
          size count;
          threshold value;
        }
        destination-ip {
          duration interval;
          size count;
          threshold value;
        }
        policy match {
          duration interval;
          size count;
          threshold value;
        }
        source-ip {
          duration interval;
          size count;
          threshold value;
        }
      }
      replay-attacks {
        threshold value;
      }
      security-log-percent-full percentage;
    }
  }
}
```

**Related Documentation**

- IPsec VPNs for Security Devices
- Device and Routing Operations Monitoring
- Troubleshooting for Security Devices

## [edit security alg] Hierarchy Level

```
security {
  alg {
    alg-manager {
      traceoptions {
```

```
      flag {
        all <extensive>;
      }
    }
  }
  alg-support-lib {
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
  dns {
    disable;
    doctoring (none | sanity-check);
    maximum-message-length number;
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
  ftp {
    allow-mismatch-ip-address;
    disable;
    ftps-extension;
    line-break-extension;
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
  h323 {
    application-screen {
      message-flood {
        gatekeeper {
          threshold rate;
        }
      }
      unknown-message {
        permit-nat-applied;
        permit-routed;
      }
    }
    disable;
    dscp-rewrite {
      code-point string;
    }
    endpoint-registration-timeout value-in-seconds;
    media-source-port-any;
    traceoptions {
      flag flag <detail | extensive | terse>;
    }
  }
  ike-esp-nat {
```


Copyright © 2013, Juniper Networks, Inc.

```
    enable;
    esp-gate-timeout value-in-seconds;
    esp-session-timeout value-in-seconds;
    state-timeout value-in-seconds;
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
  mgcp {
    application-screen {
      connection-flood {
        threshold rate;
      }
      message-flood {
        threshold rate;
      }
      unknown-message {
        permit-nat-applied;
        permit-routed;
      }
    }
    disable;
    dscp-rewrite {
      code-point string;
    }
    inactive-media-timeout value-in-seconds;
    maximum-call-duration value-in-minutes;
    traceoptions {
      flag flag <extensive>;
    }
    transaction-timeout value-in-seconds;
  }
  msrpc {
    disable;
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
  pptp {
    disable;
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
  real {
    disable;
    traceoptions {
      flag {
        all <extensive>;
      }
```

```
    }
  }
  rsh {
    disable;
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
  rtsp {
    disable;
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
  sccp {
    application-screen {
      call-flood {
        threshold rate;
      }
      unknown-message {
        permit-nat-applied;
        permit-routed;
      }
    }
    disable;
    dscp-rewrite {
      code-point string;
    }
    inactive-media-timeout value-in-seconds;
    traceoptions {
      flag flag <extensive>;
    }
  }
  sip {
    application-screen {
      protect {
        deny {
          all {
            timeout value-in-seconds;
          }
          destination-ip address;
          timeout value-in-seconds;
        }
      }
      unknown-message {
        permit-nat-applied;
        permit-routed;
      }
    }
    c-timeout value-in-minutes;
    disable;
    dscp-rewrite {
```


Copyright © 2013, Juniper Networks, Inc.

```
            code-point string;
        }
        inactive-media-timeout value-in-seconds;
        maximum-call-duration value-in-minutes;
        retain-hold-resource;
        t1-interval value-in-milliseconds;
        t4-interval value-in-seconds;
        traceoptions {
            flag flag <detail | extensive | terse>;
        }
    }
    sql {
        disable;
        traceoptions {
            flag {
                all <extensive>;
            }
        }
    }
    sunrpc {
        disable;
        traceoptions {
            flag {
                all <extensive>;
            }
        }
    }
    talk {
        disable;
        traceoptions {
            flag {
                all <extensive>;
            }
        }
    }
    tftp {
        disable;
        traceoptions {
            flag {
                all <extensive>;
            }
        }
    }
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            (no-world-readable | world-readable);
            size maximum-file-size;
        }
        level (brief | detail | extensive | verbose);
        no-remote-trace;
    }
  }
}
```

**Related Documentation**

- Device and Routing Operations Monitoring
- Application Layer Gateways for Security Devices

## [edit security analysis] Hierarchy Level

```
security {
  analysis no-report;
}
```

**Related Documentation**

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

## [edit security application-firewall] Hierarchy Level

```
security {
  application-firewall {
    rule-sets rule-set-name {
      default-rule {
        (deny | permit);
      }
      rule rule-name {
        match {
          dynamic-application [system-application];
          dynamic-application-group [system-application-group];
        }
        then {
          (deny | permit);
        }
      }
    }
    traceoptions {
      file {
        filename;
        files number;
        match regular-expression;
        (no-world-readable | world-readable);
        size maximum-file-size;
      }
      flag flag;
      no-remote-trace;
    }
  }
}
```

**Related Documentation**

- Application Firewall
- Security Policy Applications for Security Devices
- Logical Systems for Security Devices

## [edit security application-tracking] Hierarchy Level

```
security {
  application-tracking {
```


Copyright © 2013, Juniper Networks, Inc.

```
        disable;
        (first-update | first-update-interval first-update-interval);
        session-update-interval session-update-interval;
      }
    }
```

**Related Documentation**

- Application Tracking
- Logical Systems for Security Devices

## [edit security certificates] Hierarchy Level

```
security {
  certificates {
    cache-size bytes;
    cache-timeout-negative seconds;
    certification-authority profile-name {
      ca-name name;
      crl filename;
      encoding (binary | pem);
      enrollment-url url;
      file filename;
      ldap-url url;
    }
    enrollment-retry number;
    local name {
      certificate;
      load-key-file url;
    }
    maximum-certificates number;
    path-length length;
  }
}
```

**Related Documentation**

- Device Configuration
- Upgrades and Downgrades

## [edit security datapath-debug] Hierarchy Level

```
security {
  datapath-debug {
    action-profile profile-name {
      event (jexec | lbt | lt-enter | lt-leave | mac-egress | mac-ingress | np-egress |
        np-ingress | pot) {
        count;
        packet-dump;
        packet-summary;
        trace;
      }
      module {
        flow {
          flag {
            all;
          }
```

Copyright © 2013, Juniper Networks, Inc.

```
            }
          }
          preserve-trace-order;
          record-pic-history;
        }
        capture-file {
          filename;
          files files-number;
          format pacp-format;
          (no-world-readable | world-readable);
          size maximum-file-size;
        }
        maximum-capture-size value;
        packet-filter packet-filter-name {
          action-profile (profile-name | default);
          destination-port (port-range | protocol-name);
          destination-prefix destination-prefix;
          interface logical-interface-name;
          protocol (protocol-number | protocol-name;
          source-port (port-range | protocol- name);
          source-prefix source-prefix;
          }
        trace-options {
          file {
            filename;
            files files-number;
            match regular-expression;
            (no-world-readable | world-readable);
            size maximum-file-size;
          }
          no-remote-trace;
        }
      }
    }
```

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices
- Device and Routing Operations Monitoring
- Troubleshooting for Security Devices

## [edit security dynamic-vpn] Hierarchy Level

```
security {
  dynamic-vpn {
    access-profile profile-name;
    clients configuration-name {
      ipsec-vpn vpn-name;
      remote-exceptions ip-address/mask;
      remote-protected-resources ip-address/mask;
      user username;
      user-groups user-group-names;
    }
    force-upgrade;
    config-check;
    interface;
```


Copyright © 2013, Juniper Networks, Inc.

```
    traceoptions {
      file filename;
      flag flag;
    }
  }
}
```

**Related Documentation**
- Dynamic VPNs for Security Devices

## [edit security firewall-authentication] Hierarchy Level

```
security {
  firewall-authentication {
    traceoptions {
      flag flag;
    }
  }
}
```

**Related Documentation**
- Logical Systems for Security Devices

## [edit security flow] Hierarchy Level

```
security {
  flow {
    aging {
      early-ageout seconds;
      high-watermark percent;
      low-watermark percent;
    }
    allow-dns-reply;
    bridge {
      block-non-ip-all;
      bpdu-vlan-flooding;
      bypass-non-ip-unicast;
      no-packet-flooding {
        no-trace-route;
      }
    }
    force-ip-reassembly;
    load distribution {
      session-affinity ipsec;
    }
    pending-sess-queue-length (high | moderate | normal);
    route-change-timeout seconds;
    syn-flood-protection-mode (syn-cookie | syn-proxy);
    tcp-mss {
      all-tcp mss value;
      gre-in {
        mss value;
      }
      gre-out {
        mss value;
      }
```

Copyright © 2013, Juniper Networks, Inc.

```
        ipsec-vpn {
            mss value;
        }
    }
    tcp-session {
        no-sequence-check;
        no-syn-check;
        no-syn-check-in-tunnel;
        rst-invalidate-session;
        rst-sequence-check;
        strict-syn-check;
        tcp-initial-timeout seconds;
        time-wait-state {
            (session-ageout | session-timeout seconds);
        }
    }
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            (no-world-readable | world-readable);
            size maximum-file-size;
        }
        flag flag;
        no-remote-trace;
        packet-filter filter-name {
            destination-port port-identifier;
            destination-prefix address;
            interface interface-name;
            protocol protocol-identifier;
            source-port port-identifier;
            source-prefix address;
        }
        rate-limit messages-per-second;
    }
  }
}
```

**Related Documentation**

- Flow-Based Processing for Security Devices
- Logical Systems for Security Devices
- Device and Routing Operations Monitoring
- Troubleshooting for Security Devices

## [edit security forwarding-options] Hierarchy Level

```
security {
  forwarding-options {
    family {
      inet6 {
        mode (drop | flow-based | packet-based);
      }
      iso {
```


Copyright © 2013, Juniper Networks, Inc.

```
            mode packet-based;
          }
          mpls {
            mode packet-based;
          }
        }
      }
    }
```

**Related Documentation**

- MPLS for Security Devices

## [edit security forwarding-process] Hierarchy Level

```
security {
  forwarding-process {
    application-services {
      maximize-alg-sessions;
      maximize-cp-sessions;
      maximize-idp-sessions {
        inline-tap;
        weight (equal | firewall | idp);
      }
      session-distribution-mode {
        hash-based;
      }
    }
  }
}
```

**Related Documentation**

- Processing Overview for Security Devices

## [edit security gprs] Hierarchy Level

```
security {
  gprs {
    gtp {
      enable;
      profile profile-name {
        apn pattern-string {
          mcc-mnc mcc-mnc-number {
            action {
              drop;
              pass;
              selection (ms|net|vrf);
            }
          }
        }
        drop {
          aa-create-pdp (0 | 1 | 2 | all);
          aa-delete-pdp (0 | 1 | 2 | all);
          bearer-resource (0 | 1 | 2 | all);
          change-notification (0 | 1 | 2 | all);
          config-transfer (0 | 1 | 2 | all);
          context (0 | 1 | 2 | all);
```

Copyright © 2013, Juniper Networks, Inc.

```
    create-bearer (0 | 1 | 2 | all);
    create-data-forwarding (0 | 1 | 2 | all);
    create pdp (0 | 1 | 2 | all);
    create-session (0 | 1 | 2 | all);
    create-tnl-forwarding (0 | 1 | 2 | all);
    cs-paging (0 | 1 | 2 | all);
    data-record (0 | 1 | 2 | all);
    delete-bearer (0 | 1 | 2 | all);
    delete-command (0 | 1 | 2 | all);
    delete-data-forwarding (0 | 1 | 2 | all);
    delete-pdn (0 | 1 | 2 | all);
    delete-pdp (0 | 1 | 2 | all);
    delete-session (0 | 1 | 2 | all);
    detach (0 | 1 | 2 | all);
    downlink-notification (0 | 1 | 2 | all);
    echo (0 | 1 | 2 | all);
    error-indication (0 | 1 | 2 | all);
    failure-report (0 | 1 | 2 | all);
    fwd-access (0 | 1 | 2 | all);
    fwd-relocation (0 | 1 | 2 | all);
    fwd-srns-context (0 | 1 | 2 | all);
    g-pdu (0 | 1 | 2 | all);
    identification (0 | 1 | 2 | all);
    mbms-sess-start (0 | 1 | 2 | all);
    mbms-sess-stop (0 | 1 | 2 | all);
    mbms-sess-update (0 | 1 | 2 | all);
    modify-bearer (0 | 1 | 2 | all);
    modify-command (0 | 1 | 2 | all);
    node-alive (0 | 1 | 2 | all);
    note-ms-present (0 | 1 | 2 | all);
    pdu-notification (0 | 1 | 2 | all);
    ran-info (0 | 1 | 2 | all);
    redirection (0 | 1 | 2 | all);
    release-access (0 | 1 | 2 | all);
    relocation-cancel (0 | 1 | 2 | all);
    resume (0 | 1 | 2 | all);
    send-route (0 | 1 | 2 | all);
    sgsn-context (0 | 1 | 2 | all);
    stop-paging (0 | 1 | 2 | all);
    supported-extension (0 | 1 | 2 | all);
    suspend (0 | 1 | 2 | all);
    trace-session (0 | 1 | 2 | all);
    update-bearer (0 | 1 | 2 | all);
    update-pdn (0 | 1 | 2 | all);
    update-pdp (0 | 1 | 2 | all);
    ver-not-supported (0 | 1 | 2 | all);
  }
  gtp-in-gtp-denied;
  log {
    forwarded (basic | detail);
    prohibited (basic | detail);
    rate-limited {
      (basic | detail);
      frequency-number number;
    }
    state-invalid (basic | detail);
```


Copyright © 2013, Juniper Networks, Inc.

```
        }
        max-message-length number;
        min-message-length number;
        rate-limit limit;
        remove-ie {
          version v1 {
          number ie-number;
          release (R6 | R7 | R8 | R9);
          }
        }
        restart-path (all | create | echo);
        timeout (value);
      }
      traceoptions {
        file {
          filename;
          files number;
          match regular-expression;
          (no-world-readable | world-readable);
          size maximum-file-size;
        }
        flag flag;
        no-remote-trace;
      }
    }
    sctp {
      log {
        configuration;
        decoding-error;
        dropped-packet;
        exceeding-rate-limit;
      }
      profile profile-name {
        association-timeout time-in-minutes;
        drop {
          m3ua-service {
            isup;
            sccp;
            tup;
          }
          payload-protocol {
            all;
            asap;
            bicc;
            ddp-segment;
            ddp-stream;
            dua;
            enrp;
            h248;
            h323;
            iua;
            m2pa;
            m2ua;
            m3ua;
            qipc;
            reserved;
```

```
                simco;
                sua;
                tali;
                v5ua;
              }
            }
            handshake-timeout time-in-seconds;
            limit {
              rate {
                address ip-address {
                  sccp rate-limit;
                  ssp rate-limit;
                  sst rate-limit;
                }
                sccp rate-limit;
                ssp rate-limit;
                sst rate-limit;
              }
            }
          }
          traceoptions {
            file {
              filename;
              files number;
              match regular-expression;
              (no-world-readable | world-readable);
              size maximum-file-size;
            }
            flag flag;
            no-remote-trace;
          }
        }
      }
    }
```

**Related Documentation**

- General Packet Radio Service for Security Devices

## [edit security group-vpn] Hierarchy Level

```
security {
  group-vpn {
    co-location;
    member {
      ike {
        gateway gateway-name {
          address [ip-address-or-hostname];
          ike-policy policy-name;
          local-address ip-address;
          local-identity {
            (distinguished-name | hostname hostname | inet ip-address | user-at-hostname
              e-mail-address);
          }
        }
        policy policy-name {
          certificate {
```


Copyright © 2013, Juniper Networks, Inc.

```
            local-certificate certificate-id;
            peer-certificate-type [pkcs7 | x509-signature);
            trusted-ca (ca-index | use-all);
          }
          description description;
          mode (aggressive | main);
          pre-shared-key (ascii-text key | hexadecimal key);
          proposal-set (basic | compatible | standard);
          proposals [proposal-name];
        }
        proposal proposal-name {
          authentication-algorithm (md5 | sha-256 | sha1);
          authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
          description description;
          dh-group (group1 | group14 | group2 | group5);
          encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc |
            des-cbc);
          lifetime-seconds seconds;
        }
      }
      ipsec {
        vpn vpn-name {
          group id;
          group-vpn-external-interface interface;
          heartbeat-threshold number;
          ike-gateway gateway-name;
        }
      }
    }
    server {
      group name {
        activation-time-delay seconds;
        anti-replay-time-window seconds;
        description description;
        group-id number;
        ike-gateway gateway-name;
        ipsec-sa name {
          match-policy policy-name {
            destination ip-address/netmask;
            destination-port number;
            protocol number;
            source ip-address/netmask;
            source-port number;
          }
          proposal proposal-name;
        }
        no-anti-replay;
        server-address ip-address;
        server-member-communication {
          certificate certificate-id;
          communication-type (multicast | unicast);
          encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc |
            des-cbc);
          heartbeat seconds;
          lifetime-seconds seconds;
          multicast-group address;
```

```
        multicast-outgoing-interface interface;
        number-of-retransmission number;
        retransmission-period seconds;
        sig-hash-algorithm (md5 | sha1);
    }
}
ike {
    gateway gateway-name {
        address ip-address-or-hostname;
        dynamic {
            (distinguished-name <container container-string> <wildcard wildcard-string>
              | hostname domain-name | inet ip-address | user-at-hostname
              e-mail-address);
        }
        ike-policy policy-name;
        local-identity {
            (distinguished-name | hostname hostname | inet ip-address | user-at-hostname
              e-mail-address);
        }
    }
    policy policy-name {
        certificate {
            local-certificate certificate-id;
            peer-certificate-type [pkcs7 | x509-signature);
            trusted-ca (ca-index | use-all);
        }
        description description;
        mode (aggressive | main);
        pre-shared-key (ascii-text key | hexadecimal key);
        proposal-set (basic | compatible | standard);
        proposals [proposal-name];
    }
    proposal proposal-name {
        authentication-algorithm (md5 | sha-256 | sha1);
        authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
        description description;
        dh-group (group1 | group14 | group2 | group5);
        encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc |
          des-cbc);
    }
}
ipsec {
    proposal proposal-name {
        authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
        description description;
        encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc |
          des-cbc);
        lifetime-seconds seconds;
    }
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        (no-world-readable | world-readable);
```


Copyright © 2013, Juniper Networks, Inc.

```
            size maximum-file-size;
          }
          flag flag;
          no-remote-trace;
        }
      }
    }
  }
```

**Related Documentation**

- Group VPNs for Security Devices

## [edit security idp] Hierarchy Level

```
security {
  idp {
    active-policy policy-name;
    application-ddos application-name {
      connection-rate-threshold number;
      context context-name {
        exclude-context-values [value];
        hit-rate-threshold number;
        max-context-values number;
        time-binding-count number;
        time-binding-period seconds;
        value-hit-rate-threshold number;
      }
      service service-name;
    }
    custom-attack attack-name {
      attack-type {
        anomaly {
          direction (any | client-to-server | server-to-client);
          service service-name;
          shellcode (all | intel | no-shellcode | sparc);
          test test-condition;
        }
        chain {
          expression boolean-expression;
          member member-name {
            attack-type {
              (anomaly ...same statements as in [edit security idp custom-attack
                attack-name attack-type anomaly] hierarchy level | signature ...same
                statements as in [edit security idp custom-attack attack-name attack-type
                signature] hierarchy level);
            }
          }
          order;
          protocol-binding {
            application application-name;
            icmp;
            icmpv6;
            ip {
              protocol-number transport-layer-protocol-number;
            }
            ipv6 {
```

```
            protocol-number transport-layer-protocol-number;
        }
        nested-application nested-application-name;
        rpc {
            program-number rpc-program-number;
        }
        tcp {
            minimum-port port-number <maximum-port port-number>;
        }
        udp {
            minimum-port port-number <maximum-port port-number>;
        }
    }
    reset;
    scope (session | transaction);
}
signature {
    context context-name;
    direction (any | client-to-server | server-to-client);
    negate;
    pattern signature-pattern;
    protocol {
        icmp {
            code {
                match (equal | greater-than | less-than | not-equal);
                value code-value;
            }
            data-length {
                match (equal | greater-than | less-than | not-equal);
                value data-length;
            }
            identification {
                match (equal | greater-than | less-than | not-equal);
                value identification-value;
            }
            sequence-number {
                match (equal | greater-than | less-than | not-equal);
                value sequence-number;
            }
            type {
                match (equal | greater-than | less-than | not-equal);
                value type-value;
            }
        }
        ipv4 {
            destination {
                match (equal | greater-than | less-than | not-equal);
                value ip-address-or-hostname;
            }
            identification {
                match (equal | greater-than | less-than | not-equal);
                value identification-value;
            }
            ip-flags {
                (df | no-df);
                (mf | no-mf);
```


Copyright © 2013, Juniper Networks, Inc.

```
        (rb | no-rb);
    }
    protocol {
        match (equal | greater-than | less-than | not-equal);
        value transport-layer-protocol-id;
    }
    source {
        match (equal | greater-than | less-than | not-equal);
        value ip-address-or-hostname;
    }
    tos {
        match (equal | greater-than | less-than | not-equal);
        value type-of-service-in-decimal;
    }
    total-length {
        match (equal | greater-than | less-than | not-equal);
        value total-length-of-ip-datagram;
    }
    ttl {
        match (equal | greater-than | less-than | not-equal);
        value time-to-live;
    }
}
ipv6 {
    destination {
        match (equal | greater-than | less-than | not-equal);
        value ip-address-or-hostname;
    }
    flow-label {
        match (equal | greater-than | less-than | not-equal);
        value flow-label-value;
    }
    hop-limit {
        match (equal | greater-than | less-than | not-equal);
        value hop-limit-value;
    }
    next-header {
        match (equal | greater-than | less-than | not-equal);
        value next-header-value;
    }
    payload-length {
        match (equal | greater-than | less-than | not-equal);
        value payload-length-value;
    }
    source {
        match (equal | greater-than | less-than | not-equal);
        value ip-address-or-hostname;
    }
    traffic-class {
        match (equal | greater-than | less-than | not-equal);
        value traffic-class-value;
    }
tcp {
    ack-number {
        match (equal | greater-than | less-than | not-equal);
        value acknowledgement-number;
```

```
    }
    data-length {
      match (equal | greater-than | less-than | not-equal);
      value tcp-data-length;
    }
    destination-port {
      match (equal | greater-than | less-than | not-equal);
      value destination-port;
    }
    header-length {
      match (equal | greater-than | less-than | not-equal);
      value header-length;
    }
    mss {
      match (equal | greater-than | less-than | not-equal);
      value maximum-segment-size;
    }
    option {
      match (equal | greater-than | less-than | not-equal);
      value tcp-option;
    }
    sequence-number {
      match (equal | greater-than | less-than | not-equal);
      value sequence-number;
    }
    source-port {
      match (equal | greater-than | less-than | not-equal);
      value source-port;
    }
    tcp-flags {
      (ack | no-ack);
      (fin | no-fin);
      (psh | no-psh);
      (r1 | no-r1);
      (r2 | no-r2);
      (rst | no-rst);
      (syn | no-syn);
      (urg | no-urg);
    }
    urgent-pointer {
      match (equal | greater-than | less-than | not-equal);
      value urgent-pointer;
    }
    window-scale {
      match (equal | greater-than | less-than | not-equal);
      value window-scale-factor;
    }
    window-size {
      match (equal | greater-than | less-than | not-equal);
      value window-size;
    }
  }
  udp {
    data-length {
      match (equal | greater-than | less-than | not-equal);
      value data-length;
```


Copyright © 2013, Juniper Networks, Inc.

```
                }
                destination-port {
                  match (equal | greater-than | less-than | not-equal);
                  value destination-port;
                }
                source-port {
                  match (equal | greater-than | less-than | not-equal);
                  value source-port;
                }
              }
            }
            protocol-binding {
              application application-name;
              icmp;
              icmpv6;
              ip {
                protocol-number transport-layer-protocol-number;
              }
              ipv6 {
                protocol-number transport-layer-protocol-number;
              }
              nested-application nested-application-name;
              rpc {
                program-number rpc-program-number;
              }
              tcp {
                minimum-port port-number <maximum-port port-number>;
              }
              udp {
                minimum-port port-number <maximum-port port-number>;
              }
            }
            regexp regular-expression;
            shellcode (all | intel | no-shellcode | sparc);
          }
        }
        recommended-action (close | close-client | close-server | drop | drop-packet | ignore
          | none);
        severity (critical | info | major | minor | warning);
        time-binding {
          count count-value;
          scope (destination | peer | source);
        }
      }
      custom-attack-group custom-attack-group-name {
        group-members [attack-or-attack-group-name];
      }
      dynamic-attack-group dynamic-attack-group-name {
        filters {
          category {
            values [category-value];
          }
          direction {
            expression (and | or);
            values [any client-to-server exclude-any exclude-client-to-server
              exclude-server-to-client server-to-client];
```

```
        }
        false-positives {
          values [frequently occasionally rarely unknown];
        }
        performance {
          values [fast normal slow unknown];
        }
        products {
          values [product-value];
        }
        recommended;
        service {
          values [service-value];
        }
        severity {
          values [critical info major minor warning];
        }
        type {
          values [anomaly signature];
        }
      }
    }
    idp-policy policy-name {
      rulebase-ddos {
        rule rule-name {
          description text;
          match {
            application (application-name | any | default);
            application-ddos <application-name>;
            destination-address ([address-name] | any | any-ipv4 | any-ipv6);
            destination-except [address-name];
            from-zone (zone-name | any);
            source-address ([address-name] | any | any-ipv4 | any-ipv6);
            source-except [address-name];
            to-zone (zone-name | any);
          }
          then {
            action {
              (close-server | drop-connection | drop-packet | no-action);
            }
            ip-action {
              (ip-block | ip-close | ip-connection-rate-limit connections-per-second |
                ip-notify);
              log;
              log-create;
              refresh-timeout;
              timeout seconds;
            }
            notification {
              log-attacks {
                alert;
              }
            }
          }
        }
      }
```


Copyright © 2013, Juniper Networks, Inc.

```
rulebase-exempt {
  rule rule-name {
    description text;
    match {
      attacks {
        custom-attack-groups [attack-group-name];
        custom-attacks [attack-name];
        dynamic-attack-groups [attack-group-name];
        predefined-attack-groups [attack-group-name];
        predefined-attacks [attack-name];
      }
      destination-address ([address-name] | any | any-ipv4 | any-ipv6);
      destination-except [address-name];
      from-zone (zone-name | any );
      source-address ([address-name] | any | any-ipv4 | any-ipv6);
      source-except [address-name];
      to-zone (zone-name | any);
    }
  }
}
rulebase-ips {
  rule rule-name {
    description text;
    match {
      application (application-name | any | default);
      attacks {
        custom-attack-groups [attack-group-name];
        custom-attacks [attack-name];
        dynamic-attack-groups [attack-group-name];
        predefined-attack-groups [attack-group-name];
        predefined-attacks [attack-name];
      }
      destination-address ([address-name] | any | any-ipv4 | any-ipv6);
      destination-except [address-name];
      from-zone (zone-name | any );
      source-address ([address-name] | any | any-ipv4 | any-ipv6);
      source-except [address-name];
      to-zone (zone-name | any);
    }
    terminal;
    then {
      action {
        class-of-service {
          dscp-code-point number;
          forwarding-class forwarding-class;
        }
        (close-client | close-client-and-server | close-server |drop-connection |
          drop-packet | ignore-connection | mark-diffserv value | no-action |
          recommended);
      }
      ip-action {
        (ip-block | ip-close | ip-notify);
        log;
        log-create;
        refresh-timeout;
```

Copyright © 2013, Juniper Networks, Inc.

```
            target (destination-address | service | source-address | source-zone |
              source-zone-address | zone-service);
            timeout seconds;
          }
          notification {
            log-attacks {
              alert;
            }
            packet-log {
              post-attack number;
              post-attack-timeout seconds;
              pre-attack number;
            }
          }
          severity (critical | info | major | minor | warning);
        }
      }
    }
  }
  security-package {
    automatic {
      download-timeout minutes;
      enable;
      interval hours;
      start-time start-time;
    }
    install {
      ignore-version-check;
    }
    source-address address;
    url url-name;
  }
  sensor-configuration {
    application-ddos {
      statistics {
        interval minutes;
      }
    }
    application-identification {
      max-packet-memory value;
      max-tcp-session-packet-memory value;
      max-udp-session-packet-memory value;
    }
    detector {
      protocol-name protocol-name {
        tunable-name  tunable-name {
          tunable-value protocol-value;
        }
      }
    }
    flow {
      (allow-icmp-without-flow | no-allow-icmp-without-flow);
      fifo-max-size value;
      hash-table-size value;
      (log-errors | no-log-errors);
      max-timers-poll-ticks value;
```


Copyright © 2013, Juniper Networks, Inc.

```
    reject-timeout value;
    (reset-on-policy | no-reset-on-policy);
    udp-anticipated-timeout value;
  }
  global {
    (enable-all-qmodules | no-enable-all-qmodules);
    (enable-packet-pool | no-enable-packet-pool);
    gtp (decapsulation | no-decapsulation);
    memory-limit-percent value;
    (policy-lookup-cache | no-policy-lookup-cache);
  }
  high-availability {
    no-policy-cold-synchronization;
  }
  ips {
    content-decompression-max-memory-kb value;
    content-decompression-max-ratio value;
    (detect-shellcode | no-detect-shellcode);
    fifo-max-size value;
    (ignore-regular-expression | no-ignore-regular-expression);
    log-supercede-min minimum-value;
    pre-filter-shellcode;
    (process-ignore-s2c | no-process-ignore-s2c);
    (process-override | no-process-override);
    process-port port-number;
  }
  log {
    cache-size size;
    suppression {
      disable;
      (include-destination-address | no-include-destination-address);
      max-logs-operate value;
      max-time-report value;
      start-log value;
    }
  }
  packet-log {
    host ip-address <port number>;
    max-sessions percentage;
    source-address ip-address;
    total-memory percentage;
  }
  re-assembler {
    (ignore-memory-overflow | no-ignore-memory-overflow);
    (ignore-reassembly-memory-overflow | no-ignore-reassembly-memory-overflow);
    ignore-reassembly-overflow;
    max-flow-mem value;
    max-packet-mem value;
  }
  ssl-inspection {
    cache-prune-chunk-size number;
    key-protection;
    maximum-cache-size number;
    session-id-cache-timeout seconds;
    sessions number;
  }
```

Copyright © 2013, Juniper Networks, Inc.

```
    }
    traceoptions {
      file {
        filename;
        files number;
        match regular-expression;
        (no-world-readable | world-readable);
        size maximum-file-size;
      }
      flag all;
      level (all | error | info | notice | verbose | warning);
      no-remote-trace;
    }
  }
}
```

**Related Documentation**

- IDP Signature Database for Security Devices
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices
- Application-Level Distributed Denial of Service
- IDP Administration for Security Devices
- Master Administrator for Logical Systems on Security Devices

## [edit security ike] Hierarchy Level

```
security {
  ike {
    gateway gateway-name {
      address [ip-address-or-hostname];
      dead-peer-detection {
        always-send;
        interval seconds;
        threshold number;
      }
      dynamic {
        connections-limit number;
        (distinguished-name <container container-string> <wildcard wildcard-string> |
          hostname domain-name | inet ip-address | inet6 ipv6-address | user-at-hostname
          e-mail-address);
        ike-user-type (group-ike-id | shared-ike-id);
      }
      external-interface external-interface-name;
      general-ikeid;
      ike-policy policy-name;
      local-identity {
        (distinguished-name | hostname hostname | inet ip-address | inet6 ipv6-address
          | user-at-hostname e-mail-address);
      }
      nat-keepalive seconds;
      no-nat-traversal;
      remote-identity {
```


Copyright © 2013, Juniper Networks, Inc.

```
            (distinguished-name <container container-string> <wildcard wildcard-string> |
              hostname hostname | inet ip-address | inet6 ipv6-address | user-at-hostname
              e-mail-address);
          }
          version (v1-only | v2-only);
          xauth {
            access-profile profile-name;
          }
        }
        policy policy-name {
          certificate {
            local-certificate certificate-id;
            peer-certificate-type (pkcs7 | x509-signature);
            trusted-ca (ca-index | use-all);
          }
          description description;
          mode (aggressive | main);
          pre-shared-key (ascii-text key | hexadecimal key);
          proposal-set (basic | compatible | standard);
          proposals [proposal-name];
        }
        proposal proposal-name {
          authentication-algorithm (md5 | sha-256 | sha1);
          authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
          description description;
          dh-group (group1 | group14 | group2 | group5);
          encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
          lifetime-seconds seconds;
        }
        respond-bad-spi <max-responses>;
        traceoptions {
          file {
            filename;
            files number;
            match regular-expression;
            (no-world-readable | world-readable);
            size maximum-file-size;
          }
          flag flag;
          no-remote-trace;
          rate-limit messages-per-second;
        }
      }
    }
```

**Related Documentation**

- MPLS for Security Devices
- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices
- Master Administrator for Logical Systems on Security Devices

Copyright © 2013, Juniper Networks, Inc.

## [edit security ipsec] Hierarchy Level

```
security {
  ipsec {
    policy policy-name {
      description description;
      perfect-forward-secrecy keys (group1 | group14 | group2 | group5);
      proposal-set (basic | compatible | standard);
      proposals [proposal-name];
    }
    proposal proposal-name {
      authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
      description description;
      encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
      lifetime-kilobytes kilobytes;
      lifetime-seconds seconds;
      protocol (ah | esp);
    }
    traceoptions {
      flag flag;
    }
    vpn vpn-name {
      bind-interface interface-name;
      df-bit (clear | copy | set);
      establish-tunnels (immediately | on-traffic);
      ike {
        gateway gateway-name;
        idle-time seconds;
        install-interval seconds;
        ipsec-policy ipsec-policy-name;
        no-anti-replay;
        proxy-identity {
          local ip-prefix;
          remote ip-prefix;
          service (any | service-name);
        }
      }
      manual {
        authentication {
          algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
          key (ascii-text key | hexadecimal key);
        }
        encryption {
          algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
          key (ascii-text key | hexadecimal key);
        }
        external-interface external-interface-name;
        gateway ip-address;
        protocol (ah | esp);
        spi spi-value;
      }
      vpn-monitor {
        destination-ip ip-address;
        optimized;
        source-interface interface-name;
```


Copyright © 2013, Juniper Networks, Inc.

```
        }
      }
      vpn-monitor-options {
        interval seconds;
        threshold number;
      }
    }
  }
```

**Related Documentation**

- MPLS for Security Devices
- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices
- Master Administrator for Logical Systems on Security Devices

## [edit security log] Hierarchy Level

```
security {
  log {
    cache {
      exclude exclude-name {
        destination-address destination-address;
        destination-port destination-port;
        event-id event-id;
        failure;
        interface-name interface-name;
        policy-name policy-name;
        process process-name;
        protocol protocol;
        source-address source-address;
        source-port source-port;
        success;
        user-name user-name;
      }
      limit value;
    }
    disable;
    event-rate rate;
    file {
      files max-file-number;
      name file-name;
      path binary-log-file-path;
      size maximum-file-size;
    }
    format (binary | sd-syslog | syslog);
    mode (event | stream);
    source-address source-address;
    stream stream-name {
      category (all | content-security);
      format (binary | sd-syslog | syslog | welf);
      host {
```

Copyright © 2013, Juniper Networks, Inc.

```
            ip-address;
            port port-number;
          }
          severity (alert | critical | debug | emergency | error | info | notice | warning);
        }
        traceoptions {
          file {
            file-name;
            files max-file-number;
            match regular-expression;
            (no-world-readable | world-readable);
            size maximum-file-size;
          }
          flag flag;
          no-remote-trace;
        }
        utc-time-stamp;
      }
    }
```

**Related Documentation**

- Log File Formats
- Application Tracking
- Master Administrator for Logical Systems on Security Devices

## [edit security nat] Hierarchy Level

```
security {
  nat {
    destination {
      pool pool-name {
        address ip-address {
          (port port-number | to ip-address);
        }
        description text;
        routing-instance routing-instance-name;
      }
      rule-set rule-set-name {
        description text;
        from {
          interface [interface-name];
          routing-instance [routing-instance-name];
          zone [zone-name];
        }
        rule rule-name {
          description text;
          match {
            (destination-address <ip-address> | destination-address-name
              <address-name>);
            destination-port port-number;
            protocol [protocol-name-or-number];
            source-address [ip-address];
            source-address-name [address-name];
          }
          then {
```


Copyright © 2013, Juniper Networks, Inc.

```
            destination-nat (off | pool pool-name);
          }
        }
      }
    }
    proxy-arp {
      interface interface-name {
        address ip-address {
          to ip-address;
        }
      }
    }
    proxy-ndp {
      interface interface-name {
        address ip-address {
          to ip-address;
        }
      }
    }
    source {
      address-persistent;
      interface {
        port-overloading {
          off;
        }
      }
      pool pool-name {
        address ip-address {
          to ip-address;
        }
        description text;
        host-address-base ip-address;
        overflow-pool (interface | pool-name);
        port {
          (no-translation | port-overloading-factor number | range port-low <to port-high>);
        }
        routing-instance routing-instance-name;
      }
      pool-default-port-range lower-port-range to upper-port-range;
      pool-utilization-alarm {
        clear-threshold value;
        raise-threshold value;
      }
      port-randomization {
        disable;
      }
      rule-set rule-set-name {
        description text;
        from {
          interface [interface-name];
          routing-instance [routing-instance-name];
          zone [zone-name];
        }
        rule rule-name {
          description text;
          match {
```

```
            (destination-address <ip-address> | destination-address-name
              <address-name>);
            destination-port port-number;
            protocol [protocol-name-or-number];
            source-address [ip-address];
            source-address-name [address-name];
          }
          then {
            source-nat {
              interface {
                persistent-nat {
                  address-mapping;
                  inactivity-timeout seconds;
                  max-session-number value;
                  permit (any-remote-host | target-host | target-host-port);
                }
              }
              off;
              pool {
                persistent-nat {
                  address-mapping;
                  inactivity-timeout seconds;
                  max-session-number number;
                  permit (any-remote-host | target-host | target-host-port);
                }
                pool-name;
              }
            }
          }
        }
        to {
          interface [interface-name];
          routing-instance [routing-instance-name];
          zone [zone-name];
        }
      }
    }
    static {
      rule-set rule-set-name {
        description text;
        from {
          interface [interface-name];
          routing-instance [routing-instance-name];
          zone [zone-name];
        }
        rule rule-name {
          description text;
          match {
            (destination-address ip-address | destination-address-name address-name);
            destination-port lower-port-range to upper-port-range;
          }
          then {
            static-nat {
              inet {
                routing-instance (default | routing-instance-name);
              }
```


Copyright © 2013, Juniper Networks, Inc.

```
                prefix {
                  address-prefix;
                  mapped-port lower-port-range to upper-port-range;
                  routing-instance (default | routing-instance-name);
                }
                prefix-name {
                  address-prefix-name;
                  mapped-port lower-port-range to upper-port-range;
                  routing-instance (default | routing-instance-name);
                }
              }
            }
          }
        }
      }
      traceoptions {
        file {
          filename;
          files number;
          match regular-expression;
          (no-world-readable | world-readable);
          size maximum-file-size;
        }
        flag flag;
        no-remote-trace;
      }
    }
  }
```

**Related Documentation**

- Network Address Translation for Security Devices
- Logical Systems for Security Devices
- Device and Routing Operations Monitoring
- Troubleshooting for Security Devices

## [edit security pki] Hierarchy Level

```
security {
  pki {
    auto-re-enrollment {
      certificate-id certificate-id-name {
        ca-profile-name ca-profile-name ;
        challenge-password password ;
        re-enroll-trigger-time-percentage percentage ;
        re-generate-keypair;
      }
    }
    ca-profile ca-profile-name {
      administrator {
        e-mail-address e-mail-address;
      }
      ca-identity ca-identity;
      enrollment {
          retry number;
```

Copyright © 2013, Juniper Networks, Inc.

```
            retry-interval seconds;
            url url-name;
        }
        revocation-check {
            crl {
                disable {
                    on-download-failure;
                }
                refresh-interval hours;
                url url-name ;
            }
            disable;
        }
        routing-instance routing-instance-name;
    }
    traceoptions {
        file filename {
            files number;
            match regular-expression;
            (no-world-readable | world-readable);
            size maximum-file-size;
        }
        flag flag;
        no-remote-trace;
    }
  }
}
```

**Related Documentation**

- Security Policy Applications for Security Devices

## [edit security policies] Hierarchy Level

```
security {
  policies {
    default-policy (deny-all | permit-all);
    from-zone zone-name to-zone zone-name {
      policy policy-name {
        description description;
        match {
          application {
            [application];
            any;
          }
          destination-address {
            [address];
            any;
            any-ipv4;
            any-ipv6;
          }
          source-address {
            [address];
            any;
            any-ipv4;
            any-ipv6;
          }
```


Copyright © 2013, Juniper Networks, Inc.

```
    source-identity {
      [role-name];
      any;
      authenticated-user;
      unauthenticated-user;
      unknown-user;
    }
  }
  scheduler-name scheduler-name;
  then {
    count {
      alarm {
        per-minute-threshold number;
        per-second-threshold number;
      }
    }
    deny;
    log {
      session-close;
      session-init;
    }
    permit {
      application-services {
        application-firewall {
          rule-set rule-set-name;
        }
        application-traffic-control {
          rule-set rule-set-name;
        }
        gprs-gtp-profile profile-name;
        gprs-sctp-profile profile-name;
        idp;
        redirect-wx | reverse-redirect-wx;
        ssl-proxy {
          profile-name profile-name;
        }
        uac-policy {
          captive-portal captive-portal;
        }
        utm-policy policy-name;
      }
      destination-address {
        drop-translated;
        drop-untranslated;
      }
      firewall-authentication {
        pass-through {
          access-profile profile-name;
          client-match user-or-group-name;
          ssl-termination-profile profile-name;
          web-redirect;
          web-redirect-to-https;
        }
        web-authentication {
          client-match user-or-group-name;
        }
```

```
            }
            services-offload;
            tcp-options {
              sequence-check-required;
              syn-check-required;
            }
            tunnel {
              ipsec-group-vpn group-vpn;
              ipsec-vpn vpn-name;
              pair-policy pair-policy;
            }
          }
          reject;
        }
      }
    }
    global {
      policy policy-name {
        description description;
        match {
          application {
            [application];
            any;
          }
          destination-address {
            [address];
            any;
            any-ipv4;
            any-ipv6;
          }
          source-address {
            [address];
            any;
            any-ipv4;
            any-ipv6;
          }
          source-identity {
            [role-name];
            any;
            authenticated-user;
            unauthenticated-user;
            unknown-user;
          }
        }
        scheduler-name scheduler-name;
        then {
          count {
            alarm {
              per-minute-threshold number;
              per-second-threshold number;
            }
          }
          deny;
          log {
            session-close;
            session-init;
```


Copyright © 2013, Juniper Networks, Inc.

```
        }
        permit {
          application-services {
            application-firewall {
              rule-set rule-set-name;
            }
            application-traffic-control {
              rule-set rule-set-name;
            }
            gprs-gtp-profile profile-name;
            gprs-sctp-profile profile-name;
            idp;
            redirect-wx | reverse-redirect-wx;
            ssl-proxy {
              profile-name profile-name;
            }
            uac-policy {
              captive-portal captive-portal;
            }
            utm-policy policy-name;
          }
          destination-address {
            drop-translated;
            drop-untranslated;
          }
          firewall-authentication {
            pass-through {
              access-profile profile-name;
              client-match user-or-group-name;
              ssl-termination-profile profile-name;
              web-redirect;
              web-redirect-to-https;
            }
            web-authentication {
              client-match user-or-group-name;
            }
          }
          services-offload;
          tcp-options {
            sequence-check-required;
            syn-check-required;
          }
        }
        reject;
      }
    }
  }
  policy-rematch;
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      (no-world-readable | world-readable);
      size maximum-file-size;
    }
```

```
        flag flag;
        no-remote-trace;
      }
    }
}
```

**Related Documentation**

- MPLS for Security Devices
- Security Policy
- Application Firewall
- Application Quality of Service
- Security Policies for Security Devices
- VPN for Security Devices
- Logical Systems for Security Devices
- Unified Access Control Solution for Security Devices

## [edit security resource-manager] Hierarchy Level

```
security {
  resource-manager {
    traceoptions {
      flag flag;
    }
  }
}
```

**Related Documentation**

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

## [edit security screen] Hierarchy Level

```
security {
  screen {
    ids-option screen-name {
        alarm-without-drop;
        description text;
        icmp {
          flood {
            threshold number;
          }
          fragment;
          ip-sweep {
            threshold number;
          }
          large;
          ping-death;
        }
        ip {
          bad-option;
          block-frag;
          loose-source-route-option;
```


Copyright © 2013, Juniper Networks, Inc.

```
            record-route-option;
            security-option;
            source-route-option;
            spoofing;
            stream-option;
            strict-source-route-option;
            tear-drop;
            timestamp-option;
            unknown-protocol;
        }
        limit-session {
            destination-ip-based number;
            source-ip-based number;
        }
        tcp {
            fin-no-ack;
            land;
            port-scan {
                threshold number;
            }
            syn-ack-ack-proxy {
                threshold number;
            }
            syn-fin;
            syn-flood {
                alarm-threshold number;
                attack-threshold number;
                destination-threshold number;
                source-threshold number;
                timeout seconds;
                white-list name {
                    destination-address destination-address;
                    source-address source-address;
                }
            }
            syn-frag;
            tcp-no-flag;
            tcp-sweep {
                threshold threshold number;
            }
            winnuke;
        }
        udp {
            flood {
                threshold number;
            }
            udp-sweep {
                threshold threshold number;
            }
        }
    }
}
traceoptions {
    file filename {
        files number;
        match regular-expression;
```

```
            (no-world-readable | world-readable);
            size maximum-file-size;
          }
          flag flag;
          no-remote-trace;
        }
      }
    }
```

**Related Documentation**

- Logical Systems for Security Devices

## [edit security softwires] Hierarchy Level

```
security {
  softwires {
    softwire-name name {
      softwire-concentrator ipv6-address;
      softwire-type IPv4-in-IPv6;
    }
    traceoptions {
      file {
        filename;
        files number;
        match regular-expression;
        (no-world-readable | world-readable);
        size maximum-file-size;
      }
      flag (all | configuration | flow);
      no-remote-trace;
    }
  }
}
```

**Related Documentation**

- Logical Systems for Security Devices

## [edit security ssh-known-hosts] Hierarchy Level

```
security {
  ssh-known-hosts {
    fetch-from-server server-name;
    host hostname {
      dsa-key dsa-key;
      ecdsa-sha2-nistp256-key ecdsa-sha2-nistp256-key;
      ecdsa-sha2-nistp384-key ecdsa-sha2-nistp384-key;
      ecdsa-sha2-nistp521-key ecdsa-sha2-nistp521-key;
      rsa-key rsa-key;
      rsa1-key rsa1-key;
    }
    load-key-file key-file;
  }
}
```

**Related Documentation**

- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

- Upgrades and Downgrades

## [edit security traceoptions] Hierarchy Level

```
security {
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      (no-world-readable | world-readable);
      size maximum-file-size;
    }
    flag flag;
    no-remote-trace;
    rate-limit messages-per-second;
  }
}
```

**Related Documentation**

- Troubleshooting for Security Devices

## [edit security user-identification] Hierarchy Level

```
security {
  user-identification {
    authentication-source {
      local-authentication-table (disable | priority priority);
      unified-access-control (disable | priority priority);
    }
    traceoptions {
      file {
        filename;
        files number;
        match regular-expression;
        (no-world-readable | world-readable);
        size maximum-file-size;
      }
      flag flag;
      no-remote-trace;
    }
  }
}
```

**Related Documentation**

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

## [edit security utm] Hierarchy Level

```
security {
  utm {
    application-proxy {
      traceoptions {
        flag flag;
      }
```

Copyright © 2013, Juniper Networks, Inc.

```
}
custom-objects {
  custom-url-category object-name {
    value [value];
  }
  filename-extension object-name {
    value [value];
  }
  mime-pattern object-name {
    value [value];
  }
  protocol-command object-name {
    value [value];
  }
  url-pattern object-name {
    value [value];
  }
}
feature-profile {
  anti-spam {
    address-blacklist list-name;
    address-whitelist list-name;
    sbl {
      profile profile-name {
        custom-tag-string [string];
        (sbl-default-server | no-sbl-default-server);
        spam-action (block | tag-header | tag-subject);
      }
    }
    traceoptions {
      flag flag;
    }
  }
  anti-virus {
    juniper-express-engine {
      pattern-update {
        email-notify {
          admin-email email-address;
          custom-message message;
          custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
          password password-string;
          port port-number;
          server address-or-url;
          username name;
        }
        url url;
      }
      profile profile-name {
        fallback-options {
          content-size (block | log-and-permit);
          default (block | log-and-permit);
          engine-not-ready (block | log-and-permit);
```


Copyright © 2013, Juniper Networks, Inc.

```
            out-of-resources (block | (log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
          }
          notification-options {
            fallback-block {
              administrator-email email-address;
              allow-email;
              custom-message message;
              custom-message-subject message-subject;
              display-host;
              (notify-mail-sender | no-notify-mail-sender);
              type (message | protocol-only);
            }
            fallback-non-block {
              custom-message message;
              custom-message-subject message-subject;
              (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
              custom-message message;
              custom-message-subject message-subject;
              (notify-mail-sender | no-notify-mail-sender);
              type (message | protocol-only);
            }
          }
          scan-options {
            content-size-limit value;
            (intelligent-prescreening | no-intelligent-prescreening);
            timeout value;
          }
          trickling {
            timeout value;
          }
        }
      }
      kaspersky-lab-engine {
        pattern-update {
          email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
          }
          interval value;
          no-autoupdate;
          proxy {
            password password-string;
            port port-number;
            server address-or-url;
            username name;
          }
          url url;
        }
        profile profile-name {
          fallback-options {
            content-size (block | log-and-permit);
```

```
            corrupt-file (block | log-and-permit);
            decompress-layer (block | log-and-permit);
            default (block | log-and-permit);
            engine-not-ready (block | log-and-permit);
            out-of-resources (block | (log-and-permit);
            password-file (block | (log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        notification-options {
            fallback-block {
                administrator-email email-address;
                allow-email;
                custom-message message;
                custom-message-subject message-subject;
                display-host;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
            fallback-non-block {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
        }
        scan-options {
            content-size-limit value;
            decompress-layer-limit value;
            (intelligent-prescreening | no-intelligent-prescreening);
            scan-extension filename;
            scan-mode (all | by-extension);
            timeout value;
        }
        trickling {
            timeout value;
        }
    }
}
mime-whitelist {
    exception listname;
    list listname {
        exception listname;
    }
}
sophos-engine {
    pattern-update {
        email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
```


Copyright © 2013, Juniper Networks, Inc.

```
    }
    interval value;
    no-autoupdate;
    proxy {
      password password-string;
      port port-number;
      server address-or-url;
      username name;
    }
    url url;
  }
  profile <name> {
    fallback-options {
      content-size (block | log-and-permit | permit);
      default (block | log-and-permit | permit);
      engine-not-ready (block | log-and-permit | permit);
      out-of-resources (block | log-and-permit | permit);
      timeout (block | log-and-permit | permit);
      too-many-requests (block | log-and-permit | permit);
    }
    notification-options {
      fallback-block {
        administrator-email email-address;
        allow-email;
        custom-message message;
        custom-message-subject message-subject;
        display-host;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
      fallback-non-block {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-recipient | no-notify-mail-recipient);
      }
      virus-detection {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
    }
    scan-options {
      content-size-limit value;
      (no-uri-check | uri-check);
      timeout value;
    }
    trickling {
      timeout value;
    }
  }
  sxl-retry value;
  sxl-timeout seconds;
}
traceoptions {
  flag flag;
```

```
    }
    type (juniper-express-engine | kaspersky-lab-engine | sophos-engine);
    url-whitelist listname;
  }
  content-filtering {
    profile profile-name {
      block-command protocol-command-list;
      block-content-type (activex | exe | http-cookie | java-applet | zip);
      block-extension extension-list;
      block-mime {
        exception list-name;
        list list-name;
      }
      notification-options {
        custom-message message;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
      permit-command protocol-command-list;
    }
    traceoptions {
      flag flag;
    }
  }
  web-filtering {
    juniper-enhanced {
      cache {
        size value;
        timeout value;
      }
      profile profile-name {
        block-message {
          type {
            custom-redirect-url;
          }
          url url;
        }
        quarantine-message {
          type {
            custom-redirect-url;
          }
          url url;
        }
        category customurl-list name {
          action (block | log-and-permit | permit | quarantine);
        }
        custom-block-message value;
        custom-quarantine-message value;
        default (block | log-and-permit | permit | quarantine);
        fallback-settings {
          default (block | log-and-permit);
          server-connectivity (block | log-and-permit);
          timeout (block | log-and-permit);
          too-many-requests (block | log-and-permit);
        }
        no-safe-search;
```


Copyright © 2013, Juniper Networks, Inc.

```
        site-reputation-action {
            fairly-safe (block | log-and-permit | permit | quarantine);
            harmful (block | log-and-permit | permit | quarantine);
            moderately-safe (block | log-and-permit | permit | quarantine);
            suspicious (block | log-and-permit | permit | quarantine);
            very-safe (block | log-and-permit | permit |quarantine);
        }
        timeout value;
    }
    server {
        host host-name;
        port number;
    }
}
juniper-local {
    profile profile-name {
        custom-block-message value;
        default (block | log-and-permit | permit);
        fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        timeout value;
    }
}
surf-control-integrated {
    cache {
        size value;
        timeout value;
    }
    profile profile-name {
        category customurl-list name {
            action (block | log-and-permit | permit);
        }
        custom-block-message value;
        default (block | log-and-permit | permit);
        fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        timeout value;
    }
    server {
        host host-name;
        port number;
    }
}
traceoptions {
    flag flag;
}
type (juniper-enhanced | juniper-local | surf-control-integrated |
    websense-redirect);
```

Copyright © 2013, Juniper Networks, Inc.

```
        url-blacklist listname;
        url-whitelist listname;
        websense-redirect {
          profile profile-name {
            account value;
            custom-block-message value;
            fallback-settings {
              default (block | log-and-permit);
              server-connectivity (block | log-and-permit);
              timeout (block | log-and-permit);
              too-many-requests (block | log-and-permit);
            }
            server {
              host host-name;
              port number;
            }
            sockets value;
            timeout value;
          }
        }
      }
    }
    ipc {
      traceoptions flag flag;
    }
    traceoptions {
      flag flag;
    }
    utm-policy policy-name {
      anti-spam {
        smtp-profile profile-name;
      }
      anti-virus {
        ftp {
          download-profile profile-name;
          upload-profile profile-name;
        }
        http-profile profile-name;
        imap-profile profile-name;
        pop3-profile profile-name;
        smtp-profile profile-name;
      }
      content-filtering {
        ftp {
          download-profile profile-name;
          upload-profile profile-name;
        }
        http-profile profile-name;
        imap-profile profile-name;
        pop3-profile profile-name;
        smtp-profile profile-name;
      }
      traffic-options {
        sessions-per-client {
          limit value;
          over-limit (block | log-and-permit);
```


Copyright © 2013, Juniper Networks, Inc.

```
        }
      }
      web-filtering {
        http-profile profile-name;
      }
    }
  }
}
```

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices

## [edit security zones] Hierarchy Level

```
security {
  zones {
    functional-zone {
      management {
        description text;
        host-inbound-traffic {
          protocols protocol-name {
            except;
          }
          system-services service-name {
            except;
          }
        }
        interfaces interface-name  {
          host-inbound-traffic {
            protocols protocol-name {
              except;
            }
            system-services service-name {
              except;
            }
          }
        }
        screen screen-name;
      }
    }
    security-zone zone-name {
      address-book {
        address address-name {
          ip-prefix {
            description text;
          }
          description text;
          dns-name domain-name {
            ipv4-only;
            ipv6-only;
          }
          range-address lower-limit to upper-limit;
          wildcard-address ipv4-address/wildcard-mask;
        }
```

Copyright © 2013, Juniper Networks, Inc.

```
        address-set address-set-name {
          address address-name;
          address-set address-set-name;
          description text;
        }
      }
      application-tracking;
      description text;
      host-inbound-traffic {
        protocols protocol-name {
          except;
        }
        system-services service-name {
          except;
        }
      }
      interfaces interface-name {
        host-inbound-traffic {
          protocols protocol-name {
            except;
          }
          system-services service-name {
            except;
          }
        }
      }
      screen screen-name;
      tcp-rst;
    }
  }
}
```

**Related Documentation**

- Application Tracking
- Security Zones and Interfaces for Security Devices
- Logical Systems for Security Devices
- Unified Access Control Solution for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## access-profile (Security Dynamic VPN)

**Syntax** access-profile *profile-name*;

**Hierarchy Level** [edit security dynamic-vpn]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Specify the access profile to use for Extended Authentication for remote users trying to download the Access Manager.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Dynamic VPNs for Security Devices

## access-profile (Security IKE Gateway)

**Syntax** access-profile *profile-name*;

**Hierarchy Level** [edit security ike gateway *gateway-name* xauth]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the access profile to use for Extended Authentication for remote users trying to access a Virtual Private Network (VPN) tunnel.

**Options** ***profile-name*** —Name of the access profile.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Dynamic VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## ack-number

**Syntax**

```
ack-number {
  match (equal | greater-than | less-than | not-equal);
  value acknowledgement-number;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the ACK number of the packet. This number identifies the next sequence number; the ACK flag must be set to activate this field.

**Options**

- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***acknowledgement-number***—Match the ACK number of the packet.

  **Range:** 0 through 4,294,967,295

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Administration for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## action (APN GTP)

**Syntax**

```
action {
  drop;
  pass;
  selection (ms|net|vrf);
}
```

**Hierarchy Level** [edit security gprs gtp profile *profile-name* apn *pattern-string* mcc-mnc *mcc-mnc-number*]

**Release Information** Statement introduced in Junos OS Release 10.0.

**Description** Configure GTP profile access point (AP) name filtering action to allow or deny access to specific access points.

**Options**

- **drop**—Specify to deny GTP packets from all selection modes for the specified access points.
- **pass**—Specify to permit GTP packets from all selection modes for the access points.
- **selection**—Specify one of the following selection modes for the access points:
  - **ms**—The access point name is provided by a mobile station, and the user-subscription is not verified.
  - **net**—The access point name is provided by a network, and the user subscription is not verified.
  - **vrf**— The access point name is provided by a network or an MS, and the user-subscription is verified.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- General Packet Radio Service for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## action (Security Application-Level DDoS)

**Syntax**

```
action {
   (close-server | drop-connection | drop-packet | no-action);
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* then]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Specify the actions you want IDP to take when the monitored traffic matches the application-ddos objects specified in the application-level DDoS rule.

**Options**

- **close-server**—Closes the connection and sends an RST packet to the server but not to the client.
- **drop-connection**—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing.
- **drop-packet**—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source-IP address.
- **no-action**—No action is taken. Use this action when you want to only generate logs for some traffic.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## action (Security Rulebase IPS)

**Syntax**

```
action {
  class-of-service {
    dscp-code-point number;
    forwarding-class forwarding-class;
  }
  (close-client | close-client-and-server | close-server |drop-connection | drop-packet |
    ignore-connection | mark-diffserv value | no-action | recommended);
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify the actions you want IDP to take when the monitored traffic matches the attack objects specified in the rules.

**Options**

- **class-of-service**—Associates a class-of-service forwarding class as an action to the IDP policy; also sets the value of the DSCP code point. You can use the default forwarding class names or define new ones. Forwarding-class and dscp-code-point are optional, but one must be set.
- **close-client**—Closes the connection and sends an RST packet to the client but not to the server.
- **close-client-and-server**—Closes the connection and sends an RST packet to both the client and the server.
- **close-server**—Closes the connection and sends an RST packet to the server but not to the client.
- **drop-connection**—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing.
- **drop-packet**—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source-IP address.
- **ignore-connection**—Stops scanning traffic for the rest of the connection if an attack match is found. IDP disables the rulebase for the specific connection.
- **mark-diffserv *value***—Assigns the indicated service-differentiation value to the packet in an attack, then passes them on normally.
- **no-action**—No action is taken. Use this action when you want to only generate logs for some traffic.
- **recommended**—All predefined attack objects have a default action associated with them. This is the action that Juniper Networks recommends when that attack is detected.

Copyright © 2013, Juniper Networks, Inc.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices
- IDP Class of Service Action for Security Devices

## action (Security UTM Web Filtering)

**Syntax**
action (block | log-and-permit | permit | quarantine);

**Hierarchy Level**
[edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name* category *customurl-last-name*]
[edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name* category *customurl-last-name*]

**Release Information**
Statement introduced in Release 9.5 of Junos OS.
Statement introduced in Release 11.4 of Junos OS for UTM Enhanced Web Filtering.

**Description**
Enter an action to go with the customurl-list filter.

**Options**
- block—Log the error and deny the traffic.
- log-and-permit—Log the error and permit the traffic.
- permit—Permit the traffic.
- quarantine—Show the warning message and permit/block the traffic based on user input.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- Unified Threat Management


Copyright © 2013, Juniper Networks, Inc.

## action-profile

**Syntax**

```
action-profile profile-name {
  event (jexec | lbt | lt-enter | lt-leave | mac-egress | mac-ingress | np-egress | np-ingress |
    pot) {
    count;
    packet-dump;
    packet-summary;
    trace;
  }
  module {
    flow {
      flag {
        all;
      }
    }
  }
  preserve-trace-order;
  record-pic-history;
}
```

**Hierarchy Level** [edit security datapath-debug]

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Configure the action profile options for data path debugging.

**Options**

- ***action-profile name*** — Name of the action profile.
- **event**—Enable the events to trace the packet when the packet hit the events (jexec, lbt, lt-enter, lt-leave, mac-egress, mac-ingress, np-egress, np-ingress, pot)
  - **count**—Number of times a packet hits the specified event.
  - **packet-dump**—Capture the packet that hits the specified event.
  - **packet-summary**—Print the source/destination IP address details with protocol number and IP length details along with trace message for the specified event.
  - **trace**—Print the standard trace message when the packet hits the specified event.
- **module**—Turn on the flow session related trace messages.
  - **flow**—Trace flow session related messages.
  - **flag**—Specify which flow message needs to be traced.
  - **all**—Trace all possible flow trace messages.
  - **trace**—Print the standard trace message when the packet hits the specified event.
- **preserve-trace-order**—Preserve trace order.
- **record-pic-history**—Record the PICs in which the packet has been processed.

Copyright © 2013, Juniper Networks, Inc.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## active-policy

**Syntax**
active-policy *policy-name*;

**Hierarchy Level**
[edit security idp]

**Release Information**
Statement introduced in Release 9.2 of Junos OS.

**Description**
Specify which policy among the configured policies to activate.

**Options**
***policy-name***—Name of the active policy.



NOTE: You need to make sure the active policy is enforced in the data plane.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices
- IDP Signature Database for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## address (Security Address Book)

**Syntax**

```
address address-name {
  ip-prefix {
    description text;
  }
  description text;
  dns-name domain-name {
    ipv4-only;
    ipv6-only;
  }
  range-address lower-limit to upper-limit;
  wildcard-address ipv4-address/wildcard-mask;
}
```

**Hierarchy Level** [edit security address-book *book-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 10.2 of Junos OS. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Release 10.4 of Junos OS. Support for wildcard addresses added in Release 11.1 of Junos OS. Support for address range added in Release 12.1 of Junos OS. The **description** option added in Release 12.1 of Junos OS.

**Description** Add an entry containing an IP address or DNS hostname, or wildcard address to the address book. An address book contains entries for addressable entities in security zones, policies, and NAT rules. Address book entries can include any combination of IPv4 addresses, IPv6 addresses, and DNS names.

**Options**

- **address *address-name*—**Name of an address entry.
- **description *text*—**Descriptive text about an address entry.
- dns-address ***domain-name*—**DNS address name.
- ***ip-prefix*—**IP address with prefix.
- **range-address *lower-limit* to *upper-limit*—**Address range for an address book.
- **wildcard-address *ipv4-address/wildcard-mask*—**IPv4 wildcard address in the form of A.B.C.D/wildcard-mask.



NOTE: IPv6 wildcard address configuration is not supported in this release.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Address Books and Address Sets for Security Devices
- Security Zones and Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## address (Security ARP Proxy)

**Syntax** address *ip-address* <to *ip-address*>;

**Hierarchy Level** [edit security nat proxy-arp interface *interface-name*],

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify a single address or an address range of ARP proxy.

**Options** **to**—Specify the upper limit of the address range.

***ip-address*** —IP address of an ARP proxy.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

## address (Security Destination NAT)

**Syntax**
```
address ip-address {
   (port port-number | to ip-address);
}
```

**Hierarchy Level** [edit security nat destination pool *pool-name*]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify a single address or an address range of the destination NAT pool.

**Options**
- **to**—Specify the upper limit of the address range.
- ***ip-address*** —IP address of a pool.
- **port** ***port-number***—Specify the port number.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## address (Security IKE Gateway)

**Syntax** address [*ip-address-or-hostname*];

**Hierarchy Level** [edit security group-vpn member ike gateway *gateway-name*]
[edit security ike gateway *gateway-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS.

**Description** Specify the IPv4 or IPv6 address or the hostname of the primary Internet Key Exchange (IKE) gateway and up to four backup gateways.

**Options** ***ip-address-or-hostname*** —IPv4 or IPv6 address or hostname of an IKE gateway.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPNs for Security Devices

## address (Security IKE Gateway Server)

**Syntax** address *ip-address-or-hostname* ;

**Hierarchy Level** [edit security group-vpn server ike gateway *gateway-name*]

**Release Information** Statement introduced in Junos OS Release 8.5. Support for **group-vpn** hierarchies added in Junos OS Release 10.2 of Junos OS. Support for IPv6 addresses added in Junos OS Release 11.1.

**Description** Specify the IPv4 or IPv6 address or the hostname of the primary Internet Key Exchange (IKE) gateway and up to four backup gateways.

**Options** ***ip-address-or-hostname***—IPv4 or IPv6 address or hostname of an IKE gateway.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## address (Security NDP Proxy)

**Syntax**

```
address ip-address {
    to ip-address;
}
```

**Hierarchy Level** [edit security nat proxy-ndp interface *interface-name*],

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify a single address or an address range of NDP proxy.

**Options**

- ***ip-address***—IP address of an NDP proxy.
- **to**—Specify the upper limit of the address range.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

## address (Security Source NAT)

**Syntax**

```
address ip-address {
    (port port-number | to ip-address);
}
```

**Hierarchy Level** [edit security nat source pool *pool-name*]

**Release Information** Statement modified in Release 9.6 of Junos OS.

**Description** Specify a single address or an address range of the source NAT pool.

**Options**

- **to**—Specify the upper limit of the address range.
- ***ip-address*** —IP address of a pool.
- **port *port-number***—Specify the port number.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## address-blacklist

**Syntax** address-blacklist *list-name*;

**Hierarchy Level** [edit security utm feature-profile anti-spam]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Enter an address-blacklist (or whitelist) custom-object for local list spam filtering.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## address-book

**Syntax**

```
address-book (book-name | global) {
  address address-name {
    ip-prefix {
      description text;
    }
    description text;
    dns-name domain-name {
      ipv4-only;
      ipv6-only;
    }
    range-address lower-limit to upper-limit;
    wildcard-address ipv4-address/wildcard-mask;
  }
  address-set address-set-name {
    address address-name;
    address-set address-set-name;
    description text;
  }
  attach {
    zone zone-name;
  }
  description text;
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for wildcard addresses added in Release 11.1 of Junos OS. Statement moved under the security hierarchy in Release 11.2 of Junos OS. Support for address range added in Release 12.1 of Junos OS. The **description** option added in Release 12.1 of Junos OS.

**Description** Define entries in the address book. Address book entries can include any combination of IPv4 addresses, IPv6 addresses, DNS names, wildcard addresses, and address range. You define addresses and address sets in an address book and then use them when configuring different features, such as security policies and NAT.



NOTE: IPv6 wildcard address configuration is not supported in this release.

**Options**

- **address-book *book-name*—**Name of the address book.
- **global—**An address book that is available by default. You can add any combination of IPv4 addresses, IPv6 addresses, wildcard addresses, DNS names, or address range to the global address book. You do not need to attach the global address book to a security zone; entries in the global address book are available to all security zones that are not attached to address books.

The remaining statements are explained separately.


Copyright © 2013, Juniper Networks, Inc.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Address Books and Address Sets for Security Devices
- Logical Systems for Security Devices

## address-mapping

**Syntax**
address-mapping;

**Hierarchy Level**
[edit security nat source rule-set *ruleset* rule *rule* then source-nat interface persistent-nat]
[edit security nat source rule-set *ruleset* rule *rule* then source-nat pool persistent-nat]

**Release Information**
Statement introduced in Junos OS Release 10.2.

**Description**
Allows requests from a specific internal IP address to be mapped to the same reflexive IP address (the public IP address created by the NAT device closest to the STUN server); internal and external ports can be any ports. An external host using any port can send a packet to the internal host by sending the packet to the reflexive IP address (with a configured incoming policy that allows external to internal traffic). If this option is not configured, the persistent NAT binding is for specific internal and reflexive transport addresses.

You can only specify this option when the persistent NAT type is **any-remote-host** and the source NAT rule action is one of the following:

- Source NAT pool with IP address shifting
- Source NAT pool with no port translation and no overflow pool

**Required Privilege Level**
**security**—To view this statement in the configuration.
**security-control**—To add this statement to the configuration

**Related Documentation**
- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## address-persistent

**Syntax** address-persistent;

**Hierarchy Level** [edit security nat source]

**Release Information** Statement modified in Junos OS Release 9.2.

**Description** Enable the device to assign the same IP address from a source pool to a host for multiple concurrent sessions that require the same source IP address for each session.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

## address-set

**Syntax**
```
address-set address-set-name {
    address address-name;
    address-set address-set-name;
    description text;
}
```

**Hierarchy Level** [edit security address-book *book-name*]

**Release Information** Statement introduced in Junos OS Release 8.5. Support for nested address sets introduced in Release 11.2 of Junos OS. The **description** option added in Junos OS Release 12.1.

**Description** Specify a collection of addresses, as defined in the **address (Address Book)** statement. Using address sets, you can organize addresses in logical groups and use them to easily configure other features, such as policies and NAT rules. Using this statement, you can also include a description for an address set.

You can also define address sets within address sets.

**Options** ***address-set-name*—**Name of the address set.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Address Books and Address Sets for Security Devices
- Security Zones and Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## address-whitelist

**Syntax** address-whitelist *list-name*;

**Hierarchy Level** [edit security utm feature-profile anti-spam]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Enter an address-whitelist (or blacklist) custom-object for local list spam filtering.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

## admin-email

**Syntax** admin-email *email-address*;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine pattern-update email-notify]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update email-notify]
[edit security utm feature-profile anti-virus sophos-engine pattern-update email-notify]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** You can configure the device to notify a specified administrator when patterns are updated. This is an email notification with a custom message and a custom subject line.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Express Antivirus Protection for Security Devices
- UTM Full Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## administrator

**Syntax**

```
administrator {
  e-mail-address e-mail-address ;
}
```

**Hierarchy Level** [edit security pki ca-profile *ca-profile-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify an administrator e-mail address to which the certificate request is sent.

**Options** **e-mail-address** ***e-mail-address*** —E-mail address where the certificate request is sent. By default, there is no preset e-mail address.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Certificates and Public Key Cryptography for Security Devices

## administrator-email (Security Fallback Block)

**Syntax** administrator-email *email-address*;

**Hierarchy Level**
[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options fallback-block]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** Configure the administrator e-mail address that will be notified when a fallback-block occurs. This is an e-mail notification with a custom message and a custom subject line.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## administrator-email (Security Virus Detection)

**Syntax** administrator-email *email address*;

**Hierarchy Level** [edit security utm feature-profile anti-virus sophos-engine profile *profile name* notification-options virus-detection]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Configure the administrator e-mail address that will be notified when a virus is detected by Sophos antivirus. This is an e-mail notification with a custom message and a custom subject line.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

## aging

**Syntax**
```
aging {
  early-ageout seconds;
  high-watermark percent;
  low-watermark percent;
}
```

**Hierarchy Level** [edit security flow]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Direct the device to begin aggressively aging out sessions when the percentage of entries in the session table exceeds the high-watermark setting and then stops when the percentage of sessions falls below the low-watermark setting.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Flow-Based Processing for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## alarm-threshold

**Syntax** alarm-threshold *number*;

**Hierarchy Level** [edit security screen ids-option *screen-name* tcp syn-flood]

**Release Information** Statement modified in Junos OS Release 9.2.

**Description** Define the number of half-complete proxy connections per second at which the device makes entries in the event alarm log.

**Options** *number* —Threshold value.
**Range:** 1 through 500,000 per second
**Default:** 1024 per second



NOTE: For SRX Series devices the applicable range is 1 through 1,000,000 per second.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## alarm-without-drop

**Syntax** alarm-without-drop;

**Hierarchy Level** [edit security screen ids-option *screen-name*]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Direct the device to generate an alarm when detecting an attack but not block the attack. Use this statement to allow an attack to enter a segment of your network that you have previously prepared to receive it (for example, a honeynet, which is a decoy network with extensive monitoring capabilities).

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## alarms (Security)

**Syntax**

```
alarms {
  audible {
    continuous;
  }
  potential-violation {
    authentication failures;
    cryptographic-self-test;
    decryption-failures {
      threshold value;
    }
    encryption-failures {
      threshold value;
    }
    idp;
    ike-phase1-failures {
      threshold value;
    }
    ike-phase2-failures {
      threshold value;
    }
    key-generation-self-test;
    non-cryptographic-self-test;
    policy {
      application {
        duration interval;
        size count;
        threshold value;
      }
      destination-ip {
        duration interval;
        size count;
        threshold value;
      }
      policy match {
        duration interval;
        size count;
        threshold value;
      }
      source-ip {
        duration interval;
        size count;
        threshold value;
      }
    }
    replay-attacks {
      threshold value;
    }
    security-log-percent-full percentage;
  }
}
```

**Hierarchy Level** [edit security]

Copyright © 2013, Juniper Networks, Inc.

**Release Information** Statement introduced in Junos OS Release 11.2.

**Description** Configures security alarms.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## alert

**Syntax** alert;

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* then notification]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then notification]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Release 10.0 of Junos OS.

**Description** Set an alert flag in the Alert column of the Log Viewer for the matching log record.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- Application-Level Distributed Denial of Service
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## alg

**Syntax**

```
alg {
  alg-manager {
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
  alg-support-lib {
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
  dns {
    disable;
    doctoring (none | sanity-check);
    maximum-message-length number;
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
  ftp {
    allow-mismatch-ip-address;
    disable;
    ftps-extension;
    line-break-extension;
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
  h323 {
    application-screen {
      message-flood {
        gatekeeper {
          threshold rate;
        }
      }
      unknown-message {
        permit-nat-applied;
        permit-routed;
      }
    }
    disable;
    dscp-rewrite {
      code-point string;
    }
```

Copyright © 2013, Juniper Networks, Inc.

```
    endpoint-registration-timeout value-in-seconds;
    media-source-port-any;
    traceoptions {
      flag flag <detail | extensive | terse>;
    }
  }
  ike-esp-nat {
    enable;
    esp-gate-timeout value-in-seconds;
    esp-session-timeout value-in-seconds;
    state-timeout value-in-seconds;
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
  mgcp {
    application-screen {
      connection-flood {
        threshold rate;
      }
      message-flood {
        threshold rate;
      }
      unknown-message {
        permit-nat-applied;
        permit-routed;
      }
    }
    disable;
    dscp-rewrite {
      code-point string;
    }
    inactive-media-timeout value-in-seconds;
    maximum-call-duration value-in-minutes;
    traceoptions {
      flag flag <extensive>;
    }
    transaction-timeout value-in-seconds;
  }
  msrpc {
    disable;
    traceoptions {
      flag {
        all <extensive>;
      }
    }
  }
  pptp {
    disable;
    traceoptions {
      flag {
        all <extensive>;
      }
    }
```


Copyright © 2013, Juniper Networks, Inc.

```
}
real {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
rsh {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
rtsp {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
sccp {
    application-screen {
        call-flood {
            threshold rate;
        }
        unknown-message {
            permit-nat-applied;
            permit-routed;
        }
    }
    disable;
    dscp-rewrite {
        code-point string;
    }
    inactive-media-timeout value-in-seconds;
    traceoptions {
        flag flag <extensive>;
    }
}
sip {
    application-screen {
        protect {
            deny {
                all {
                    timeout value-in-seconds;
                }
                destination-ip address;
                timeout value-in-seconds;
            }
        }
        unknown-message {
```

```
            permit-nat-applied;
            permit-routed;
        }
    }
    c-timeout value-in-minutes;
    disable;
    dscp-rewrite {
        code-point string;
    }
    inactive-media-timeout value-in-seconds;
    maximum-call-duration value-in-minutes;
    retain-hold-resource;
    t1-interval value-in-milliseconds;
    t4-interval value-in-seconds;
    traceoptions {
        flag flag <detail | extensive | terse>;
    }
}
sql {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
sunrpc {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
talk {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
tftp {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        (no-world-readable | world-readable);
```


Copyright © 2013, Juniper Networks, Inc.

```
        size maximum-file-size;
      }
      level (brief | detail | extensive | verbose);
      no-remote-trace;
    }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure an Application Layer Gateway (ALG) on the device. An ALG runs as a service and can be associated in policies with specified types of traffic. ALGs are enabled by default.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Device and Routing Operations Monitoring
- Troubleshooting for Security Devices
- Application Layer Gateways for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## ike-esp-nat

**Syntax**

```
ike-esp-nat {
  enable;
  esp-gate-timeout value-in-seconds;
  esp-session-timeout value-in-seconds;
  state-timeout value-in-seconds;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configures Application Layer Gateway (ALG) for Internet Key Exchange (IKE) and Encapsulating Security Payload (ESP) traffic with Network Address Translation (NAT).

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- ALG for IKE and ESP for Security Devices

## alg-manager

**Syntax**

```
alg-manager {
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

**Hierarchy Level** [edit security alg]

**Description** Configures Application Layer Gateway (ALG) manager.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Layer Gateways for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## support-lib

**Syntax**

```
alg-support-lib {
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configures the Application Layer Gateway (ALG) support library.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Layer Gateways for Security Devices

## algorithm (Security)

**Syntax** algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);

**Hierarchy Level** [edit security ipsec vpn *vpn-name* manual encryption]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Select the encryption algorithm for the internal Routing-Engine-to-Routing-Engine IPsec security association (SA) configuration. (This statement is not supported on dynamic VPN implementations.)

**Options**
- **3des-cbc**—3DES-CBC encryption algorithm.
- **aes-128-cbc**—AES-CBC 128-bit encryption algorithm.
- **aes-192-cbc**—AES-CBC 192-bit encryption algorithm.
- **aes-256-cbc**—AES-CBC 256-bit encryption algorithm.
- **des-cbc**—DES-CBC encryption algorithm.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## all-tcp

**Syntax** all-tcp mss *value*;

**Hierarchy Level** [edit security flow tcp-mss]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Set the TCP maximum segment size (MSS) value for all TCP packets for network traffic.

**Options** **mss *value***—TCP MSS value.
**Range:** 64 through 65,535 bytes

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Flow-Based Processing for Security Devices

## allow-dns-reply

**Syntax** allow-dns-reply;

**Hierarchy Level** [edit security flow]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Allow an incoming Domain Name Service (DNS) reply packet without a matched request. By default, if an incoming UDP first-packet has dst-port 53, the device checks the DNS message packet header to verify that the query bit (QR) is 0, which denotes a query message. If the QR bit is 1, which denotes a response message, the device drops the packet, does not create a session, and increments the illegal packet flow counter for the interface. Using the **allow-dns-reply** statement directs the device to skip the check.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Flow-Based Processing for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## allow-email (Security Fallback Block)

**Syntax** allow-email;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options fallback-block]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** Enable e-mail notification to notify a specified administrator when a fallback-block occurs.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

## allow-email (Security Virus Detection)

**Syntax** allow–email;

**Hierarchy Level** [edit security utm feature-profile anti-virus profile notification-options virus-detect]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Enable e-mail notification to notify a specified administrator when a virus is detected.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## allow-icmp-without-flow

**Syntax** (allow-icmp-without-flow | no-allow-icmp-without-flow);

**Hierarchy Level** [edit security idp sensor-configuration flow]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Allow an ICMP packet without matched request. By default the ICMP flow is enabled.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## always-send

**Syntax** always-send;

**Hierarchy Level** [edit security ike gateway *gateway-name* dead-peer-detection]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Instructs the device to send dead peer detection (DPD) requests regardless of whether there is outgoing IPsec traffic to the peer.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## analysis

**Syntax** analysis no-report;

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** By default, logging information is automatically reported with the J-Web reporting feature. Configure the **analysis** statement to turn off reporting.

**Options** **no-report**—Stops security analysis reporting.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Monitoring and Troubleshooting Guide for Security Devices*

## anomaly

**Syntax**
```
anomaly {
  direction (any | client-to-server | server-to-client);
  service service-name;
  shellcode (all | intel | no-shellcode | sparc);
  test test-condition;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Protocol anomaly attack objects detect abnormal or ambiguous messages within a connection according to the set of rules for the particular protocol being used.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## anti-spam (Security Feature Profile)

**Syntax**

```
anti-spam {
  address-blacklist list-name;
  address-whitelist list-name;
  sbl {
    profile profile-name {
      custom-tag-string [string];
      (sbl-default-server | no-sbl-default-server);
      spam-action (block | tag-header | tag-subject);
    }
  }
  traceoptions flag flag;
}
```

**Hierarchy Level** [edit security utm feature-profile]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure UTM antispam features.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

## anti-spam (Security UTM Policy)

**Syntax**

```
anti-spam {
  smtp-profile profile-name;
}
```

**Hierarchy Level** [edit security utm utm-policy *policy-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the antispam SMTP protocol and attach this policy to a security profile to implement it.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## anti-virus (Security Feature Profile)

**Syntax**

```
anti-virus {
  juniper-express-engine {
    pattern-update {
      email-notify {
        admin-email email-address;
        custom-message message;
        custom-message-subject message-subject;
      }
      interval value;
      no-autoupdate;
      proxy {
        password password-string;
        port port-number;
        server address-or-url;
        username name;
      }
      url url;
    }
    profile profile-name {
      fallback-options {
        content-size (block | log-and-permit);
        default (block | log-and-permit);
        engine-not-ready (block | log-and-permit);
        out-of-resources (block | (log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
      }
      notification-options {
        fallback-block {
          administrator-email email-address;
          allow-email;
          custom-message message;
          custom-message-subject message-subject;
          display-host;
          (notify-mail-sender | no-notify-mail-sender);
          type (message | protocol-only);
        }
        fallback-non-block {
          custom-message message;
          custom-message-subject message-subject;
          (notify-mail-recipient | no-notify-mail-recipient);
        }
        virus-detection {
          custom-message message;
          custom-message-subject message-subject;
          (notify-mail-sender | no-notify-mail-sender);
          type (message | protocol-only);
        }
      }
      scan-options {
        content-size-limit value;
        (intelligent-prescreening | no-intelligent-prescreening);
```

```
            timeout value;
        }
        trickling {
            timeout value;
        }
    }
}
kaspersky-lab-engine {
    pattern-update {
        email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
            password password-string;
            port port-number;
            server address-or-url;
            username name;
        }
        url url;
    }
    profile profile-name {
        fallback-options {
            content-size (block | log-and-permit);
            corrupt-file (block | log-and-permit);
            decompress-layer (block | log-and-permit);
            default (block | log-and-permit);
            engine-not-ready (block | log-and-permit);
            out-of-resources (block | (log-and-permit);
            password-file (block | (log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
        }
        notification-options {
            fallback-block {
                administrator-email email-address;
                allow-email;
                custom-message message;
                custom-message-subject message-subject;
                display-host;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
            fallback-non-block {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
```


Copyright © 2013, Juniper Networks, Inc.

```
        }
      }
      scan-options {
        content-size-limit value;
        decompress-layer-limit value;
        (intelligent-prescreening | no-intelligent-prescreening);
        scan-extension filename;
        scan-mode (all | by-extension);
        timeout value;
      }
      trickling {
        timeout value;
      }
    }
  }
  mime-whitelist {
    exception listname;
    list listname {
      exception listname;
    }
  }
  sophos-engine {
    pattern-update {
      email-notify {
        admin-email email-address;
        custom-message message;
        custom-message-subject message-subject;
      }
      interval value;
      no-autoupdate;
      proxy {
        password password-string;
        port port-number;
        server address-or-url;
        username name;
      }
      url url;
    }
    profile <name> {
      fallback-options {
        content-size (block | log-and-permit | permit);
        default (block | log-and-permit | permit);
        engine-not-ready (block | log-and-permit | permit);
        out-of-resources (block | log-and-permit | permit);
        timeout (block | log-and-permit | permit);
        too-many-requests (block | log-and-permit | permit);
      }
      notification-options {
        fallback-block {
          administrator-email email-address;
          allow-email;
          custom-message message;
          custom-message-subject message-subject;
          display-host;
          (notify-mail-sender | no-notify-mail-sender);
          type (message | protocol-only);
```

Copyright © 2013, Juniper Networks, Inc.

```
        }
        fallback-non-block {
          custom-message message;
          custom-message-subject message-subject;
          (notify-mail-recipient | no-notify-mail-recipient);
        }
        virus-detection {
          custom-message message;
          custom-message-subject message-subject;
          (notify-mail-sender | no-notify-mail-sender);
          type (message | protocol-only);
        }
      }
      scan-options {
        content-size-limit value;
        (no-uri-check | uri-check);
        timeout value;
      }
      trickling {
        timeout value;
      }
    }
    sxl-retry value;
    sxl-timeout seconds;
  }
  traceoptions flag flag;
  type (juniper-express-engine | kaspersky-lab-engine | sophos-engine);
  url-whitelist listname;
}
```

**Hierarchy Level** [edit security utm feature-profile]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure UTM antivirus full and express features.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## anti-virus (Security UTM Policy)

**Syntax**

```
anti-virus {
  ftp {
    download-profile profile-name;
    upload-profile profile-name;
  }
  http-profile profile-name;
  imap-profile profile-name;
  pop3-profile profile-name;
  smtp-profile profile-name;
}
```

**Hierarchy Level** [edit security utm utm-policy *policy-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the antivirus protocols and attach this policy to a security profile to implement it.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## apn

**Syntax**

```
apn pattern-string {
  imsi-prefix imsi-prefix-digits {
    action {
      drop;
      pass;
      selection (ms|net|vrf);
    }
  }
}
```

**Hierarchy Level** [edit security gprs gtp profile *profile-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS. Support for GTPv2 added in Release 11.4 of Junos OS. Option mcc-mnc replaced with imsi-prefix in Junos OS Release 12.1x44-D10.

**Description** Allow or deny access to specific access point names (APNs).

**Options**

- *pattern-string*—Set an APN suffix, such as “juniper.net.mcc123.mnc456.gprs”.
- *imsi-prefix-digits*—Specify an IMSI prefix.
- **drop**—Specify to deny GTP packets from all selection modes for the APN.
- **pass**—Specify to permit GTP packets from all selection modes for the APN.
- **selection**—Specify one of the following selection modes for the APN:
  - **ms**—The APN is provided by a Mobile Station (MS), and the user-subscription is not verified.
  - **net**—The APN is provided by a network, and the user-subscription is not verified.
  - **vrf**—The APN is provided by a network or an MS, and the user-subscription is verified.



NOTE: Because APN filtering is based on a perfect match, using the wildcard (*) when setting an APN suffix can prevent the inadvertent exclusion of APNs you would otherwise authorize. The security device automatically denies all other APNs that do not match, if the action is pass. You can only use the wildcard as the first character in the APN string.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- General Packet Radio Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## application (Security Alarms)

**Syntax**

```
application {
  duration interval;
  size count;
  threshold value;
}
```

**Hierarchy Level** [edit security alarms potential-violation policy]

**Release Information** Statement introduced in Junos OS Release 11.2.

**Description** Configure alarms for a number of policy violations to an application within a specified time period.

**Options**

- **duration *interval***—Indicate the duration of counters.

  **Range:** 1 through 3600 seconds.
  **Default:** 1 second.

- **size *count***—Indicate the number of applications for which policy violation checks can be done concurrently.

  **Range:** 1 through 10240.
  **Default:** 1024.

- **threshold *value***—Indicate the maximum number of application matches required to raise an alarm.

  **Range:** 1 through 4294967295.
  **Default:** 1000.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## application (Security Application-Level DDoS)

**Syntax** application (*application-name* | any | default);

**Hierarchy Level** [edit security idp idp-policy *idp-policy-name* rulebase-ddos rule *rule-name* match]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure the application or application-set name to match.

**Options**
- ***application-name***—Name of the application or application set to match.
- **any**—Match all ports to the only application implied in the attack objects.
- **default**—Match default and automatically detected ports to the applications implied in the attack object.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application-Level Distributed Denial of Service
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## application (Security Custom Attack)

**Syntax** application *application-name*;

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type chain protocol-binding]
[edit security idp custom-attack *attack-name* attack-type signature protocol-binding]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Allow IDP to match the attack for a specified application.

**Options** ***application-name***—Name of the application.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## application (Security IDP)

**Syntax** application *application-name*;

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match]

**Release Information** Statement introduced in Junos OS Release 9.2.

**Description** Specify an application or an application set name to match.

**Options** *application-name*—Name of the application.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## application (Security Policies)

**Syntax**
```
application {
  [application];
  any;
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the IP or remote procedure call (RPC) application or set of applications to be used as match criteria.

**Options** ***application-name-or-set***—Name of the application or application set used as match criteria.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policy
- Security Policies for Security Devices
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## application-ddos

**Syntax**

```
application-ddos application-name {
  connection-rate-threshold number;
  context context-name {
    exclude-context-values [value];
    hit-rate-threshold number;
    max-context-values number;
    time-binding-count number;
    time-binding-period seconds;
    value-hit-rate-threshold number;
  }
  service service-name;
}
```

**Hierarchy Level** [edit security idp]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure application-level distributed denial-of-service (DDoS) protection.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## application-ddos (Security IDP)

**Syntax**

```
application-ddos {
  statistics {
    interval minutes;
  }
}
```

**Hierarchy Level** [edit security idp sensor-configuration]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Enables Application-Level DDoS statistics collection.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application-Level Distributed Denial of Service

## application-ddos (Security IDP Policy)

**Syntax** application-ddos <*application-name*>;

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* match]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specifies the DDoS application.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application-Level Distributed Denial of Service

Copyright © 2013, Juniper Networks, Inc.

## application-firewall

**Syntax**

```
application-firewall {
  rule-sets rule-set-name {
    default-rule {
      (deny | permit);
    }
    rule rule-name {
      match {
        dynamic-application [system-application];
        dynamic-application-group [system-application-group];
      }
      then {
        (deny | permit);
      }
    }
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Configure application firewall rule sets with rules defining match criteria and the action to be performed.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Firewall
- Logical Systems for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## application-firewall (Application Services)

**Syntax**

```
application-firewall {
  rule-set rule-set-name;
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]

**Release Information** Statement introduced in Junos OS Release 11.1.

**Description** Configure application firewall rule sets with rules defining match criteria and the action to be performed.

**Options** **rule-set** *rule-set-name*—Name of the rule set that contains application firewall specification rules.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Firewall

## application-identification

**Syntax**

```
application-identification {
  max-packet-memory value;
  max-tcp-session-packet-memory value;
  max-udp-session-packet-memory value;
}
```

**Hierarchy Level** [edit security idp sensor-configuration]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Enable to identify the TCP/UDP application session running on nonstandard ports to match the application properties of transiting network traffic.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## application-proxy (Security UTM)

**Syntax**

```
application-proxy {
  traceoptions {
    flag flag;
  }
}
```

**Hierarchy Level** [edit security utm]

**Release Information** Statement introduced in Junos OS Release 9.5.

**Description** Configure trace options for the application proxy.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM Basics for Security Devices
- Unified Threat Management

## application-screen (Security H323)

**Syntax**

```
application-screen {
  message-flood {
    gatekeeper {
      threshold rate;
    }
  }
  unknown-message {
    permit-nat-applied;
    permit-routed;
  }
}
```

**Hierarchy Level** [edit security alg h323]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the security screens for the H.323 protocol Application Layer Gateway (ALG).

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Layer Gateways for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## application-screen (Security MGCP)

**Syntax**

```
application-screen {
  connection-flood {
    threshold rate;
  }
  message-flood {
    threshold rate;
  }
  unknown-message {
    permit-nat-applied;
    permit-routed;
  }
}
```

**Hierarchy Level** [edit security alg mgcp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the security screens for the Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG).

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- MGCP ALGs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## application-screen (Security SCCP)

**Syntax**

```
application-screen {
  call-flood {
    threshold rate;
  }
  unknown-message {
    permit-nat-applied;
    permit-routed;
  }
}
```

**Hierarchy Level** [edit security alg sccp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the security screens for the Skinny Client Control Protocol (SCCP) Application Layer Gateway (ALG).

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- SCCP ALGs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## application-screen (Security SIP)

**Syntax**

```
application-screen {
  protect {
    deny {
      all {
        timeout value-in-seconds;
      }
      destination-ip address;
      timeout value-in-seconds;
    }
  }
  unknown-message {
    permit-nat-applied;
    permit-routed;
  }
}
```

**Hierarchy Level** [edit security alg sip]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the security screens for the Session Initiation Protocol (SIP) Application Layer Gateway (ALG).

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- SIP ALGs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## application-services (Security Forwarding Process)

**Syntax**

```
application-services {
  maximize-alg-sessions;
  maximize-cp-sessions;
  maximize-idp-sessions {
    inline-tap;
    weight (equal | firewall | idp);
  }
  maximize-persistent-nat-capacity;
  session-distribution-mode {
    hash-based;
  }
}
```

**Hierarchy Level** [edit security forwarding-process]

**Release Information** Statement introduced in Release 9.6 of Junos OS.
Statement updated in Release 10.4 of Junos OS. Support for maximizing persistent NAT capacity added in Junos OS Release 12.1X44-D10.

**Description** You can configure the device to switch from an integrated firewall mode to maximize IDP mode to increase the capacity of IDP processing with the **maximize-idp-sessions** option. When you maximize IDP, you are decoupling IDP processes from firewall processes, allowing the device to support the same number of firewall and IDP sessions.

With the **maximize-cp-sessions** option you can increase the maximum number of central point sessions from 12.5 million sessions to 14 million sessions on a fully loaded SRX5800 device. Note that this option is supported only on SRX5800 devices. Using this optimization technique precludes other optimization methods, disables advanced GTP processing, and reduces routing capacity to 100K prefixes.

You can configure maximum ALG sessions by using the **maximize-alg-sessions** option. By default the session capacity number for RTSP, FTP, and TFTP ALG sessions is 10K per flow SPU. You must reboot the device (and its peer in chassis cluster mode) for the configuration to take effect. The **maximize-alg-sessions** option now enables you to increase defaults as follows:

- RTSP, FTP, and TFTP ALG session capacity: 25K per flow SPU
- TCP Proxy connection capacity: 40K per flow SPU



NOTE: Flow session capacity will be reduced to half per flow SPU and that the above capacity numbers will not change on CP-flow.

With the **maximize-persistent-nat-capacity** option you can increase the maximum persistent NAT binding capacity. The supported central point maximum binding capacity can be approximately increased to 1/8 of the central point session capacity up to 2M and


Copyright © 2013, Juniper Networks, Inc.

the supported SPU maximum binding capacity can be approximately increased to 1/4 of each of the SPU session capacity.

For example, a high-end SRX series device with 4 GB of memory can support a maximum of 2M persistent NAT binding capacity sessions on the central point and 275K on each of the SPU. You must reboot the device for the configuration to take effect.

Using this optimization technique reduces the number of flow sessions on both the central point and the SPU.

**Options** The remaining statements are explained separately.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Processing Overview for Security Devices
- IDP Policies for Security Devices

## application-services (Security Policies)

**Syntax**

```
application-services {
  application-firewall {
    rule-set rule-set-name;
  }
  application-traffic-control {
    rule-set rule-set-name;
  }
  gprs-gtp-profile profile-name;
  gprs-sctp-profile profile-name;
  idp;
  redirect-wx | reverse-redirect-wx;
  ssl-proxy {
    profile-name profile-name;
  }
  uac-policy {
    captive-portal captive-portal;
  }
  utm-policy policy-name;
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit]

**Release Information** Statement modified in Junos OS Release 11.1.

**Description** Enable application services within a security policy.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Firewall
- Application Quality of Service
- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## application-tracking

**Syntax**

```
application-tracking {
  disable;
  (first-update | first-update-interval first-update-interval);
  session-update-interval session-update-interval;
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Release 10.2 of Junos OS; support for disable added in Release 11.4 of Junos OS.

**Description** AppTrack, an application tracking tool, is a form of statistical profiling. Enabling this feature for a zone logs flow statistics (the byte count, packet count, and start and end times for a session) at session end. You can modify the logging time and log frequency with command options. Periodically, a network management tool, such as STRM, collects the logged statistics sent by each network device for bandwidth usage analysis of the network.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Tracking
- Logical Systems for Security Devices

## application-tracking (Security Zones)

**Syntax** application-tracking;

**Hierarchy Level** [edit security zones security-zone *zone-name*]

**Release Information** Statement introduced in Junos OS Release 10.2.

**Description** Enable application tracking support for the zone.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Tracking
- Security Zones and Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## application-traffic-control (Application Services)

**Syntax**
```
application-traffic-control {
  rule-set rule-set-name;
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]

**Release Information** Statement introduced in Junos OS Release 11.4.

**Description** Enables AppQoS, application-aware quality of service, as specified in the rules of the specified rule set.

**Options**
- **rule-set** ***rule-set-name***—Name of the rule set that contains application-aware traffic control specification rules.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Quality of Service
- Security Policies for Security Devices

## association-timeout

**Syntax** association-timeout *time-in-minutes*;

**Hierarchy Level** [edit security gprs sctp profile *profile-name*]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Set the association timeout for Stream Control Transmission Protocol (SCTP).

**Options** ***time-in-minutes***—Number of minutes of association time that elapse before the session is terminated. **Range:** 10 to 1440 (24 hours)

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- General Packet Radio Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## attach

**Syntax**

```
attach {
  zone zone-name;
}
```

**Hierarchy Level** [edit security address-book *book-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Attach a security zone to an address book. You do not need to attach a security zone to the global address book. The global address book is available by default.

**Options** **zone *zone-name*—**Name of a security zone to be attached to the address book.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Address Books and Address Sets for Security Devices

## attack-threshold

**Syntax** attack-threshold *number*;

**Hierarchy Level** [edit security screen ids-option *screen-name* tcp syn-flood]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Define the number of SYN packets per second required to trigger the SYN proxy response.

**Options** ***number*** —Number of SYN packets per second required to trigger the SYN proxy response.
**Range:** 1 through 500,000 per second
**Default:** 200 per second



NOTE: For SRX Series devices, the applicable range is 1 through 1.000,000 per second.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Configuration Statement Hierarchy
- destination-threshold on page 533

Copyright © 2013, Juniper Networks, Inc.

## attacks (Security Exempt Rulebase)

**Syntax**

```
attacks {
  custom-attack-groups [attack-group-name];
  custom-attacks [attack-name];
  dynamic-attack-groups [attack-group-name];
  predefined-attack-groups [attack-group-name];
  predefined-attacks [attack-name];
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify the attacks that you do not want the device to match in the monitored network traffic. Each attack is defined as an attack object, which represents a known pattern of attack.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## attacks (Security IPS Rulebase)

**Syntax**

```
attacks {
  custom-attack-groups [attack-group-name];
  custom-attacks [attack-name];
  dynamic-attack-groups [attack-group-name];
  predefined-attack-groups [attack-group-name];
  predefined-attacks [attack-name];
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify the attacks you want the device to match in the monitored network traffic. Each attack is defined as an attack object, which represents a known pattern of attack.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## attack-type (Security Anomaly)

**Syntax**

```
attack-type {
  anomaly {
    direction (any | client-to-server | server-to-client);
    service service-name;
    shellcode (all | intel | no-shellcode | sparc);
    test test-condition;
  }
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name*]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the type of attack.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## attack-type (Security Chain)

**Syntax**

```
attack-type {
  chain {
    expression boolean-expression;
    member member-name {
      attack-type {
        (anomaly ...same statements as in [edit security idp custom-attack attack-name
          attack-type anomaly] hierarchy level | signature ...same statements as in [edit
          security idp custom-attack attack-name attack-type signature] hierarchy level);
      }
    }
    order;
    protocol-binding {
      application application-name;
      icmp;
      icmpv6;
      ip {
        protocol-number transport-layer-protocol-number;
      }
      ipv6 {
        protocol-number transport-layer-protocol-number;
      }
      nested-application nested-application-name;
      rpc {
        program-number rpc-program-number;
      }
      tcp {
        minimum-port port-number <maximum-port port-number>;
      }
      udp {
        minimum-port port-number <maximum-port port-number>;
      }
    }
    reset;
    scope (session | transaction);
  }
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name*]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the type of attack.



NOTE: In a chain attack, you can configure multiple member attacks.

In an attack, under protocol binding TCP/UDP, you can specify multiple ranges of ports.

**Options** The remaining statements are explained separately.


Copyright © 2013, Juniper Networks, Inc.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## attack-type (Security IDP)

**Syntax**

```
attack-type {
anomaly {
  direction (any | client-to-server | server-to-client);
  shellcode (all | intel |no-shellcode | sparc);
  test-condition condition-name;
}
signature {
  context context-name;
  direction (any | client-to-server | server-to-client);
  negate;
  pattern signature-pattern;
  protocol {
    icmp {
      code {
        match (equal | greater-than | less-than | not-equal);
        value code-value;
      }
      data-length {
        match (equal | greater-than | less-than | not-equal);
        value data-length;
      }
      identification {
        match (equal | greater-than | less-than | not-equal);
        value identification-value;
      }
      sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number;
      }
      type {
        match (equal | greater-than | less-than | not-equal);
        value type-value;
      }
    }
    ipv4 {
      destination {
        match (equal | greater-than | less-than | not-equal);
        value ip-address-or-hostname;
      }
      identification {
        match (equal | greater-than | less-than | not-equal);
        value identification-value;
      }
      ip-flags {
        (df | no-df);
        (mf | no-mf);
        (rb | no-rb);
      }
      protocol {
        match (equal | greater-than | less-than | not-equal);
        value transport-layer-protocol-id;
      }
```


Copyright © 2013, Juniper Networks, Inc.

```
    source {
      match (equal | greater-than | less-than | not-equal);
      value ip-address-or-hostname;
    }
    tos {
      match (equal | greater-than | less-than | not-equal);
      value type-of-service-in-decimal;
    }
    total-length {
      match (equal | greater-than | less-than | not-equal);
      value total-length-of-ip-datagram;
    }
    ttl {
      match (equal | greater-than | less-than | not-equal);
      value time-to-live;
    }
  }
  ipv6 {
    destination {
      match (equal | greater-than | less-than | not-equal);
      value ip-address-or-hostname;
    }
    flow-label {
      match (equal | greater-than | less-than | not-equal);
      value flow-label-value;
    }
    hop-limit {
      match (equal | greater-than | less-than | not-equal);
      value hop-limit-value;
    }
    next-header {
      match (equal | greater-than | less-than | not-equal);
      value next-header-value;
    }
    payload-length {
      match (equal | greater-than | less-than | not-equal);
      value payload-length-value;
    }
    source {
      match (equal | greater-than | less-than | not-equal);
      value ip-address-or-hostname;
    }
    traffic-class {
      match (equal | greater-than | less-than | not-equal);
      value traffic-class-value;
    }
  tcp {
    ack-number {
      match (equal | greater-than | less-than | not-equal);
      value acknowledgement-number;
    }
    data-length {
      match (equal | greater-than | less-than | not-equal);
      value tcp-data-length;
    }
    destination-port {
```

```
        match (equal | greater-than | less-than | not-equal);
        value destination-port;
      }
      header-length {
        match (equal | greater-than | less-than | not-equal);
        value header-length;
      }
      mss {
        match (equal | greater-than | less-than | not-equal);
        value maximum-segment-size;
      }
      option {
        match (equal | greater-than | less-than | not-equal);
        value tcp-option;
      }
      sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number;
      }
      source-port {
        match (equal | greater-than | less-than | not-equal);
        value source-port;
      }
      tcp-flags {
        (ack | no-ack);
        (fin | no-fin);
        (psh | no-psh);
        (r1 | no-r1);
        (r2 | no-r2);
        (rst | no-rst);
        (syn | no-syn);
        (urg | no-urg);
      }
      urgent-pointer {
        match (equal | greater-than | less-than | not-equal);
        value urgent-pointer;
      }
      window-scale {
        match (equal | greater-than | less-than | not-equal);
        value window-scale-factor;
      }
      window-size {
        match (equal | greater-than | less-than | not-equal);
        value window-size;
      }
    }
    udp {
      data-length {
        match (equal | greater-than | less-than | not-equal);
        value data-length;
      }
      destination-port {
        match (equal | greater-than | less-than | not-equal);
        value destination-port;
      }
      source-port {
```


Copyright © 2013, Juniper Networks, Inc.

```
            match (equal | greater-than | less-than | not-equal);
            value source-port;
          }
        }
      }
      protocol-binding {
        application application-name;
        icmp;
        icmpv6;
        ip {
          protocol-number transport-layer-protocol-number;
        }
        ipv6 {
          protocol-number transport-layer-protocol-number;
        }
        nested-application nested-application-name;
        rpc {
          program-number rpc-program-number;
        }
        tcp {
          minimum-port port-number <maximum-port port-number>;
        }
        udp {
          minimum-port port-number <maximum-port port-number>;
        }
      }
      regexp regular-expression;
      shellcode (all | intel | no-shellcode | sparc);
    }
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type chain member *member-name*]

**Release Information** Statement introduced in Junos OS Release 9.3.

**Description** Specify the type of attack.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## attack-type (Security Signature)

**Syntax**

```
attack-type {
  signature {
    context context-name;
    direction (any | client-to-server | server-to-client);
    negate;
    pattern signature-pattern;
    protocol {
      icmp {
        code {
          match (equal | greater-than | less-than | not-equal);
          value code-value;
        }
        data-length {
          match (equal | greater-than | less-than | not-equal);
          value data-length;
        }
        identification {
          match (equal | greater-than | less-than | not-equal);
          value identification-value;
        }
        sequence-number {
          match (equal | greater-than | less-than | not-equal);
          value sequence-number;
        }
        type {
          match (equal | greater-than | less-than | not-equal);
          value type-value;
        }
      }
      ipv4 {
        destination {
          match (equal | greater-than | less-than | not-equal);
          value ip-address-or-hostname;
        }
        identification {
          match (equal | greater-than | less-than | not-equal);
          value identification-value;
        }
        ip-flags {
          (df | no-df);
          (mf | no-mf);
          (rb | no-rb);
        }
        protocol {
          match (equal | greater-than | less-than | not-equal);
          value transport-layer-protocol-id;
        }
        source {
          match (equal | greater-than | less-than | not-equal);
          value ip-address-or-hostname;
        }
        tos {
```


Copyright © 2013, Juniper Networks, Inc.

```
        match (equal | greater-than | less-than | not-equal);
        value type-of-service-in-decimal;
      }
      total-length {
        match (equal | greater-than | less-than | not-equal);
        value total-length-of-ip-datagram;
      }
      ttl {
        match (equal | greater-than | less-than | not-equal);
        value time-to-live;
      }
    }
    ipv6 {
      destination {
        match (equal | greater-than | less-than | not-equal);
        value ip-address-or-hostname;
      }
      flow-label {
        match (equal | greater-than | less-than | not-equal);
        value flow-label-value;
      }
      hop-limit {
        match (equal | greater-than | less-than | not-equal);
        value hop-limit-value;
      }
      next-header {
        match (equal | greater-than | less-than | not-equal);
        value next-header-value;
      }
      payload-length {
        match (equal | greater-than | less-than | not-equal);
        value payload-length-value;
      }
      source {
        match (equal | greater-than | less-than | not-equal);
        value ip-address-or-hostname;
      }
      traffic-class {
        match (equal | greater-than | less-than | not-equal);
        value traffic-class-value;
      }
    tcp {
      ack-number {
        match (equal | greater-than | less-than | not-equal);
        value acknowledgement-number;
      }
      data-length {
        match (equal | greater-than | less-than | not-equal);
        value tcp-data-length;
      }
      destination-port {
        match (equal | greater-than | less-than | not-equal);
        value destination-port;
      }
      header-length {
        match (equal | greater-than | less-than | not-equal);
```

```
            value header-length;
        }
        mss {
            match (equal | greater-than | less-than | not-equal);
            value maximum-segment-size;
        }
        option {
            match (equal | greater-than | less-than | not-equal);
            value tcp-option;
        }
        sequence-number {
            match (equal | greater-than | less-than | not-equal);
            value sequence-number;
        }
        source-port {
            match (equal | greater-than | less-than | not-equal);
            value source-port;
        }
        tcp-flags {
            (ack | no-ack);
            (fin | no-fin);
            (psh | no-psh);
            (r1 | no-r1);
            (r2 | no-r2);
            (rst | no-rst);
            (syn | no-syn);
            (urg | no-urg);
        }
        urgent-pointer {
            match (equal | greater-than | less-than | not-equal);
            value urgent-pointer;
        }
        window-scale {
            match (equal | greater-than | less-than | not-equal);
            value window-scale-factor;
        }
        window-size {
            match (equal | greater-than | less-than | not-equal);
            value window-size;
        }
    }
    udp {
        data-length {
            match (equal | greater-than | less-than | not-equal);
            value data-length;
        }
        destination-port {
            match (equal | greater-than | less-than | not-equal);
            value destination-port;
        }
        source-port {
            match (equal | greater-than | less-than | not-equal);
            value source-port;
        }
    }
}
```


Copyright © 2013, Juniper Networks, Inc.

```
    protocol-binding {
      application application-name;
      icmp;
      icmpv6;
      ip {
        protocol-number transport-layer-protocol-number;
      }
      ipv6 {
        protocol-number transport-layer-protocol-number;
      }
      nested-application nested-application-name;
      rpc {
        program-number rpc-program-number;
      }
      tcp {
        minimum-port port-number <maximum-port port-number>;
      }
      udp {
        minimum-port port-number <maximum-port port-number>;
      }
    }
    regexp regular-expression;
    shellcode (all | intel | no-shellcode | sparc);
  }
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name*]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the type of attack.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## audible (Security Alarms)

**Syntax**
```
audible {
  continuous;
}
```

**Hierarchy Level** [edit security alarms]

**Release Information** Statement modified in Junos OS Release 11.2.

**Description** Configure alarm to beep when a new security alarm is enabled.

**Options** **continuous**—Specify alarm to keep beeping until all security alarms are cleared.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## authentication (Security Alarms)

**Syntax** authentication *failures*;

**Hierarchy Level** [edit security alarms potential-violation]

**Release Information** Statement introduced in Junos OS Release 11.2.

**Description** Raise a security alarm when the device or switch detects a specified number of authentication failures (bad password attempts) before an alarm is raised.

This value must be equal to or less than the **tries-before-disconnect** setting at the **[edit system login retry-options]** hierarchy level; otherwise, the login session ends before the user reaches the alarmable threshold.

**Default** Multiple authentication failures do not cause an alarm to be raised.

**Options** *failures*—Number of authentication failures that causes an alarm to be raised.
**Range:** 1 through 10.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- retry-options
- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## authentication (Security IPsec)

**Syntax**

```
authentication {
  algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
  key (ascii-text key | hexadecimal key );
}
```

**Hierarchy Level** [edit security ipsec vpn *vpn-name* manual]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Configure IP Security (IPsec) authentication parameters for a manual security association (SA). (This statement is not supported on dynamic VPN implementations.)

**Options**

- **algorithm**—Hash algorithm that authenticates packet data. It can be one of the following:
  - **hmac-md5-96**—Produces a 128-bit digest.
  - **hmac-sha-256-128**—Produces a 256-bit digest.
  - **hmac-sha1-96**—Produces a 160-bit digest.
- **key**—Type of authentication key. It can be one of the following:
  - **ascii-text *key***—ASCII text key. For **hmac-md5-96**, the key is 16 ASCII characters; for **hmac-sha1-96**, the key is 20 ASCII characters.
  - **hexadecimal *key***—Hexadecimal key. For **hmac-md5-96**, the key is 32 hexadecimal characters; for **hmac-sha1-96**, the key is 40 hexadecimal characters.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## authentication-algorithm (Security)

**Syntax** authentication-algorithm (md5 | sha-256 | sha1);

**Hierarchy Level** [edit security group-vpn member ike proposal *proposal-name*]
[edit security group-vpn server ike proposal *proposal-name*]
[edit security ike proposal *proposal-name*]

**Release Information** Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

**Description** Configure the Internet Key Exchange (IKE) authentication algorithm.



NOTE:

- The device does not delete existing IPsec SAs when you update the **encryption-algorithm** configuration in the IKE proposal.
- The device deletes existing IPsec SAs when you update the **encryption-algorithm** configuration in the IPsec proposal.

**Options** **authentication-algorithm**—Hash algorithm that authenticates packet data. It can be one of three algorithms:

- **md5**—Produces a 128-bit digest.
- **sha-256**—Produces a 256-bit digest.
- **sha1**—Produces a 160-bit digest.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## authentication-algorithm (Security IPsec)

**Syntax** authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);

**Hierarchy Level** [edit security ipsec proposal *proposal-name*]
[edit security group-vpn server ipsec proposal *proposal-name*]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Configure the IPsec authentication algorithm.

**Options** The hash algorithm to authenticate data can be one of the following:

- **hmac-md5-96**—Produces a 128-bit authenticator value.
- **hmac-sha-256-128**—Produces a 256-bit authenticator value.
- **hmac-sha1-96**—Produces a 160-bit authenticator value.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## authentication-method

**Syntax** authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);

**Hierarchy Level** [edit security group-vpn member ike proposal *proposal-name*]
[edit security group-vpn server ike proposal *proposal-name*]
[edit security ike proposal *proposal-name*]

**Release Information** Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

**Description** Specify the method the device uses to authenticate the source of Internet Key Exchange (IKE) messages. The **pre-shared-keys** option refers to a preshared key, which is a key for encryption and decryption that both participants must have before beginning tunnel negotiations. The **rsa-signatures** and **dsa-signatures** options refer to two kinds of digital signatures, which are certificates that confirm the identity of the certificate holder. (The default method is a preshared key.) (The **rsa-signatures** and **dsa-signatures** options are not supported on dynamic VPN implementations.)



NOTE: The device does not delete existing IPsec SAs when you update the **authentication-method** configuration in the IKE proposal.

**Options**

- **dsa-signatures**—Specify that the Digital Signature Algorithm (DSA) is used.
- **pre-shared-keys**—Specify that a preshared key, which is a secret key shared between the two peers, is used during authentication to identify the peers to each other. The same key must be configured for each peer. This is the default method.
- **rsa-signatures**—Specify that a public key algorithm, which supports encryption and digital signatures, is used.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## authentication-source

**Syntax**

```
authentication-source {
    local-authentication-table (disable | priority priority);
    unified-access-control (disable | priority priority);
}
```

**Hierarchy Level** [edit security user-identification]

**Release Information** Statement introduced in Release 12.1 of Junos OS.

**Description** Identifies one or more tables to be used as the source for user role information.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Understanding User Role Firewalls
- Understanding the User Identification Table
- *Unified Access Control Solution Guide for SRX Series Services Gateways*

## auto-re-enrollment (Security)

**Syntax**

```
auto-re-enrollment {
    certificate-id certificate-id-name {
        ca-profile-name ca-profile-name ;
        challenge-password password ;
        re-enroll-trigger-time-percentage percentage ;
        re-generate-keypair;
    }
}
```

**Hierarchy Level** [edit security pki]

**Release Information** Statement modified in Release 9.0 of Junos OS.

**Description** Configure the automatic reenrollment of a certificate authority (CA) certificate.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Certificates and Public Key Cryptography for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## automatic (Security)

**Syntax**

```
automatic {
  download-timeout minutes;
  enable;
  interval hours;
  start-time start-time;
}
```

**Hierarchy Level** [edit security idp security-package]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Enable the device to automatically download the updated signature database from the specified URL.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices
- IDP Signature Database for Security Devices

## bind-interface

**Syntax** bind-interface *interface-name*;

**Hierarchy Level** [edit security ipsec vpn *vpn-name*]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Configure the tunnel interface to which the route-based virtual private network (VPN) is bound.

**Options** *interface-name* —Tunnel interface.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## block-command

**Syntax** block-command *protocol-command-list*;

**Hierarchy Level** [edit security utm feature-profile content-filtering profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Apply protocol block command custom-objects to the content-filtering profile.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## block-content-type

**Syntax** block-content-type (activex | exe | http-cookie | java-applet | zip);

**Hierarchy Level** [edit security utm feature-profile content-filtering profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Apply blocks to other available content such as exe, http-cookie, java-applet. This is for HTTP only.

**Options**
- **activex**—Block ActiveX.
- **exe**—Block EXE files.
- **http-cookie**—Block cookies.
- **java-applet**—Block Java applets.
- **zip**—Block ZIP files.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## block-extension

**Syntax** block-extension *extension-list*;

**Hierarchy Level** [edit security utm feature-profile content-filtering profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Apply block extensions to the content-filtering profile.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## block-message (Security UTM)

**Syntax**
```
block-message {
  type {
    custom-redirect-url;
  }
  url url;
}
```

**Hierarchy Level** [edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name*]

**Release Information** Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.4 for Enhanced Web Filtering.

**Description** Configure Juniper enhanced block message settings.

**Options**
- **type**—Specify the following type of the block message:
  - **custom-redirect-url**—Specify Custom redirect URL server.
- **url *url***—Specify an URL of the block message.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## block-mime

**Syntax**

```
block-mime {
    exception list-name;
    list list-name;
}
```

**Hierarchy Level** [edit security utm feature-profile content-filtering profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Apply MIME pattern list custom-objects to the content-filtering profile for blocking MIME types.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## bridge

**Syntax**

```
bridge {
  block-non-ip-all;
  bpdu-vlan-flooding;
  bypass-non-ip-unicast;
  no-packet-flooding {
    no-trace-route;
  }
}
```

**Hierarchy Level** [edit security flow]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Changes default Layer 2 forwarding behavior.

**Options**

- **block-non-ip-all**—Block all Layer 2 non-IP and non-ARP traffic, including multicast and broadcast traffic.
- **bpdu-vlan-flooding**—Set 802.1D bridge protocol data unit (BPDU) flooding based on VLAN.
- **bypass-non-ip-unicast**—Allow all Layer 2 non-IP traffic to pass through the device.
- **no-packet-flooding**—Stop IP flooding and send ARP or ICMP requests to discover the destination MAC address for a unicast packet.
  - **no-trace-route**—Do not send ICMP requests to discover the destination MAC address for a unicast packet. Only ARP requests are sent. This option only allows the device to discover the destination MAC address for a unicast packet if the destination IP address is in the same subnetwork as the ingress IP address.



NOTE: **The block-non-ip-all and bypass-non-ip-unicast options cannot be configured at the same time.**

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Flow-Based Processing for Security Devices
- Routing Protocols
- Layer 2 Bridging and Transparent Mode for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## c-timeout

**Syntax** c-timeout *value-in-minutes*;

**Hierarchy Level** [edit security alg sip]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the timeout interval for Session Initiation Protocol (SIP) transactions in minutes.

**Options** ***value-in-minutes***—Timeout interval.
**Range:** 3 through 10 minutes
**Default:** 3 minutes

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- SIP ALGs for Security Devices

## ca-identity (Security)

**Syntax** ca-identity *ca-identity*;

**Hierarchy Level** [edit security pki ca-profile *ca-profile-name*]

**Release Information** Statement modified in Release 11.1 of Junos OS.

**Description** Specify the certificate authority (CA) identity to use in requesting digital certificates.

**Options**
- ***ca-identity*** —Name of CA identity. This name is typically the domain name of the CA.
- ***routing-instance-name*** —Name of routing instance. The routing instance name is chosen from the list of configured routing instances.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Certificates and Public Key Cryptography for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## ca-profile (Security)

**Syntax**

```
ca-profile ca-profile-name {
  administrator {
    e-mail-address e-mail-address;
  }
  ca-identity ca-identity ;
  enrollment {
      retry number;
      retry-interval seconds;
      url url-name;
  }
  routing-instance routing-instance-name ;
  revocation-check {
    crl {
      disable {
        on-download-failure;
      }
      refresh-interval hours;
      url url-name;
    }
    disable;
  }
}
```

**Hierarchy Level** [edit security pki]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Configure certificate authority (CA) profile.

**Options** *ca-profile-name* —Name of a trusted CA.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Certificates and Public Key Cryptography for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ca-profile-name

**Syntax** ca-profile-name *ca-profile-name*;

**Hierarchy Level** [edit security pki auto-re-enrollment certificate-id *certificate-id-name*]

**Release Information** Statement modified in Release 9.0 of Junos OS.

**Description** Specify the name of the certificate authority (CA) profile.

**Options** ***ca-profile-name*** —Name of the specific CA profile.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Certificates and Public Key Cryptography for Security Devices

## cache

**Syntax**
```
cache {
  size value;
  timeout value;
}
```

**Hierarchy Level** [edit security utm feature-profile web-filtering surf-control-integrated]
[edit security utm feature-profile web-filtering juniper-enhanced]

**Release Information** Statement introduced in Release 9.5 of Junos OS for surf-control integrated.
Statement introduced in Release 11.4 of Junos OS for Enhanced Web Filtering.

**Description** Set the cache parameters for Surf-Control-Integrated Web filtering and Enhanced Web Filtering.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## cache (Security Log)

**Syntax**

```
cache {
  exclude exlude-name {
    destination-address destination-address;
    destination-port destination-port;
    event-id event-id;
    failure;
    interface-name interface-name;
    policy-name policy-name;
    process process-name;
    protocol protocol;
    source-address source-address;
    source-port source-address;
    success;
    user-name user-name;
  }
  limit value;
}
```

**Hierarchy Level** [edit security log]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Cache security log events in the audit log buffer.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- System Log Messages
- Security Logs
- CLI Statements and Commands
- Troubleshooting for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## cache-prune-chunk-size

**Syntax** cache-prune-chunk-size *number*;

**Hierarchy Level** [edit security idp sensor-configuration ssl-inspection]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Number of cache entries to delete when pruning SSL session ID cache.

**Options** ***cache-prune-chunk-size***—Number of cache entries to delete when pruning SSL session ID cache.

**Range:** 1 through 100000

**Default:** 10000

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- System Log Messages
- Security Logs
- CLI Statements and Commands
- Troubleshooting for Security Devices

## cache-size (Security)

**Syntax** cache-size *size*;

**Hierarchy Level** [edit security idp sensor-configuration log]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify the size in bytes for each user's log cache.

**Options** **size**—Cache size.

**Range:** 1 through 65,535 bytes

**Default:** 12800 bytes

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## call-flood

**Syntax**

```
call-flood {
    threshold rate;
}
```

**Hierarchy Level** [edit security alg sccp application-screen]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Limit the number of calls per second allowed to Skinny Client Control Protocol (SCCP) client. Calls exceeding the threshold are dropped by the SCCP Application Layer Gateway (ALG).

**Options**

**threshold *rate***—Number of calls per second per client.

**Range:** 2 through 1000

**Default:** 20

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## capture-file (Security)

**Syntax**

```
capture-file {
  filename;
  files number;
  format pacp-format;
  size maximum-file-size;
  (world-readable | no-world-readable);
}
```

**Hierarchy Level** [edit security datapath-debug]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Sets packet capture for performing the datapath-debug action.

**Options**

- ***filename***—Name of the file to receive the output of the packet capturing operation.
- **files**—Maximum number of capture files.

  If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

  Range: 1 through 10 files
- **format**—Describes the format of the capture file. The default format file is pcap. You can also set it as private (binary) format.
- **size**—Describes the size limit of the capture file.

  If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and a filename.

  Range: 10 KB through 100 MB
- **world-readable** | **no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The world-readable option enables any user to read the file. To explicitly set the default behavior, use the no-world-readable option.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security IDP
- System Log Messages
- Security Logs
- Troubleshooting for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## category (Security Dynamic Attack Group)

**Syntax**

```
category {
  values [category-value];
}
```

**Hierarchy Level** [edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify a category filter to add attack objects based on the category.

**Options** **values**—Name of the category filter. You can configure multiple filters separated by spaces and enclosed in square brackets.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## category (Security Logging)

**Syntax** category (all | content-security)

**Hierarchy Level** [edit security log stream *stream-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Set the category of logging to **all** or **content-security**. Note that for the WELF format, the category must be set to **content-security**.



NOTE: On SRX3400, SRX3600, SRX5600, and SRX 5800 devices, if the stream configuration does not specify a destination port, the default destination port will be the syslog port. If you specify a destination port in the stream configuration, then that port will be used instead.

**Options**

- **all**— All events are logged.
- **content-security**—Only content security events are logged.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Log File Formats
- Application Tracking
- Master Administrator for Logical Systems on Security Devices

Copyright © 2013, Juniper Networks, Inc.

## category (Security Web Filtering)

**Syntax**

```
category customurl-list name {
    action (block | log-and-permit | permit | quarantine);
}
```

**Hierarchy Level**

[edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name*]
[edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name*]

**Release Information**

Statement introduced in Release 9.5 of Junos OS.
Statement introduced in Release 11.4 of Junos OS for Enhanced Web Filtering.

**Description**

Select a custom URL category list you created (custom objects) for filtering against.


Copyright © 2013, Juniper Networks, Inc.

Table 4: List of categories predefined by websense

| Category ID | Category Name | Parent ID |
|---|---|---|
| 1 | Adult Material | 0 |
| 2 | Business and Economy | 0 |
| 3 | Education | 0 |
| 4 | Government | 0 |
| 5 | News and Media | 0 |
| 6 | Religion | 0 |
| 7 | Society and Lifestyles | 0 |
| 8 | Special Events | 0 |
| 9 | Information Technology | 0 |
| 10 | Abortion | 0 |
| 11 | Advocacy Groups | 0 |
| 12 | Entertainment | 0 |
| 13 | Gambling | 0 |
| 14 | Games | 0 |
| 15 | Illegal or Questionable | 0 |
| 16 | Job Search | 0 |
| 17 | Shopping | 0 |
| 18 | Sports | 0 |
| 19 | Tasteless | 0 |
| 20 | Travel | 0 |
| 21 | Vehicles | 0 |
| 22 | Violence | 0 |
| 23 | Weapons | 0 |
| 24 | Drugs | 0 |

Copyright © 2013, Juniper Networks, Inc.

Table 4: List of categories predefined by websense *(continued)*

| Category ID | Category Name | Parent ID |
|---|---|---|
| 25 | Militancy and Extremist | 0 |
| 26 | Racism and Hate | 0 |
| 27 | Health | 0 |
| 28 | URL Translation Sites | 9 |
| 29 | Advertisements | 110 |
| 64 | User-Defined | 0 |
| 65 | Nudity | 1 |
| 66 | Adult Content | 1 |
| 67 | Sex | 1 |
| 68 | Financial Data and Services | 2 |
| 69 | Cultural Institutions | 3 |
| 70 | MP3 and Audio Download Services | 12 |
| 72 | Military | 4 |
| 73 | Political Organizations | 4 |
| 74 | General Email | 91 |
| 75 | Proxy Avoidance | 9 |
| 76 | Search Engines and Portals | 9 |
| 78 | Web Hosting | 9 |
| 79 | Web Chat | 91 |
| 80 | Hacking | 9 |
| 81 | Alternative Journals | 5 |
| 82 | Non-Traditional Religions and Occult and Folklore | 6 |
| 83 | Traditional Religions | 6 |
| 84 | Restaurants and Dining | 7 |


Copyright © 2013, Juniper Networks, Inc.

Table 4: List of categories predefined by websense *(continued)*

| Category ID | Category Name | Parent ID |
|---|---|---|
| 85 | Gay or Lesbian or Bisexual Interest | 7 |
| 86 | Personals and Dating | 7 |
| 87 | Alcohol and Tobacco | 7 |
| 88 | Prescribed Medications | 24 |
| 89 | Supplements and Unregulated Compounds | 24 |
| 90 | Abused Drugs | 24 |
| 91 | Internet Communication | 0 |
| 92 | Pro-Choice | 10 |
| 93 | Pro-Life | 10 |
| 94 | Sex Education | 1 |
| 95 | Lingerie and Swimsuit | 1 |
| 96 | Online Brokerage and Trading | 110 |
| 97 | Educational Institutions | 3 |
| 98 | Instant Messaging | 110 |
| 99 | Freeware and Software Download | 110 |
| 100 | Pay-to-Surf | 110 |
| 101 | Internet Auctions | 17 |
| 102 | Real Estate | 17 |
| 103 | Hobbies | 7 |
| 107 | Sport Hunting and Gun Clubs | 18 |
| 108 | Internet Telephony | 116 |
| 109 | Streaming Media | 116 |
| 110 | Productivity | 0 |
| 111 | Marijuana | 24 |

Copyright © 2013, Juniper Networks, Inc.

Table 4: List of categories predefined by websense *(continued)*

| Category ID | Category Name | Parent ID |
|---|---|---|
| 112 | Message Boards and Forums | 110 |
| 113 | Personal Network Storage and Backup | 116 |
| 114 | Internet Radio and TV | 116 |
| 115 | Peer-to-Peer File Sharing | 116 |
| 116 | Bandwidth | 0 |
| 117 | Social Networking and Personal Sites | 7 |
| 118 | Educational Materials | 3 |
| 121 | Reference Materials | 3 |
| 122 | Social Organizations | 0 |
| 123 | Service and Philanthropic Organizations | 122 |
| 124 | Social and Affiliation Organizations | 122 |
| 125 | Professional and Worker Organizations | 122 |
| 126 | Security | 0 |
| 128 | Malicious Web Sites | 126 |
| 138 | Computer Security | 9 |
| 146 | Miscellaneous | 0 |
| 147 | Images | 146 |
| 148 | Image Servers | 146 |
| 149 | Private IP Addresses | 146 |
| 150 | Content Delivery Networks | 146 |
| 151 | Dynamic Content | 146 |
| 152 | Network Errors | 146 |
| 153 | Uncategorized | 146 |
| 154 | Spyware | 126 |


Copyright © 2013, Juniper Networks, Inc.

Table 4: List of categories predefined by websense *(continued)*

| Category ID | Category Name | Parent ID |
|---|---|---|
| 156 | File Download Servers | 146 |
| 164 | Phishing and Other Frauds | 126 |
| 166 | Keyloggers | 126 |
| 167 | Potentially Unwanted Software | 126 |
| 172 | Bot Networks | 126 |
| 191 | Extended Protection | 0 |
| 192 | Elevated Exposure | 191 |
| 193 | Emerging Exploits | 191 |
| 194 | Potentially Damaging Content | 191 |
| 195 | Organizational Email | 91 |
| 196 | Text and media messaging | 91 |
| 200 | Web and Email Spam | 9 |

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## certificate

**Syntax**

```
certificate {
  local-certificate certificate-id;
  peer-certificate-type (pkcs7 | x509-signature);
}
```

**Hierarchy Level**

[edit security group-vpn member ike policy *policy-name*]
[edit security group-vpn server ike policy *policy-name*]
[edit security ike policy *policy-name*]

**Release Information**

Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

**Description**

Specify usage of a digital certificate to authenticate the virtual private network (VPN) initiator and recipient. (This statement is not supported on dynamic VPN implementations.)

**Options**

The remaining statements are explained separately.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

## certificate-id (Security)

**Syntax**

```
certificate-id certificate-id-name {
  ca-profile-name ca-profile-name;
  challenge-password password;
  re-enroll-trigger-time-percentage percentage;
  re-generate-keypair;
}
```

**Hierarchy Level**

[edit security pki auto-re-enrollment]

**Release Information**

Statement modified in Release 9.0 of Junos OS.

**Description**

Specify the certificate authority (CA) certificate to use for automatic reenrollment.

**Options**

***certificate-id-name*** —Identifier of the certificate that needs automatic reenrollment.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Certificates and Public Key Cryptography for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## certificates

**Syntax**

```
certificates {
  cache-size bytes;
  cache-timeout-negative seconds;
  certification-authority profile-name {
    ca-name name;
    crl filename;
    encoding (binary | pem);
    enrollment-url url;
    file filename;
    ldap-url url;
  }
  enrollment-retry number;
  local name {
    certificate;
    load-key-file url;
  }
  maximum-certificates number;
  path-length length;
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced before Release 12.1 of Junos OS.

**Description** Configure X.509 certificate information.

**Options**

- **cache-size** ***bytes***—Maximum size, in bytes, of the certificate cache. Enter a value from 64 through 4,294,967,295.
- **cache-timeout-negative** ***seconds***—Number of seconds to cache negative responses. Enter a value from 10 through 4,294,967,295.
- **enrollment-retry** ***number***—Number of retry attempts for an enrollment request. Enter a value from 0 through 1080.
- **maximum-certificates** ***number***—Maximum number of certificates to cache. Enter a value from 64 through 4,294,967,295.
- **path-length** ***length***—Maximum certificate path length. Enter a value from 0 through 15.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- System Log Messages
- Security Logs
- Troubleshooting for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## certification-authority

**Syntax**

```
certification-authority profile-name {
    ca-name name;
    crl filename;
    encoding (binary | pem);
    enrollment-url url;
    file filename;
    ldap-url url;
}
```

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before Release 12.1 of Junos OS.

**Description** Configure certification authority (CA) for X.509 certificate.

**Options**

- *profile-name*—Name of this CA configuration.
- **ca-name *name***—Name of the CA.
- **crl *filename***—Certificate revocation list (CRL) filename.
- **encoding**—Certificate encoding, either **binary** or **pem** (privacy-enhanced mail).
- **enrollment-url *url***—Enrollment URL.
- **file *filename***—Certificate filename.
- **ldap-url *url***—Lightweight Directory Access Protocol (LDAP) URL.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- System Log Messages
- Security Logs
- Troubleshooting for Security Devices
- Security Basics


Copyright © 2013, Juniper Networks, Inc.

## chain

**Syntax**

```
chain {
  expression boolean-expression;
  member member-name {
    attack-type {
      (anomaly ...same statements as in [edit security idp custom-attack attack-name
        attack-type anomaly] hierarchy level | signature ...same statements as in [edit security
        idp custom-attack attack-name attack-type signature] hierarchy level);
    }
  }
  order;
  protocol-binding {
    application application-name;
    icmp;
    icmpv6;
    ip {
      protocol-number transport-layer-protocol-number;
    }
    ipv6 {
      protocol-number transport-layer-protocol-number;
    }
    nested-application nested-application-name;
    rpc {
      program-number rpc-program-number;
    }
    tcp {
      minimum-port port-number <maximum-port port-number>;
    }
    udp {
      minimum-port port-number <maximum-port port-number>;
    }
  }
  reset;
  scope (session | transaction);
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Chain attack object combines multiple signatures and/or protocol anomalies into a single object. Traffic must match all of the combined signatures and/or protocol anomalies to match the chain attack object.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## challenge-password (Security)

**Syntax** challenge-password *password*;

**Hierarchy Level** [edit security pki auto-re-enrollment certificate-id *certificate-id-name*]

**Release Information** Statement modified in Release 9.0 of Junos OS.

**Description** Specify the password used by the certificate authority (CA) for enrollment and revocation. If the CA does not provide the challenge password, choose your own password.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Certificates and Public Key Cryptography for Security Devices

## clear-threshold

**Syntax** clear-threshold *clear-threshold*;

**Hierarchy Level** [edit security nat source pool-utilization-alarm]

**Release Information** Statement modified in Junos OS Release 9.2.

**Description** Configure the lower threshold at which an SNMP trap is triggered when pool utilization for a source pool without Port Address Translation (PAT) falls below the threshold.

**Options** ***clear-threshold*** —Threshold at which an SNMP trap is triggered.
**Range:** 40 through 100

**Required Privilege Level** security–To view this statement in the configuration.
security-control–To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## clients (Security)

**Syntax**

```
clients configuration-name {
  ipsec-vpn vpn-name;
  remote-exceptions ip-address/mask;
  remote-protected-resources ip-address/mask;
  user username;
  user-groups user-group-name;
}
```

**Hierarchy Level** [edit security dynamic-vpn]

**Release Information** Statement introduced in Junos OS Release 9.5.

**Description** Create a client configuration for the dynamic VPN feature. Within the configuration, specify a name for the configuration, reference a standard VPN configuration to use for IPsec negotiations, specify which resources to protect, define any exceptions, and list the users to which the dynamic VPN configuration applies.

**Options** ***configuration-name***—Name of the client configuration.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Dynamic VPNs for Security Devices

## co-location

**Syntax** co-location;

**Hierarchy Level** [edit security group-vpn]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Specifies that the group server and group member functions coexist in the same device. The group server and group member must have different IP addresses so that packets can be delivered properly. In colocation mode, there can only be one IP address assigned to the server and one IP address assigned to the member across groups.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Group VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## code

**Syntax**

```
code {
  match (equal | greater-than | less-than | not-equal);
  value code-value;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol icmp]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the secondary code that identifies the function of the request/reply within a given type.

**Options**

- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***code-value***—Match a decimal value.

  **Range:** 0 through 255

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## config-check (Security Dynamic VPN)

**Syntax** config-check;

**Hierarchy Level** [edit security dynamic-vpn]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Enable extra dynamic VPN configuration checking. If you include this statement in your configuration, it is automatically enabled. If the statement is not present in your configuration, the configuration check option is not enabled.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Dynamic VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## connection-flood

**Syntax**

```
connection-flood {
  threshold rate;
}
```

**Hierarchy Level** [edit security alg mgcp application-screen]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Limit the number of new connection requests allowed per Media Gateway (MG) per second. Messages exceeding the threshold are dropped by the Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG).

**Options**

**threshold *rate***—Number of connection requests per second allowed per MG.

**Range:** 2 through 10000

**Default:** 200

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Layer Gateways for Security Devices

## connection-rate-threshold

**Syntax** connection-rate-threshold *number*;

**Hierarchy Level** [edit security idp application-ddos *application-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure the connections-per-second threshold at which to start monitoring the application context values for application-level DDoS protection.

**Options**

**threshold *number***—connection rate requests per second.

**Range:**

- SRX3400/3600– 1 to 200,000
- SRX5600/5800–1 to 400,000

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service

Copyright © 2013, Juniper Networks, Inc.

## connections-limit

**Syntax** connections-limit *number*;

**Hierarchy Level** [edit security ike gateway *gateway-name* dynamic]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the number of concurrent connections that the group profile supports. When the maximum number of connections is reached, no more dynamic virtual private network (VPN) endpoints dialup users attempting to access an IPsec VPN are allowed to begin Internet Key Exchange (IKE) negotiations.

**Options** ***number***—Maximum number of concurrent connections allowed.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IPsec VPNs for Security Devices
- System Log Messages
- Security Logs
- Troubleshooting for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## container

**Syntax** container *container-string*;

**Hierarchy Level** [edit security group-vpn server ike gateway *gateway-name* dynamic distinguished-name]
[edit security ike gateway *gateway-name* dynamic distinguished-name]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn server** hierarchy added in Release 10.2 of Junos OS.

**Description** Specify that the value in the identity fields of a dynamic virtual private network (VPN) endpoint user's distinguished name exactly match the values in the group IKE user's distinguished name. The order of the identity fields in the fields of the distinguished name strings must be identical when matching. (This statement is not supported on dynamic VPN implementations.)

**Options** ***container-string***—Distinguished name identity value to be matched. For example, **cn**=admin, **ou**=eng, **o**=juniper, **dc**=net.



NOTE: **Add a space between each container string. For example, edit security ike gateway jsr_gateway dynamic distinguished-name container o=juniper, ou=eng;**

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices
- System Log Messages
- Security Logs
- Troubleshooting for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## content-decompression-max-memory-kb

**Syntax** content-decompression-max-memory-kb *value*;

**Hierarchy Level** [edit security idp sensor-configuration ips]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Set the maximum memory allocation in kilobytes for content decompression.

The default memory allocation provides 33 KB per session for an average number of sessions requiring decompression at the same time. To determine if this value is consistent with your environment, analyze values from decompression-related counters and the total number of IDP sessions traversing the device. Estimate the number of sessions requiring decompression at the same time. Assuming that each of these sessions requires 33 KB of memory for decompression, compare your estimated needs to the default value.



NOTE: Because content decompression requires a significant allocation of memory, system performance will be impacted by increasing the maximum memory allocation for decompression.

**Options** **Range:** 50 through 2,000,000 KB

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## content-decompression-max-ratio

**Syntax** content-decompression-max-ratio *value*;

**Hierarchy Level** [edit security idp sensor-configuration ips]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Set the maximum decompression ratio of the size of decompressed data to the size of compressed data.

Some attacks are introduced through compressed content. When the content is decompressed, it can inflate to a very large size taking up valuable system resources resulting in denial of service. This type of attack can be recognized by the ratio of the size of decompressed data to the size of compressed data. Keep in mind, however, that a higher ratio lessens the chance of detecting this type of attack.

**Options** **Range:** 1 through 128

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## content-filtering (Security Feature Profile)

**Syntax**

```
content-filtering {
  profile profile-name {
    block-command protocol-command-list;
    block-content-type (activex | exe | http-cookie | java-applet | zip);
    block-extension extension-list;
    block-mime {
      exception list-name;
      list list-name;
    }
    notification-options {
      custom-message message;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
    permit-command protocol-command-list;
  }
  traceoptions flag flag;
}
```

**Hierarchy Level** [edit security utm feature-profile]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure UTM content-filtering features.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Content Filtering for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## content-filtering (Security UTM Policy)

**Syntax**

```
content-filtering {
  ftp {
    download-profile profile-name;
    upload-profile profile-name;
  }
  http-profile profile-name;
  imap-profile profile-name;
  pop3-profile profile-name;
  smtp-profile profile-name;
}
```

**Hierarchy Level** [edit security utm utm-policy *policy-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the content-filtering protocols and attach this policy to a security profile to implement it.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM Content Filtering for Security Devices
- Unified Threat Management

Copyright © 2013, Juniper Networks, Inc.

## content-size

**Syntax** content-size (block | log-and-permit);

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* fallback-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** If the content size exceeds a set limit, the content is either passed or blocked. The default action is log-and-permit.



NOTE: When you configure the content-size value, keep in mind that in certain cases, content size is available in the protocol headers, so the max-content-size fallback is applied before a scan request is sent. However, in many cases, content size is not provided in the protocol headers. In these cases, the TCP payload is sent to the antivirus scanner and accumulates until the end of the payload. If the accumulated payload exceeds the maximum content size value, then max-content-size fallback is applied. The default fallback action is log and permit, so you may want to change this option to block, in which case such a packet is dropped and a block message is sent to the client.

**Options**
- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## content-size (Security Antivirus Sophos Engine)

**Syntax** content-size (block | log-and-permit | permit);

**Hierarchy Level** [edit security utm feature-profile anti-virus sophos-engine profile *profile-name* fallback-options]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** If the content size exceeds a set limit, the content is either passed or blocked.



NOTE: When you configure the content-size value, keep in mind that in certain cases, content size is available in the protocol headers, so the max-content-size fallback is applied before a scan request is sent. However, in many cases, content size is not provided in the protocol headers. In these cases, the TCP payload is sent to the antivirus scanner and accumulates until the end of the payload. If the accumulated payload exceeds the maximum content size value, then max-content-size fallback is applied. You might want to set the fallback action to block, in which case such a packet is dropped and a block message is sent to the client.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## content-size-limit

**Syntax** content-size-limit *value*;

**Hierarchy Level**
[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* scan-options]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* scan-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** The content size check occurs before the scan request is sent. The content size refers to accumulated TCP payload size.

Range: 20 through 20,000

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## context (Security Application-Level DDoS)

**Syntax**

```
context context-name {
    exclude-context-values [value];
    hit-rate-threshold number;
    max-context-values number;
    time-binding-count number;
    time-binding-period seconds;
    value-hit-rate-threshold number;
}
```

**Hierarchy Level** [edit security idp application-ddos *application-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure the name of the application context that the IDP protocol decoder generates while parsing the application protocol from traffic data.

**Options** ***context-name***—Name of the protocol context under which the attack has to be matched.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service

## context (Security Custom Attack)

**Syntax** context *context-name*;

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Define the location of the signature where IDP should look for the attack in a specific Application Layer protocol.

**Options** ***context-name***—Name of the context under which the attack has to be matched.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## corrupt-file

**Syntax** corrupt-file (block | log-and-permit);

**Hierarchy Level** [edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* fallback-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Corrupt file is the error returned by the scan engine when engine detects a corrupted file. The default action is log-and-permit.

**Options**
- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## count (Security Custom Attack)

**Syntax** count *count-value*;

**Hierarchy Level** [edit security idp custom-attack *attack-name* time-binding]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the number of times that IDP detects the attack within the specified scope before triggering an event.

**Options** ***count-value***—Number of times IDP detects the attack.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## count (Security Policies)

**Syntax**

```
count {
  alarm {
    per-minute-threshold number;
    per-second-threshold number;
  }
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Enable a count, in bytes or kilobytes, of all network traffic the security policy allows to pass through the device.

**Options** **alarm**—Enable alarm.

- **per-minute-threshold** ***number*** —Alarm threshold in kilobytes per minute. The range is from 0 through 4294967295.
- **per-second-threshold** ***number*** —Alarm threshold in bytes per second. The range is from 0 through 4294967295.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## crl (Security)

**Syntax**

```
crl {
  disable {
    on-download-failure;
  }
  refresh-interval hours;
  url url-name;
}
```

**Hierarchy Level** [edit security pki ca-profile *ca-profile-name* revocation-check]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.

**Options**

- **disable on-download-failure**—(Optional) Override the default behavior and permit certificate verification even if the CRL fails to download.
- **refresh-interval** *hours*—Time interval, in hours, between CRL updates.

  Range — 0 through 8784 hours.
- **url** ***url-name*** —Name of the location from which to retrieve the CRL through HTTP or Lightweight Directory Access Protocol (LADP). You can specify one URL for each configured CA profile. By default, no location is specified. Use a fully qualified domain name (FQDN) or an IP address and, optionally, a port number. If no port number is specified, port 80 is used for HTTP and port 443 is used for LDAP.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Certificates and Public Key Cryptography for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## cryptographic-self-test

**Syntax** cryptographic-self-test;

**Hierarchy Level** [edit security alarms potential-violation ]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Raise a security alarm when the device or switch detects a cryptographic self-test failure. Cryptographic self-tests are a set of preoperational tests that are performed after the device or switch is powered on. The self-test run without operator intervention.

**Default** No alarm is raised upon failure of a cryptographic self-test.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## custom-attack

**Syntax**

```
custom-attack attack-name {
  attack-type {
    anomaly {
      direction (any | client-to-server | server-to-client);
      service service-name;
      shellcode (all | intel | no-shellcode | sparc);
      test test-condition;
    }
    chain {
      expression boolean-expression;
      member member-name {
        attack-type {
          (anomaly ...same statements as in [edit security idp custom-attack attack-name
            attack-type anomaly] hierarchy level | signature ...same statements as in [edit
            security idp custom-attack attack-name attack-type signature] hierarchy level);
        }
      }
      order;
      protocol-binding {
        application application-name;
        icmp;
        icmpv6;
        ip {
          protocol-number transport-layer-protocol-number;
        }
        ipv6 {
          protocol-number transport-layer-protocol-number;
        }
        nested-application nested-application-name;
        rpc {
          program-number rpc-program-number;
        }
        tcp {
          minimum-port port-number <maximum-port port-number>;
        }
        udp {
          minimum-port port-number <maximum-port port-number>;
        }
      }
      reset;
      scope (session | transaction);
    }
    signature {
      context context-name;
      direction (any | client-to-server | server-to-client);
      negate;
      pattern signature-pattern;
      protocol {
        icmp {
          code {
            match (equal | greater-than | less-than | not-equal);
            value code-value;
```


Copyright © 2013, Juniper Networks, Inc.

```
    }
    data-length {
      match (equal | greater-than | less-than | not-equal);
      value data-length;
    }
    identification {
      match (equal | greater-than | less-than | not-equal);
      value identification-value;
    }
    sequence-number {
      match (equal | greater-than | less-than | not-equal);
      value sequence-number;
    }
    type {
      match (equal | greater-than | less-than | not-equal);
      value type-value;
    }
  }
  ipv4 {
    destination {
      match (equal | greater-than | less-than | not-equal);
      value ip-address-or-hostname;
    }
    identification {
      match (equal | greater-than | less-than | not-equal);
      value identification-value;
    }
    ip-flags {
      (df | no-df);
      (mf | no-mf);
      (rb | no-rb);
    }
    protocol {
      match (equal | greater-than | less-than | not-equal);
      value transport-layer-protocol-id;
    }
    source {
      match (equal | greater-than | less-than | not-equal);
      value ip-address-or-hostname;
    }
    tos {
      match (equal | greater-than | less-than | not-equal);
      value type-of-service-in-decimal;
    }
    total-length {
      match (equal | greater-than | less-than | not-equal);
      value total-length-of-ip-datagram;
    }
    ttl {
      match (equal | greater-than | less-than | not-equal);
      value time-to-live;
    }
  }
  ipv6 {
    destination {
      match (equal | greater-than | less-than | not-equal);
```

```
        value ip-address-or-hostname;
    }
    flow-label {
        match (equal | greater-than | less-than | not-equal);
        value flow-label-value;
    }
    hop-limit {
        match (equal | greater-than | less-than | not-equal);
        value hop-limit-value;
    }
    next-header {
        match (equal | greater-than | less-than | not-equal);
        value next-header-value;
    }
    payload-length {
        match (equal | greater-than | less-than | not-equal);
        value payload-length-value;
    }
    source {
        match (equal | greater-than | less-than | not-equal);
        value ip-address-or-hostname;
    }
    traffic-class {
        match (equal | greater-than | less-than | not-equal);
        value traffic-class-value;
    }
tcp {
    ack-number {
        match (equal | greater-than | less-than | not-equal);
        value acknowledgement-number;
    }
    data-length {
        match (equal | greater-than | less-than | not-equal);
        value tcp-data-length;
    }
    destination-port {
        match (equal | greater-than | less-than | not-equal);
        value destination-port;
    }
    header-length {
        match (equal | greater-than | less-than | not-equal);
        value header-length;
    }
    mss {
        match (equal | greater-than | less-than | not-equal);
        value maximum-segment-size;
    }
    option {
        match (equal | greater-than | less-than | not-equal);
        value tcp-option;
    }
    sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number;
    }
    source-port {
```


Copyright © 2013, Juniper Networks, Inc.

```
            match (equal | greater-than | less-than | not-equal);
            value source-port;
          }
          tcp-flags {
            (ack | no-ack);
            (fin | no-fin);
            (psh | no-psh);
            (r1 | no-r1);
            (r2 | no-r2);
            (rst | no-rst);
            (syn | no-syn);
            (urg | no-urg);
          }
          urgent-pointer {
            match (equal | greater-than | less-than | not-equal);
            value urgent-pointer;
          }
          window-scale {
            match (equal | greater-than | less-than | not-equal);
            value window-scale-factor;
          }
          window-size {
            match (equal | greater-than | less-than | not-equal);
            value window-size;
          }
        }
        udp {
          data-length {
            match (equal | greater-than | less-than | not-equal);
            value data-length;
          }
          destination-port {
            match (equal | greater-than | less-than | not-equal);
            value destination-port;
          }
          source-port {
            match (equal | greater-than | less-than | not-equal);
            value source-port;
          }
        }
      }
      protocol-binding {
        application application-name;
        icmp;
        icmpv6;
        ip {
          protocol-number transport-layer-protocol-number;
        }
        ipv6 {
          protocol-number transport-layer-protocol-number;
        }
        nested-application nested-application-name;
        rpc {
          program-number rpc-program-number;
        }
        tcp {
```

```
            minimum-port port-number <maximum-port port-number>;
          }
          udp {
            minimum-port port-number <maximum-port port-number>;
          }
        }
        regexp regular-expression;
        shellcode (all | intel | no-shellcode | sparc);
      }
    }
    recommended-action (close | close-client | close-server | drop | drop-packet | ignore |
      none);
    severity (critical | info | major | minor | warning);
    time-binding {
      count count-value;
      scope (destination | peer | source);
    }
}
```

**Hierarchy Level** [edit security idp]

**Release Information** Statement modified in Release 9.3 of Junos OS.

**Description** Configure custom attack objects to detect a known or unknown attack that can be used to compromise your network.

**Options** ***attack-name***—Name of the custom attack object.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## custom-attack-group

**Syntax**

```
custom-attack-group custom-attack-group-name {
  group-members [attack-or-attack-group-name];
}
```

**Hierarchy Level** [edit security idp]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Configure custom attack group. A custom attack group is a list of attacks that would be matched on the traffic if the group is selected in a policy.

**Options** ***custom-attack-group-name***—Name of the custom attack group.

The remaining statement is explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## custom-attack-groups (Security IDP)

**Syntax** custom-attack-groups *attack-group-name*;

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match attacks]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match attacks]

**Release Information** Statement introduced in Junos OS Release 9.2.

**Description** Specify a name for the custom attack group.

**Options** *attack-group-name*—Name of the custom attack group.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## custom-attacks

**Syntax** custom-attacks [*attack-name*];

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match attacks],
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match attacks]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Select custom attacks defined under [**edit security idp custom-attack**] by specifying their names.

**Options** ***attack-name***—Name of the new custom attack object.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## custom-block-message

**Syntax** custom-block-message *value*;

**Hierarchy Level** [edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name*]
[edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.
Statement introduced in Release 11.4 of Junos OS for Enhanced Web Filtering.

**Description** Enter a custom message to be sent when HTTP requests are blocked.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## custom-message (Security Content Filtering)

**Syntax** custom-message *message*;

**Hierarchy Level** [edit security utm feature-profile content-filtering profile *profile-name* notification-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Custom message notifications are generally used when content is blocked by the content filter.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices

## custom-message (Security Email Notify)

**Syntax** custom-message *message*;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine pattern-update email-notify]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update email-notify]
[edit security utm feature-profile anti-virus sophos-engine pattern-update email-notify]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** You can configure the device to notify a specified administrator when patterns are updated. This is an email notification with a custom message.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## custom-message (Security Fallback Block)

**Syntax** custom-message *message*;

**Hierarchy Level**
[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options fallback-block]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## custom-message (Security Fallback Non-Block)

**Syntax** custom-message *message*;

**Hierarchy Level**
[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options fallback-non-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options fallback-non-block]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options fallback-non-block]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## custom-message (Security Virus Detection)

**Syntax** custom-message *message*;

**Hierarchy Level**
[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options virus-detection]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options virus-detection]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

## custom-message-subject (Security Email Notify)

**Syntax** custom-message-subject *message-subject*;

**Hierarchy Level**
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update email-notify]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update email-notify]
[edit security utm feature-profile anti-virus sophos-engine pattern-update email-notify]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** You can configure the device to notify a specified administrator when patterns are updated. This is an email notification with a custom message and a custom subject line.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## custom-message-subject (Security Fallback Block)

**Syntax** custom-message-subject *message-subject*;

**Hierarchy Level**
[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options fallback-block]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file. As part of a custom message, you can customize the message subject line.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## custom-message-subject (Security Fallback Non-Block)

**Syntax** custom-message-subject *message-subject*;

**Hierarchy Level**
[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options fallback-non-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options fallback-non-block]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options fallback-non-block]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file. As part of a custom message, you can customize the message subject line.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## custom-message-subject (Security Virus Detection)

**Syntax** custom-message-subject *message-subject*;

**Hierarchy Level**
[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options virus-detection]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options virus-detection]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** Custom message notifications are mainly used in file replacement or in a response message when the antivirus scan result is to drop the file. As part of a custom message, you can customize the message subject line.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## custom-objects

**Syntax**

```
custom-objects {
  custom-url-category object-name {
    value [value];
  }
  filename-extension object-name {
    value [value];
  }
  mime-pattern object-name {
    value [value];
  }
  protocol-command object-name {
    value [value];
  }
  url-pattern object-name {
    value [value];
  }
}
```

**Hierarchy Level** [edit security utm]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure custom objects before configuring UTM feature-profile features.



WARNING: Custom category does not take precedence over pre-defined categories when it has the same name as one of the pre-defined categories. It is recommended not to have a custom category name be the same as the predefined category name.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Content Filtering for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## custom-tag-string

**Syntax** custom-tag-string [*string*];

**Hierarchy Level** [edit security utm feature-profile anti-spam sbl profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a custom string for identifying a message as spam.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## custom-url-category

**Syntax**

```
custom-url-category object-name {
  value [value];
}
```

**Hierarchy Level** [edit security utm custom-objects]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Use URL pattern lists to create Custom URL category lists. These are lists of patterns that bypass scanning.



WARNING: Custom category does not take precedence over pre-defined categories when it has the same name as one of the pre-defined categories. It is recommended not to have a custom category name be the same as the predefined category name.

**Options**

- ***object-name***—Name of the URL category-list object.
- **value *value***—Value of the URL category-list object. You can configure multiple values separated by spaces and enclosed in square brackets.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- Understanding UTM Custom Objects
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## data-length

**Syntax**

```
data-length {
  match (equal | greater-than | less-than | not-equal);
  value tcp-data-length;
}
```

**Hierarchy Level**

[edit security idp custom-attack *attack-name* attack-type signature protocol udp]
[edit security idp custom-attack *attack-name* attack-type signature protocol icmp]
[edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

**Release Information**

Statement introduced in Release 9.3 of Junos OS.

**Description**

Specify the number of bytes in the data payload. In the TCP header, for SYN, ACK, and FIN packets, this field should be empty.

**Options**

- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***data-length***—Match the number of bytes in the data payload.

  **Range:** 0 through 65,535

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## datapath-debug

**Syntax**

```
datapath-debug {
  action-profile profile-name {
    event (jexec | lbt | lt-enter | lt-leave | mac-egress | mac-ingress | np-egress | np-ingress
      | pot) {
      count;
      packet-dump;
      packet-summary;
      trace;
    }
    module {
      flow {
        flag {
          all;
        }
      }
    }
    preserve-trace-order;
    record-pic-history;
  }
  capture-file {
    filename;
    files number;
    format pacp-format;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  maximum-capture-size value;
  packet-filter packet-filter-name {
    action-profile (profile-name | default);
    destination-port (port-range | protocol-name);
    destination-prefix destination-prefix;
    interface logical-interface-name;
    protocol (protocol-number | protocol-name;
    source-port (port-range | protocol- name);
    source-prefix source-prefix;
    }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    no-remote-trace;
  }
}
```

**Hierarchy Level** [edit security]

**Release Information** Command introduced in Release 10.0 of Junos OS.


Copyright © 2013, Juniper Networks, Inc.

**Description** Configure the data path debugging options.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Master Administrator for Logical Systems on Security Devices

## dead-peer-detection

**Syntax**
```
dead-peer-detection {
  always-send;
  interval seconds;
  threshold number;
}
```

**Hierarchy Level** [edit security ike gateway *gateway-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable the device to use dead peer detection (DPD). DPD is a method used by devices to verify the current existence and availability of IPsec peer devices. A device performs this verification by sending encrypted IKE Phase 1 notification payloads (R-U-THERE) to peers and waiting for DPD acknowledgements (R-U-THERE-ACK).

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## decompress-layer

**Syntax** decompress-layer (block | log-and-permit);

**Hierarchy Level** [edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* fallback-options]

**Description** Decompress layer error is the error returned by the scan engine when the scanned file has too many compression layers. The default action is block.

**Options**
- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## decompress-layer-limit

**Syntax** decompress-layer-limit *value*;

**Hierarchy Level** [edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* scan-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** The decompression layer limit specifies how many layers of nested compressed files and files with internal extractable objects, such as archive files (tar), the internal antivirus scanner can decompress before it executes the virus scan.

Range: 1 through 4

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## decryption-failures

**Syntax**

```
decryption-failures {
  threshold value;
}
```

**Hierarchy Level** [edit security alarms potential-violation]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Raise a security alarm after exceeding a specified number of decryption failures.

**Default** Multiple decryption failures do not cause an alarm to be raised.

**Options** *failures*—Number of decryption failures up to which an alarm is not raised. When the configured number is exceeded, an alarm is raised.

**Range:** 0 through 1 through 1000000000.

**Default:** 1000

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices
- Troubleshooting for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## default (Security UTM)

**Syntax** default (block |log-and-permit | permit);

**Hierarchy Level** [edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name*]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Specify the default action to take for a URL.

**Options**
- block—Log the error and deny the traffic.
- log-and-permit—Log the error and permit the traffic.
- permit—Permit the traffic.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

## default (Security Antivirus)

**Syntax** default (block | log-and-permit);

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* fallback-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** All errors other than those specifically listed fall into this category. This could include either unhandled system exceptions (internal errors) or other unknown errors.

**Options**
- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## default (Security Antivirus Sophos Engine)

**Syntax** default (block | log-and-permit | permit);

**Hierarchy Level** [edit security utm feature-profile anti-virus sophos-engine profile *profile-name* fallback-options]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** All errors other than those specifically listed fall into this category. This could include either unhandled system exceptions (internal errors) or other unknown errors.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## default (Security Web Filtering)

**Syntax** default (block | log-and-permit | permit | quarantine);

**Hierarchy Level**
[edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name* fallback-settings]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name* fallback-settings]
[edit security utm feature-profile web-filtering juniper–local profile *profile-name* fallback-settings]
[edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name* fallback-settings]

**Release Information**
Statement introduced in Release 9.5 of Junos OS.
Statement introduced in Release 11.4 of Junos OS for Enhanced Web Filtering.

**Description** Specify an action for the profile, for requests that experience internal errors in the Web-filtering module.

**Options**
- block—Log the error and deny the traffic
- log-and-permit—Log the error and permit the traffic
- permit —Permit the traffic.
- quarantine—Show the warning message and permit/block the traffic based on user input.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## default-policy

**Syntax** default-policy (deny-all | permit-all);

**Hierarchy Level** [edit security policies]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Configure the default security policy that defines the actions the device takes on a packet that does not match any user-defined policy.

**Options** **deny-all**—Deny all traffic. Packets are dropped. This is the default.

**permit-all**—Permit all traffic that does not match a policy.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## default-rule

**Syntax**

```
default-rule {
   (deny | permit | reject);
}
```

**Hierarchy Level** [edit security application-firewall rule-sets *rule-set-name*]

**Release Information** Statement introduced in Junos OS Release 11.1. Statement updated in Junos OS Release 12.1X44-D10 with the **reject** option.

**Description** Configure the default rule that defines the actions to be performed on a packet that does not match any defined rule.

Note that an application firewall is applied after a session has already been created by the security firewall. When traffic is rejected or denied by an application firewall, therefore, logs contain a session open message, a session reject or deny message, and a session close message.

**Options**

- **deny**—Block the traffic at the firewall. The device drops the packet. No message is returned to the sender.
- **permit**—Permit traffic at the firewall.
- **reject**—Block the traffic at the firewall. For TCP traffic, the device drops the packet and returns a TCP reset (RST) message to the source host and to the server in some cases. For UDP and other protocol traffic, the device drops the packet and returns an ICMP "destination unreachable, port unreachable" message to both the client and the server.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Firewall

## deny (Security Policies)

**Syntax**

```
deny;
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Block the service at the firewall. The device drops the packets.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## deny (Security SIP)

**Syntax**

```
deny {
  all {
    timeout value-in-seconds;
  }
  destination-ip address;
  timeout value-in-seconds;
}
```

**Hierarchy Level** [edit security alg sip application-screen protect]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Protect servers against INVITE attacks.

**Options**

- **all**—Configure the Session Initiation Protocol (SIP) application screen to protect servers at all destination IP addresses against INVITE attacks.
- **destination-ip *address***—Configure the SIP application screen to protect the server at this destination IP address against INVITE attacks. You can include up to 16 destination IP addresses of servers to be protected. Enabling this option disables the all option.
- **timeout *value-in-seconds***—Amount of time (in ***seconds*** ) to make an attack table entry for each INVITE, which is listed in the application screen.

  **Range:** 1 through 3600 seconds

  **Default:** 5 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- SIP ALGs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## description (Security Address Book)

**Syntax** description *text*;

**Hierarchy Level** [edit security address-book *book-name*]

**Release Information** Statement introduced in Release 12.1 of Junos OS.

**Description** Specify descriptive text for an address book.



NOTE: The descriptive text should not include characters, such as “<”, “>”, “&”, or “\n”.

**Options** ***text***—Descriptive text about an address book.

**Range:** 1 through 300 characters



NOTE: The upper limit of the description text range is related to character encoding, and is therefore dynamic. However, if you configure the descriptive text length beyond 300 characters, the configuration might fail to take effect.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Address Books and Address Sets for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## description (Security IDP Policy)

**Syntax** description *text*;

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name*]
[edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name*]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name*]

**Release Information** Statement modified in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Release 10.0 of Junos OS.

**Description** Specify descriptive text for an exempt rule, or IPS rule.

**Options** ***text***—Descriptive text about an exempt rule, or IPS rule.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- Application-Level Distributed Denial of Service
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## description (Security NAT Pool)

**Syntax** description *text*;

**Hierarchy Level** [edit security nat destination pool *pool-name*]
[edit security nat source pool *pool-name*]

**Release Information** Statement introduced in Junos OS Release 12.1.

**Description** Specify descriptive text for a source or destination NAT pool.



NOTE: The descriptive text should not include characters, such as “<”, “>”, “&”, or “\n”.

**Options** ***text***—Descriptive text about a source or destination NAT pool.

**Range:** 1 through 300 characters



NOTE: The upper limit of the description text range is related to character encoding, and is therefore dynamic. However, if you configure the descriptive text length beyond 300 characters, the configuration might fail to take effect.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## description (Security NAT Rule)

**Syntax** description *text*;

**Hierarchy Level** [edit security nat destination rule-set *rule-set-name* rule *rule-name*]
[edit security nat source rule-set *rule-set-name* rule *rule-name*]
[edit security nat static rule-set *rule-set-name* rule *rule-name*]

**Release Information** Statement introduced in Junos OS Release 12.1.

**Description** Specify descriptive text for a source, destination, or static NAT rule.



NOTE: The descriptive text should not include characters, such as “<”, “>”, “&”, or “\n”.

**Options** *text*—Descriptive text about a source, destination, or static NAT rule.

**Range:** 1 through 300 characters



NOTE: The upper limit of the description text range is related to character encoding, and is therefore dynamic. However, if you configure the descriptive text length beyond 300 characters, the configuration might fail to take effect.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## description (Security NAT Rule-Set)

**Syntax** description *text*;

**Hierarchy Level** [edit security nat destination rule-set *rule-set-name*]
[edit security nat source rule-set *rule-set-name*]
[edit security nat static rule-set *rule-set-name*]

**Release Information** Statement introduced in Junos OS Release 12.1.

**Description** Specify descriptive text for a source, destination, or static NAT rule set.

NOTE: The descriptive text should not include characters, such as “<”, “>”, “&”, or “\n”.

**Options** *text*—Descriptive text about a source, destination, or static NAT rule set.

**Range:** 1 through 300 characters

NOTE: The upper limit of the description text range is related to character encoding, and is therefore dynamic. However, if you configure the descriptive text length beyond 300 characters, the configuration might fail to take effect.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## description (Security Policies)

**Syntax** description *description*;

**Hierarchy Level**
[edit security group-vpn member ike policy *policy-name*]
[edit security group-vpn member ike proposal *proposal-name*]
[edit security group-vpn server ike policy *policy-name*]
[edit security group-vpn server ipsec proposal *proposal-name*]
[edit security group-vpn server ike proposal *proposal-name*]
[edit security ike policy *policy-name*],
[edit security ike proposal *proposal-name*],
[edit security ipsec policy *policy-name*],
[edit security ipsec proposal *proposal-name*]
[edit security polices from-zone *zone-name* to-zone *zone-name* policy *policy-name*]

**Release Information** Statement modified in Junos OS Release 8.5. Support for **group-vpn** hierarchies added in Junos OS Release 10.2. Support for the **security policies** hierarchy added in Junos OS Release 12.1.

**Description** Specify descriptive text for an IKE policy, an IPsec policy, an IKE proposal, an IPsec proposal, or a security policy.

**Options** ***description*** —Descriptive text about an IKE policy, an IPsec policy, an IKE proposal, an IPsec proposal, or a security policy.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPNs for Security Devices
- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## description (Security Screen)

**Syntax** description *text*;

**Hierarchy Level** [edit security screen ids-option *screen-name*]

**Release Information** Statement introduced in Release 12.1 of Junos OS.

**Description** Specify descriptive text for a screen.



NOTE: The descriptive text should not include characters, such as “<”, “>”, “&”, or “\n”.

**Options** ***text***—Descriptive text about a screen.

**Range:** 1 through 300 characters



NOTE: The upper limit of the description text range is related to character encoding, and is therefore dynamic. However, if you configure the descriptive text length beyond 300 characters, the configuration might fail to take effect.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Configuration Statement Hierarchy


Copyright © 2013, Juniper Networks, Inc.

## description (Security Zone)

**Syntax** description *text*;

**Hierarchy Level** [edit security zones functional-zone management]
[edit security zones security-zone *zone-name*]

**Release Information** Statement introduced in Junos OS Release 12.1.

**Description** Specify descriptive text for a security zone.



NOTE: The descriptive text should not include characters, such as “<”, “>”, “&”, or “\n”.

**Options** *text*—Descriptive text about a security zone.

**Range:** 1 through 300 characters



NOTE: The upper limit of the description text range is related to character encoding, and is therefore dynamic. However, if you configure the descriptive text length beyond 300 characters, the configuration might fail to take effect.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Zones and Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## destination (Security Destination NAT)

**Syntax**

```
destination {
  pool pool-name {
    address ip-address {
      (port port-number | to ip-address);
    }
    description text;
    routing-instance routing-instance-name;
  }
  rule-set rule-set-name {
    description text;
    from {
      interface [interface-name];
      routing-instance [routing-instance-name];
      zone [zone-name];
    }
    rule rule-name {
      description text;
      match {
        (destination-address <ip-address> | destination-address-name <address-name>);
        destination-port port-number;
        protocol [(protocol-name | protocol-number)];
        source-address [ip-address];
        source-address-name [address-name];
      }
      then {
        destination-nat (off | pool pool-name);
      }
    }
  }
}
```

**Hierarchy Level** [edit security nat]

**Release Information** Statement modified in Junos OS Release 9.6. The **description** option added in Junos OS Release 12.1.

**Description** Configure destination NAT, which allows you to configure the following:

- Translate destination IP address or addresses to a specific IP address.
- Translate destination IP address or addresses and port number(s) to a specific IP address and one port number.
- Translate a range of destination IP addresses to another range of IP addresses. This mapping is one-to-one, static, and without PAT.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.


Copyright © 2013, Juniper Networks, Inc.

**Related Documentation**
- Network Address Translation for Security Devices

## destination (Security IP Headers Attack)

**Syntax**

```
destination {
  match (equal | greater-than | less-than | not-equal);
  value ip-address-or-hostname;
}
```

**Hierarchy Level**

[edit security idp custom-attack *attack-name* attack-type signature protocol ipv4]
[edit security idp custom-attack *attack-name* attack-type signature protocol ipv6]

**Release Information**

Statement introduced in Release 9.3 of Junos OS.

**Description**

Specify the IP address of the attack target.

**Options**
- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***ip-address-or-hostname***—Match an ip-address or a host name.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## destination-address (Security Destination NAT)

**Syntax** destination-address <*ip-address*>;

**Hierarchy Level** [edit security nat destination rule-set *rule-set-name* rule *rule-name* match]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify a destination address to match the rule. You can configure one address or a subnet.



NOTE:

- If the destination address is IPv4 and the pool is an IPv6 prefix, the length of the IPv6 prefix must be 96.
- If the destination address is an IPv6 prefix and the pool is an IPv6 prefix, their length must be the same.

**Options** ***ip-address***— Destination address or a subnet.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## destination-address (Security IDP Policy)

**Syntax** destination-address ([*address-name*] | any | any-ipv4 | any-ipv6);

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* match]
[edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Release 10.0 of Junos OS.

**Description** Specify a destination IP address or IP address set object to be used as the match destination address object. The default value is any.

**Options**

- ***address-name***—IP address or IP address set object.
- ***any***—Specify any IPv4 or IPv6 address.
- ***any-ipv4***—Specify any IPv4 address.
- ***any-ipv6***—Specify any IPv6 address.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- Application-Level Distributed Denial of Service
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## destination-address (Security Policies)

**Syntax**

```
destination-address {
    [address];
    any;
    any-ipv4;
    any-ipv6;
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]

**Release Information** Statement modified in Junos OS Release 8.5. Support for IPv6 addresses added in Junos OS Release 10.2. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Junos OS Release 10.4. Support for wildcard addresses added in Junos OS Release 11.1.

**Description** Define the matching criteria. You can specify one or more IP addresses, address sets, or wildcard addresses. You can specify wildcards **any**, **any-ipv4**, or **any-ipv6**.

**Options**

***address***—IP address (**any**, **any-ipv4**, **any-ipv6**), IP address set, or address book entry, or wildcard address (represented as A.B.C.D/wildcard-mask). You can configure multiple addresses or address prefixes separated by spaces and enclosed in square brackets.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## destination-address (Security Policies Flag)

**Syntax**

```
destination-address {
  drop-translated;
  drop-untranslated;
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit]

**Release Information** Statement introduced in Junos OS Release 9.2.

**Description** Specify whether the traffic permitted by the security policy is limited to packets where the destination IP address has been translated by means of a destination NAT rule or to packets where the destination IP address has not been translated.

On Juniper Networks security devices, destination NAT rules are processed before security policy lookup. Therefore, it is possible for a security policy to permit traffic from a source **S** to a destination **D** (where no destination NAT is performed) and also to permit traffic from the source **S** to the destination **d** (where **d** has been translated to **D**).

**Options**

- **drop-translated**—Drop packets with translated destination IP addresses. Traffic permitted by the security policy is limited to packets where the destination IP address has not been translated.
- **drop-untranslated**—Drop packets without translated destination IP addresses. Traffic permitted by the security policy is limited to packets where the destination IP address has been translated by means of a destination NAT rule.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## destination-address (Security Source NAT)

**Syntax** destination-address <*ip-address*>;

**Hierarchy Level** [edit security nat source rule-set *rule-set-name* rule *rule-name* match]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify a destination address to match the rule. You can configure multiple addresses or subnets.

**Options** ***ip-address***—Destination address or a subnet.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

## destination-address (Security Static NAT)

**Syntax** destination-address [destination-address];

**Hierarchy Level** [edit security nat static rule-set *rule-set-name* rule *rule-name* match]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify a destination address to match the rule. You can configure one address or a subnet.

**Options** ***destination-address***—Destination address or a subnet.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## destination-address-name (Security Destination NAT)

**Syntax** destination-address-name <*address-name*>;

**Hierarchy Level** [edit security nat destination rule-set *rule-set-name* rule *rule-name* match]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify a destination address name to match the rule. You can configure multiple address names.

**Options** ***address-name***—Destination address name.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

## destination-address-name (Security Source NAT)

**Syntax** destination-address-name <*address-name*>;

**Hierarchy Level** [edit security nat source rule-set *rule-set-name* rule *rule-name* match]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify a destination address name to match the rule. You can configure multiple address names.

**Options** ***address-name***—Destination address name.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## destination-address-name (Security Static NAT)

**Syntax** destination-address-name [address-name];

**Hierarchy Level** [edit security nat static rule-set *rule-set-name* rule *rule-name* match]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify a destination address name to match the rule.

**Options** ***destination-address***—Destination address name.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

## destination-except

**Syntax** destination-except [*address-name*];

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* match]
[edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Release 10.0 of Junos OS.

**Description** Specify a destination IP address or IP address set object to specify all destination address objects except the specified address objects. The default value is any.

**Options** ***address-name***—IP address or IP address set object.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- Application-Level Distributed Denial of Service
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## destination-ip (Security Alarms)

**Syntax**

```
destination-ip {
    duration interval;
    size count;
    threshold value;
}
```

**Hierarchy Level** [edit security alarms potential-violation policy]

**Release Information** Statement introduced in Junos OS Release 11.2.

**Description** Configure alarms for a number of policy violations to a destination network identifier within a specified time period.

**Options**

- **duration *interval***—Indicate the duration of counters.

  **Range:** 1 through 3600 seconds.
  **Default:** 1 second.

- **size *count***—Indicate the number of destination IP addresses for which policy violation checks can be done concurrently.

  **Range:** 1 through 10240.
  **Default:** 1024.

- **threshold *value***—Indicate the maximum number of destination IP address matches required to raise an alarm.

  **Range:** 1 through 4294967295.
  **Default:** 1000.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## destination-ip (Security IPsec)

**Syntax** destination-ip *ip-address*;

**Hierarchy Level** [edit security ipsec vpn *vpn-name* vpn-monitor]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the destination of the Internet Control Message Protocol (ICMP) pings. If this statement is used, the device uses the peer's gateway address by default. (This statement is not supported on dynamic VPN implementations.)

**Options** *ip-address*—Destination IP address.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

## destination-ip-based

**Syntax** destination-ip-based *number*;

**Hierarchy Level** [edit security screen ids-option *screen-name* limit-session]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Limit the number of concurrent sessions the device can direct to a single destination IP address.

**Options** *number* —Maximum number of concurrent sessions that can be directed to a destination IP address.

**Range:** 1 through 1000000

**Default:** 128



NOTE: For SRX Series devices, the applicable range is 1 through 8000000.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Configuration Statement Hierarchy


Copyright © 2013, Juniper Networks, Inc.

## destination-nat

**Syntax** destination-nat (off | pool *pool-name*);

**Hierarchy Level** [edit security nat destination rule-set *rule-set-name* rule *rule-name* then]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify the action of the destination NAT rule.

**Options**
- **off**—Do not perform destination NAT operation.
- **pool** ***pool-name*** —Use user-defined destination NAT pool to perform destination NAT.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

## destination-port (Security Destination NAT)

**Syntax** destination-port *port-number*;

**Hierarchy Level** [edit security nat destination rule-set *rule-set-name* rule *rule-name* match]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify a destination port to match the rule. You can configure one port.

**Options** ***port-number*** —Destination port number.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## destination-port (Security Signature Attack)

**Syntax**

```
destination-port {
  match (equal | greater-than | less-than | not-equal);
  value destination-port;
}
```

**Hierarchy Level**

[edit security idp custom-attack *attack-name* attack-type signature protocol udp]
[edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

**Release Information**

Statement introduced in Release 9.3 of Junos OS.

**Description**

Specify the port number of the attack target.

**Options**

- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***destination-port***—Match the port number of the attack target.

  **Range:** 0 through 65,535

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## destination-port (Security Source NAT)

**Syntax**

```
destination-port port-number;
```

**Hierarchy Level**

[edit security nat source rule-set *rule-set-name* rule *rule-name* match]

**Release Information**

Statement modified in Junos OS Release 9.6.

**Description**

Specify a source port to match the rule. You can configure one port.

**Options**

***port-number*** —Source port number.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## destination-port (Security Static NAT)

**Syntax** destination-port *lower-port-range* to *upper-port-range*;

**Hierarchy Level** [edit security nat static rule-set *rule-set-name* rule *rule-name* match]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify a destination port or port range to allow static NAT to map ports.

**Options**
- **lower-port-range**—Specify the lower limit of the port range.
- **upper-port-range**—Specify the upper limit of the port range.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## destination-threshold

**Syntax** destination-threshold *number* ;

**Hierarchy Level** [edit security screen ids-option *screen-name* tcp syn-flood]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Specify the number of SYN segments received per second for a single destination IP address before the device begins dropping connection requests to that destination. If a protected host runs multiple services, you might want to set a threshold based only on the destination IP address, regardless of the destination port number.

**Options** *number* —Number of SYN segments received per second before the device begins dropping connection requests.

**Range:** 4 through 500,000 per second

**Default:** 2048 per second



NOTE: For SRX Series devices, the applicable range is 4 through 1,000,000 per second.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Configuration Statement Hierarchy
- attack-threshold on page 423

Copyright © 2013, Juniper Networks, Inc.

## detect-shellcode

**Syntax** (detect-shellcode | no-detect-shellcode);

**Hierarchy Level** [edit security idp sensor-configuration ips]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Enable to detect the shell code and prevent buffer overflow attacks. By default this setting is enabled.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## detector

**Syntax**
```
detector {
  protocol-name protocol-name {
    tunable-name  tunable-name {
      tunable-value protocol-value;
    }
  }
}
```

**Hierarchy Level** [edit security idp sensor-configuration]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Configure protocol detector engine for a specific service.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## df-bit

**Syntax** df-bit (clear | copy | set);

**Hierarchy Level** [edit security ipsec vpn *vpn-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify how the device handles the Don't Fragment (DF) bit in the outer header.

**Options**
- **clear**—Clear (disable) the DF bit from the outer header. This is the default.
- **copy**—Copy the DF bit to the outer header.
- **set**—Set (enable) the DF bit in the outer header.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## dh-group (Security)

**Syntax** dh-group (group1 | group14 | group2 | group5);

**Hierarchy Level** [edit security group-vpn member ike proposal *proposal-name*]
[edit security group-vpn server ike proposal *proposal-name*]
[edit security ike proposal *proposal-name*]

**Release Information** Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS. Support for dh-group group 14 is added in Release 11.1 of Junos OS.

**Description** Specify the IKE Diffie-Hellman group.



NOTE: The device does not delete existing IPsec SAs when you update the **dh-group** configuration in the IKE proposal.

**Options** **dh-group**—Type of Diffie-Hellman prime modulus group for performing a Diffie-Hellman authentication key exchange.

- **group1**—768-bit algorithm.
- **group14**—2048-bit algorithm. (This option is not supported on dynamic VPN implementations.)
- **group2**—1024-bit algorithm.
- **group5**—1536-bit algorithm.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## direction (Security Custom Attack)

**Syntax** direction (any | client-to-server | server-to-client);

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type anomaly]
[edit security idp custom-attack *attack-name* attack-type signature]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Define the connection direction of the attack.

**Options**
- **any**—Detect the attack in either direction.
- **client-to-server**—Detect the attack only in client-to-server traffic.
- **server-to-client**—Detect the attack only in server-to-client traffic.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## direction (Security Dynamic Attack Group)

**Syntax**

```
direction {
  expression (and | or);
  values [any client-to-server exclude-any exclude-client-to-server exclude-server-to-client
    server-to-client];
}
```

**Hierarchy Level** [edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

**Release Information** Statement introduced in Release 9.3 of Junos OS. The **expression** option added in Release 11.4 of Junos OS.

**Description** Specify a direction filter to add predefined attacks to the dynamic group based on the direction specified in the attacks.

**Options** **expression**—Boolean operators:

- **and**— If both the member name patterns match, the expression matches.
- **or**— If either of the member name patterns match, the expression matches.

**values**—Name of the direction filter. You can select from the following directions:

- **any**—Monitors traffic from client to server and server to client.
- **client-to-server**—Monitors traffic from client to server (most attacks occur over **client-to-server** connections) only.
- **exclude-any**—Allows traffic from client to server and server to client.
- **exclude-client-to-server**—Allows traffic from client to server only.
- **exclude-server-to-client**—Allows traffic from server to client only.
- **server-to-client**—Monitors traffic from server to client only.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## disable (Application Tracking)

**Syntax** disable;

**Hierarchy Level** [edit security application-tracking]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Disable application tracking on a device without deleting the zone configuration. Application tracking is enabled by default.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Tracking

## disable (PKI)

**Syntax** disable;

**Hierarchy Level** [edit security pki ca-profile *profile-name* revocation-check]

**Release Information** Statement modified in Release 9.0 of Junos OS.

**Description** Disable revocation checks.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Certificates and Public Key Cryptography for Security Devices

## disable-call-id-hiding

**Syntax** disable-call-id-hiding;

**Hierarchy Level** [edit security alg sip]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Disable translation of the host IP address in call-ID header. Translation is enabled by default.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- SIP ALGs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## display-host (Security Fallback Block)

**Syntax** display-host;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options fallback-block]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** Display the computer host name in the notification e-mail sent to the administrator when a fallback-block notification occurs.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

## display-host (Security Virus Detection)

**Syntax** display-host;

**Hierarchy Level** [edit security utm feature-profile anti-virus profile *profile name* notification-options virus-detection]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Display the computer host name in the notification e-mail sent to the administrator when a virus is detected by Sophos antivirus.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## distinguished-name (Security)

**Syntax** distinguished-name <container *container-string*> <wildcard *wildcard-string*>

**Hierarchy Level** [edit security group-vpn server ike gateway *gateway-name*]
[edit security ike gateway *gateway-name* dynamic]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn server** hierarchy added in Release 10.2 of Junos OS.

**Description** Specify a distinguished name as the identifier for the remote gateway with a dynamic IP address. (This statement is not supported on dynamic VPN implementations.)

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## dns

**Syntax**

```
dns {
  disable;
  doctoring (none | sanity-check);
  maximum-message-length number;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the Domain Name Service (DNS) Application Layer Gateway (ALG) on the device.

**Options**

- **disable**—Disable the DNS ALG. By default, the DNS ALG is enabled. This option will enable or disable DNS ALG for both IPV4 and IPV6 mode.
- **doctoring**—Configure DNS ALG doctoring.
  - **none**— Disable all DNS ALG Doctoring.
  - **sanity-check**—Perform only DNS ALG sanity checks.
- **maximum-message-length**—A limit imposed on the size of individual DNS messages (see related section).
- **traceoptions**—Configure SQL ALG tracing options.
  - **flag**—Trace operation to perform.
    - **all**—Trace all events.
    - ***extensive***—Display extensive amount of data.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Layer Gateways for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## download-profile (Security Antivirus FTP)

**Syntax** download-profile *profile-name*;

**Hierarchy Level** [edit security utm utm-policy *policy-name* anti-virus ftp]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the antivirus FTP (download) protocol and attach this policy to a security profile to implement it.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## download-profile (Security Content Filtering FTP)

**Syntax** download-profile *profile-name*;

**Hierarchy Level** [edit security utm utm-policy *policy-name* content-filtering ftp]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the content-filtering FTP (download) protocol and attach this policy to a security profile to implement it.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## drop (Security GTP)

**Syntax**

```
drop {
    aa-create-pdp (0 | 1 | 2 | all);
    aa-delete-pdp (0 | 1 | 2 | all);
    bearer-resource (0 | 1 | 2 | all);
    change-notification (0 | 1 | 2 | all);
    config-transfer (0 | 1 | 2 | all);
    context (0 | 1 | 2 | all);
    create-bearer (0 | 1 | 2 | all);
    create-data-forwarding (0 | 1 | 2 | all);
    create pdp (0 | 1 | 2 | all);
    create-session (0 | 1 | 2 | all);
    create-tnl-forwarding (0 | 1 | 2 | all);
    cs-paging (0 | 1 | 2 | all);
    data-record (0 | 1 | 2 | all);
    delete-bearer (0 | 1 | 2 | all);
    delete-command (0 | 1 | 2 | all);
    delete-data-forwarding (0 | 1 | 2 | all);
    delete-pdn (0 | 1 | 2 | all);
    delete-pdp (0 | 1 | 2 | all);
    delete-session (0 | 1 | 2 | all);
    detach (0 | 1 | 2 | all);
    downlink-notification (0 | 1 | 2 | all);
    echo (0 | 1 | 2 | all);
    error-indication (0 | 1 | 2 | all);
    failure-report (0 | 1 | 2 | all);
    fwd-access (0 | 1 | 2 | all);
    fwd-relocation (0 | 1 | 2 | all);
    fwd-srns-context (0 | 1 | 2 | all);
    g-pdu (0 | 1 | 2 | all);
    identification (0 | 1 | 2 | all);
    mbms-sess-start (0 | 1 | 2 | all);
    mbms-sess-stop (0 | 1 | 2 | all);
    mbms-sess-update (0 | 1 | 2 | all);
    modify-bearer (0 | 1 | 2 | all);
    modify-command (0 | 1 | 2 | all);
    node-alive (0 | 1 | 2 | all);
    note-ms-present (0 | 1 | 2 | all);
    pdu-notification (0 | 1 | 2 | all);
    ran-info (0 | 1 | 2 | all);
    redirection (0 | 1 | 2 | all);
    release-access (0 | 1 | 2 | all);
    relocation-cancel (0 | 1 | 2 | all);
    resume (0 | 1 | 2 | all);
    send-route (0 | 1 | 2 | all);
    sgsn-context (0 | 1 | 2 | all);
    stop-paging (0 | 1 | 2 | all);
    supported-extension (0 | 1 | 2 | all);
    suspend (0 | 1 | 2 | all);
    trace-session (0 | 1 | 2 | all);
    update-bearer (0 | 1 | 2 | all);
    update-pdn (0 | 1 | 2 | all);
    update-pdp (0 | 1 | 2 | all);
```


Copyright © 2013, Juniper Networks, Inc.

```
    ver-not-supported (0 | 1 | 2 | all);
}
```

**Hierarchy Level** [edit security gprs gtp profile *profile-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS. New GTP message types added in Release 11.4 of Junos OS. Support for GTPv2 added in Release 11.4 of Junos OS.

**Description** Drop GTP message types. Specify **All** to drop messages for all GTP versions. Specify **0**, **1**, or **2** to drop messages for GTP versions 0, 1, or 2, respectively.

Copyright © 2013, Juniper Networks, Inc.

**Options** The following lists CLI keywords that each represent a GTP message type.

You must specify *(0 | 1 | 2 | all)* to specify the GTP release version number for the specified message type. The possible versions are 0, 1, 2, or all.



NOTE: A GTP message type includes one or many messages. When you drop a message type, you automatically drop all messages of the specified type.

- **aa-create-pdp** —Represents Create AA PDP Context Request and Create AA PDP Context Response messages.
- **aa-delete-pdp** —Represents Delete AA PDP Context Request and Delete AA PDP Context Response messages.
- **bearer-resource**—Represents Bearer Resource Command and Bearer Resource Failure messages.
- **change-notification**—Represents Change Notification Request and Change Notification Response messages.
- **context**—Represents Context Request and Context Response messages.
- **config-transfer**—Represents Configuration Transfer Tunnel messages.
- **create-bearer**—Represents Create Bearer Request and Create Bearer Response messages.
- **create-data-forwarding**—Represents Create Indirect Data Forwarding Request and Create Indirect Data Forwarding Response messages.
- **create-tnl-forwarding**—Represents Create Forwarding Tunnel Request and Create Forwarding Tunnel Response messages.
- **create-pdp**—Represents Create PDP Context Request and Create PDP Context Response messages.
- **create-session**—Represents Create Session Request and Create Session Response messages.
- **cs-paging**—Represents CS Paging Indication messages.
- **data-record**—Represents Data Record Request and Data Record Response messages.
- **delete-bearer**—Represents Delete Bearer Request and Delete Bearer Response messages.
- **delete-command**—Represents Delete Bearer Command and Delete Bearer Failure messages.
- **delete-data-forwarding**—Represents Delete Indirect Data Forwarding Request and Delete Indirect Data Forwarding Response messages.
- **delete-pdn**—Represents Delete PDN Connection Set Request and Delete PDN Connection Set Response messages.


Copyright © 2013, Juniper Networks, Inc.

- **delete-pdp**—Represents Delete PDP Context Request and Delete PDP Context Response messages.
- **delete-session**—Represents Delete Session Request and Delete Session Response messages.
- **detach**—Represents Detach Notification and Detach Acknowledgement messages.
- **downlink-notification**—Represents Downlink Data Notification, Downlink Data Acknowledgement, and Downlink Data Notification Failure Indication messages.
- **echo**—Represents Echo Request and Echo Response messages.
- **error-indication**—Represents Error Indication messages.
- **failure-report**—Represents Failure Report Request and Failure Report Response messages.
- **fwd-access**—Represents Forward Access Context Notification and Forward Access Context Acknowledgment messages.
- **fwd-relocation**—Represents Forward Relocation Request, Forward Relocation Response, Forward Relocation Complete, and Forward Relocation Complete Acknowledge messages.
- **fwd-srns-context**—Represents Forward SRNS Context Request and Forward SRNS Context Response messages.
- **g-pdu**—Represents G-PDU and T-PDU messages.
- **identification**—Represents Identification Request and Identification Response messages.
- **mbms-sess-start**—Represents MBMS Session Start Request and MBMS Session Start Response messages.
- **mbms-sess-stop**—Represents MBMS Session Stop Request and MBMS Session Stop Response messages.
- **mbms-sess-update**—Represents MBMS Session Update Request and MBMS Session Update Response messages.
- **modify-bearer**—Represents Modify Bearer Request and Modify Bearer Response messages.
- **modify-command**—Represents Modify Bearer Command and Modify Bearer Failure messages.
- **node-alive**—Represents Node Alive Request and Node Alive Response messages.
- **note-ms-present**—Represents Note MS GPRS Present Request and Note MS GPRS Present Response messages.
- **pdu-notification**—Represents PDU Notification request and PDU Notification response messages.
- **ran-info**—Represents Ran Info Relay messages.
- **redirection**—Represents Redirection Request and Redirection Response messages.

Copyright © 2013, Juniper Networks, Inc.

- **relocation-cancel**—Represents Relocations Cancel Request and Relocation Cancel Response messages.
- **resume**—Represents Resume Notification and Resume Acknowledgement messages.
- **send-route**—Represents Send Route Info Request and Send Route Info Response messages.
- **sgsn-context**—Represents SGSN Context Request and SGSN Context Response messages.
- **stop-paging**—Represents Stop Paging Indication messages.
- **supported-extension**—Represents Supported Extension Headers Notification messages.
- **suspend**—Represents Suspend Notification and Suspend Acknowledgement messages.
- **trace-session**—Represents Trace Session Activation and Trace Session Deactivation messages.
- **update-bearer**—Represents Update Bearer Request and Update Bearer Response messages.
- **update-pdn**—Represents Update PDN Set Connection Request and PDN Set Connection Response messages.
- **update-pdp**—Represents Update PDP Request and Update PDP Response messages.
- **ver-not-supported**—Represents Version Not Supported messages.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- General Packet Radio Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## drop (Security SCTP)

**Syntax**

```
drop {
  m3ua-service {
    isup;
    sccp;
    tup;
  }
  payload-protocol {
    all;
    asap;
    bicc;
    ddp-segment;
    ddp-stream;
    dua;
    enrp;
    h248;
    h323;
    iua;
    m2pa;
    m2ua;
    m3ua;
    qipc;
    reserved;
    simco;
    sua;
    tali;
    v5ua;
  }
}
```

**Hierarchy Level** [edit security gprs sctp profile *profile-name*]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Display information about the configuration of the current Stream Control Transmission Protocol (SCTP) inspection.

**Options**

- **m3ua-services**—M3UA data service indicator. The following values are supported:
  - **isup**—ISDN Upper Part.
  - **sccp**—Signaling Connection Control Part.
  - **tup**—Telephone User Part.
- **payload-protocol**—SCTP payload protocol identifier. The following values are supported.
  - **all**—All SCTP payload protocol identifiers (id:1~17).
  - **asap**—Aggregate Server Access Protocol.
  - **bicc**—Bearer Independent Call Control.

Copyright © 2013, Juniper Networks, Inc.

- **ddp-segement**—Direct Data Placement Segment chunk.
- **ddp-stream**—Direct Data Placement Stream session control.
- **dua**—DPNSS/DASS 2 extensions to IUA Protocol.
- **enrp**—Endpoint Handle escape Redundancy Protocol.
- **h248**—H.248 Protocol.
- **h323**—H.323 Protocol.
- **iua**—ISDN User Adaptation Layer.
- **m2pa**—MTP2 User Peer-to-Peer Adaption Layer.
- **m2ua**—MTP2 User Adaption Layer.
- **m3ua**—MTP3 User Adaption Layer.
- **qipc**—Q.IPC.
- **reserved**—Reserved by SCTP.
- **simco**—Simple Middlebox Configuration.
- **sua**—SCCP User Adaption Layer.
- **tali**—Transport Adapter Layer Interface.
- **v5ua**—v5.2 User Adaption Layer.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- General Packet Radio Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## dscp-rewrite

**Syntax**

```
dscp-rewrite {
  code-point 6 bit patterns;
}
```

**Hierarchy Level**

[edit security alg sip]
[edit security alg h323]
[edit security alg mgcp]
[edit security alg sccp]

**Release Information**

Statement introduced in Release 10.4 of Junos OS.

**Description**

Specify a rewrite-rule for the traffic that passes through a voice over IP Application Layer Gateway ( VoIP ALG).

**Options**

**6-bit patterns**—Value of the code point in binary form.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Layer Gateways for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## dynamic (Security)

**Syntax**

```
dynamic {
  connections-limit number;
  (distinguished-name <container container-string> <wildcard wildcard-string> | hostname
    domain-name | inet ip-address | inet6 ipv6-address | user-at-hostname e-mail-address);
  ike-user-type (group-ike-id | shared-ike-id);
}
```

**Hierarchy Level**

[edit security group-vpn server ike gateway *gateway-name*]
[edit security ike gateway *gateway-name*]

**Release Information**

Statement modified in Release 8.5 of Junos OS. Support for **group-vpn server** hierarchy added in Release 10.2 of Junos OS. The **inet6** option added in Release 11.1 of Junos OS. The **inet6** option is not supported on the **group-vpn** hierarchies.

**Description**

Specify the identifier for the remote gateway with a dynamic IPv4 or IPv6 address. Use this statement to set up a VPN with a gateway that has an unspecified IPv4 or IPv6 address.

**Options**

The remaining statements are explained separately.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

## dynamic-application

**Syntax**

dynamic-application [*system-application*];

**Hierarchy Level**

[edit security application-firewall rule-sets *rule-set-name* rule *rule-name* match]

**Release Information**

Statement introduced in Release 11.1 of Junos OS.

**Description**

Specify the dynamic application names for match criteria.

**Options**

***system-application***—Set of system applications for match criteria.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Firewall


Copyright © 2013, Juniper Networks, Inc.

## dynamic-application-group

**Syntax** dynamic-application-group [*system-application-group*];

**Hierarchy Level** [edit security application-firewall rule-sets *rule-set-name* rule *rule-name* match]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Specify the dynamic application group to match.

**Options** ***system-application-group***—Set of groups defining one or more system applications for match criteria.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Firewall

Copyright © 2013, Juniper Networks, Inc.

## dynamic-attack-group

**Syntax**

```
dynamic-attack-group dynamic-attack-group-name {
  filters {
    category {
      values [category-value];
    }
    direction {
      expression (and | or);
      values [any client-to-server exclude-any exclude-client-to-server
        exclude-server-to-client server-to-client];
    }
    false-positives {
      values [frequently occasionally rarely unknown];
    }
    performance {
      values [fast normal slow unknown];
    }
    products {
      values [product-value];
    }
    recommended;
    service {
      values [service-value];
    }
    severity {
      values [critical info major minor warning];
    }
    type {
      values [anomaly signature];
    }
  }
}
```

**Hierarchy Level** [edit security idp]

**Release Information** Statement introduced in Release 9.3 of Junos OS. The **expression** option added in Release 11.4 of Junos OS.

**Description** Configure a dynamic attack group. A dynamic attack group selects its members based on the filters specified in the group. Therefore, the list of attacks is updated (added or removed) when a new signature database is used.

**Options** ***dynamic-attack-group-name***—Name of the dynamic attack group.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## dynamic-attack-groups (Security IDP)

**Syntax** dynamic-attack-groups *attack-group-name*;

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match attacks]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match attacks]

**Release Information** Statement introduced in Junos OS Release 9.2.

**Description** Specify a name for the dynamic attack group.

**Options** *attack-group-name*—Name of the dynamic attack group.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## dynamic-vpn

**Syntax**

```
dynamic-vpn {
  access-profile profile-name;
  clients configuration-name {
    ipsec-vpn vpn-name;
    remote-exceptions ip-address/mask;
    remote-protected-resources ip-address/mask;
    user username;
    user-groups user-group-name;
  }
  force-upgrade;
  config-check;
  interface;
  traceoptions {
    file filename;
    flag flag;
  }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Junos OS Release Release 9.5.

**Description** Configure the dynamic VPN feature. The dynamic VPN feature simplifies remote access by enabling users to create IPsec VPN tunnels without having to manually configure settings on their PCs or laptops. Instead, authenticated users can simply download a preconfigured Web client to their computers with all the client-side information required to create and manage an IPsec VPN tunnel to the server.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Dynamic VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## early-ageout

**Syntax** early-ageout *seconds*;

**Hierarchy Level** [edit security flow aging]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Define the value before the device aggressively ages out a session from its session table.

**Options** ***seconds*** —Amount of time that elapses before the device aggressively ages out a session.
**Range:** 1 through 65,535 seconds
**Default:** 20 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Flow-Based Processing for Security Devices

## email-notify

**Syntax**
```
email-notify {
  admin-email email-address;
  custom-message message;
  custom-message-subject message-subject;
}
```

**Hierarchy Level** [edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update]
[edit security utm feature-profile anti-virus sophos-engine pattern-update]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** You can configure the device to notify a specified administrator when patterns are updated. This is an e-mail notification with a custom message and a custom subject line.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## enable (GPRS GTP)

**Syntax** enable;

**Hierarchy Level** [edit security gprs gtp]

**Release Information** Statement introduced in Junos OS Release 10.0.

**Description** Enable GPRS tunneling protocol functionality.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- General Packet Radio Service for Security Devices

## enable

**Syntax**
```
enable {
  download-timeout minutes;
  interval hours;
  start-time start-time;
}
```

**Hierarchy Level** [edit security idp security-package automatic]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Enables the automatic download of the IDP security package.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Signature Database for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## enable-all-qmodules

**Syntax** (enable-all-qmodules | no-enable-all-qmodules);

**Hierarchy Level** [edit security idp sensor-configuration global]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Enable all the qmodules of the global rulebase IDP security policy. By default all the qmodules are enabled.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## enable-packet-pool

**Syntax** (enable-packet-pool | no-enable-packet-pool);

**Hierarchy Level** [edit security idp sensor-configuration global]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Enable the packet pool to use when the current pool is exhausted. By default packet pool is enabled.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## encryption (Security)

**Syntax**

```
encryption {
  algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
  key (ascii-text key | hexadecimal key) ;
}
```

**Hierarchy Level** [edit security ipsec vpn *vpn-name* manual]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Configure an encryption algorithm and key for a manual Security Association (SA). (This statement is not supported on dynamic VPN implementations.)

**Options**

- **algorithm**—Type of encryption algorithm. It can be one of the following:
  - **des-cbc**—Has a block size of 8 bytes (64 bits); its key size is 48 bits long.
  - **3des-cbc**—Has block size of 8 bytes (64 bits); its key size is 192 bits long

    NOTE: For 3des-cbc, we recommend that the first 8 bytes be different from the second 8 bytes, and the second 8 bytes be the same as the third 8 bytes.
  - **aes-128-cbc**—Advanced Encryption Standard (AES) 128-bit encryption algorithm.
  - **aes-192-cbc**—Advanced Encryption Standard (AES) 192-bit encryption algorithm.
  - **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption algorithm.
- **key**—Type of encryption key. It can be one of the following:
  - **ascii-text key**—ASCII text key. For the **des-cbc** option, the key contains 8 ASCII characters; for **3des-cbc**, the key contains 24 ASCII characters.
  - **hexadecimal key**—Hexadecimal key. For the **des-cbc** option, the key contains 16 hexadecimal characters; for the **3des-cbc** option, the key contains 48 hexadecimal characters.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Group VPNs for Security Devices
- IPsec VPNs for Security Devices
- Troubleshooting for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## encryption-algorithm (Security)

**Syntax** encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);

**Hierarchy Level**
[edit security group-vpn member ike proposal *proposal-name*]
[edit security group-vpn server ike proposal *proposal-name*]
[edit security group-vpn server ipsec proposal *proposal-name*]
[edit security ike proposal *proposal-name*]
[edit security ipsec proposal *proposal-name*]

**Release Information** Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

**Description** Configure an encryption algorithm.



NOTE:

- The device does not delete existing IPSec SAs when you update the **encryption-algorithm** configuration in the IKE proposal.
- The device deletes existing IPSec SAs when you update the **encryption-algorithm** configuration in the IPsec proposal.

**Options**

- **3des-cbc**—Has a block size of 24 bytes; the key size is 192 bits long.
- **aes-128-cbc**—Advanced Encryption Standard (AES) 128-bit encryption algorithm.
- **aes-192-cbc**—Advanced Encryption Standard (AES) 192-bit encryption algorithm.
- **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption algorithm.
- **des-cbc**—Has a block size of 8 bytes; the key size is 48 bits long.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices
- Troubleshooting for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## encryption-failures

**Syntax**

```
encryption-failures {
  threshold value;
}
```

**Hierarchy Level** [edit security alarms potential-violation]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Raise a security alarm after exceeding a specified number of encryption failures.

**Default** Multiple encryption failures do not cause an alarm to be raised.

**Options** *failures*—Number of encryption failures up to which an alarm is not raised. When the configured number is exceeded, an alarm is raised.

**Range:** 1 through 1000000000.

**Default:** 1000

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

## endpoint-registration-timeout

**Syntax** endpoint-registration-timeout *value-in-seconds*;

**Hierarchy Level** [edit security alg h323]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the timeout value in seconds for entries in the NAT table.

**Options** *value-in-seconds*—Timeout value.

**Range:** 10 through 50000 seconds

**Default:** 3600 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Layer Gateways for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## engine-not-ready

**Syntax** engine-not-ready (block | log-and-permit);

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* fallback-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** The scan engine is initializing itself, for example, loading the signature database. During this phase, it is not ready to scan a file. A file could either pass or be blocked according to this setting. The default action is block.

**Options**
- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## engine-not-ready (Security Antivirus Sophos Engine)

**Syntax** default (block | log-and-permit | permit);

**Hierarchy Level** [edit security utm feature-profile anti-virus sophos-engine profile *profile-name* fallback-options]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** The scan engine is initializing itself, for example, loading the signature database. During this phase, it is not ready to scan a file. A file could either pass or be blocked according to this setting.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## enrollment (Security)

**Syntax**

```
enrollment {
  retry number;
  retry-interval seconds;
  url url-name;
}
```

**Hierarchy Level** [edit security pki ca-profile *ca-profile-name*]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Specify the enrollment parameters for a certificate authority (CA).

**Options**

- **retry** ***number*** —Number of automated attempts for online enrollment to be retried in case enrollment response is pending.

  **Range:** 0 through 1080
  **Default:** 10

- **retry-interval** ***seconds*** —Time interval, in seconds, between the enrollment retries.

  **Range:** 0 through 3600
  **Default:** 900 seconds

- **url** ***url-name*** —Enrollment URL where the Simple Certificate Enrollment Protocol (SCEP) request is sent to the certification authority (CA) as configured in this profile.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Certificates and Public Key Cryptography for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## establish-tunnels

**Syntax** establish-tunnels (immediately | on-traffic);

**Hierarchy Level** [edit security ipsec vpn *vpn-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify when IKE is activated: immediately after VPN information is configured and configuration changes are committed, or only when data traffic flows. In the second case, IKE needs to be negotiated with the peer gateway.

**Options**

- **immediately**—IKE is activated immediately after VPN configuration and configuration changes are committed.
- **on-traffic**—IKE is activated only when data traffic flows and must to be negotiated.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

## event-rate

**Syntax** Syntax event-rate *rate*

**Hierarchy Level** [edit security log]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Limits the rate (0 to 1500) at which logs will be streamed per second.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Device and Routing Operations Monitoring
- Security Logs
- Troubleshooting for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## exception (Security Antivirus Mime Whitelist)

**Syntax** exception *listname*;

**Hierarchy Level** [edit security utm feature-profile anti-virus mime-whitelist]
[edit security utm feature-profile anti-virus mime-whitelist list *listname*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure the antivirus scanner to use an exception list to the MIME bypass list (custom objects). To use the exception list, you first create a whitelist custom-object list with the **list** statement. The system will first look at any existing whitelist mime pattern. If it matches an item, it will then continue to look for any exceptions to the whitelist and will then scan any item in the exception list.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## exception (Security Content Filtering)

**Syntax** exception *list-name*;

**Hierarchy Level** [edit security utm feature-profile content-filtering profile *profile-name* block-mime]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure the content-filter to use an exception list to the MIME block list (custom objects).

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## exclude (Security Log)

**Syntax**

```
exclude exlude-name {
    destination-address destination-address;
    destination-port destination-port;
    event-id event-id;
    failure;
    interface-name interface-name;
    policy-name policy-name;
    process process-name;
    protocol protocol;
    source-address source-address;
    source-port source-port;
    success;
    user-name user-name;
}
```

**Hierarchy Level** [edit security log cache]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Configure a list of auditable events that can be excluded from the audit log.

**Options**

- **destination-ip** ***destination-address***—Destination IP address.
- **destination-port** ***destination-port***—Destination port number.
- **event-id** ***event-id***—Error message identification number.
- **failure**—Failed audit event logs.
- **interface-name** ***interface-name***—Name of the interface.
- **policy-name** ***policy-name***—Policy name filter.
- **process** ***process-name***—Process that generated the event.
- **protocol** ***protocol***—Protocol that generated the event.
- **source-ip** ***source-address***—Source IP address.
- **source-port** ***source-port***—Source port number.
- **success**—Successful audit event logs.
- **username** ***user-name***—User name filter.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- show security log on page 2082
- clear security log on page 1454
- Security Logs


Copyright © 2013, Juniper Networks, Inc.

## exclude-context-values

**Syntax** exclude-context-values [*value*];

**Hierarchy Level** [edit security idp application-ddos *application-name* context *context-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure a list of common context value patterns that should be excluded from application-level distributed denial-of-service (DDoS) detection. For example, if you have a webserver that receives a high number of HTTP requests on home/landing page, you can exclude it from application-level DDoS detection.

**Options** ***value***—List of patterns for exclusion. Example: **www.juniper.net www.acmegizmo.com**.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service

Copyright © 2013, Juniper Networks, Inc.

## expression

**Syntax** expression *boolean-expression*;

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type chain]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Configure Boolean expression. The Boolean expression defines the condition for the individual members of a chain attack that will decide if the chain attack is hit.

For standalone IDP devices, expression overrides order function.

For SRX Series devices, expression and order cannot be configured together. Only one of them can be specified.

**Options** ***boolean-expression***—Boolean operators:

- **or**—If either of the member name patterns match, the expression matches.
- **and**—If both of the member name patterns match, the expression matches. It does not matter which order the members appear in.
- **oand**—If both of the member name patterns match, and if they appear in the same order as in the Boolean Expression, the expression matches.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## external-interface (Security IKE Gateway)

**Syntax** external-interface *external-interface-name*;

**Hierarchy Level** [edit security ike gateway *gateway-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the outgoing interface for IKE SAs. This interface is associated with a zone that acts as its carrier, providing firewall security for it.

**Options** ***external-interface-name*** —Name of the interface to be used to send traffic to the IPsec VPN.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- IPsec VPNs for Security Devices

## external-interface (Security Manual SA)

**Syntax** external-interface ***external-interface-name***;

**Hierarchy Level** [edit security ipsec vpn *vpn-name* manual]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the outgoing interface for the manual SA. (This statement is not supported on dynamic VPN implementations.)

**Options** ***external-interface-name*** —Name of the outgoing interface.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## fallback-block (Security Antivirus)

**Syntax**

```
fallback-block {
  administrator-email email-address;
  allow-email;
  custom-message message;
  custom-message-subject message-subject;
  display-host;
  (notify-mail-sender | no-notify-mail-sender);
  type (message | protocol-only);
}
```

**Hierarchy Level**

[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options]

**Release Information**

Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description**

Configure notifications for fallback blocking actions. Fallback options tell the system how to handle the errors returned by either the scan engine or the scan manager.

**Options**

The remaining statements are explained separately.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## fallback-non-block (Security Antivirus)

**Syntax**

```
fallback-non-block {
  custom-message message;
  custom-message-subject message-subject;
  (notify-mail-recipient | no-notify-mail-recipient);
}
```

**Hierarchy Level**

[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options]

**Release Information**

Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description**

Configure notifications for fallback nonblocking actions.

**Options**

The remaining statements are explained separately.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## fallback-options (Security Antivirus Juniper Express Engine)

**Syntax**

```
fallback-options {
  content-size (block | log-and-permit);
  default (block | log-and-permit);
  engine-not-ready (block | log-and-permit);
  out-of-resources (block | (log-and-permit);
  timeout (block | log-and-permit);
  too-many-requests (block | log-and-permit);
}
```

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Fallback options tell the system how to handle the errors.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## fallback-options (Security Antivirus Kaspersky Lab Engine)

**Syntax**

```
fallback-options {
  content-size (block | log-and-permit);
  corrupt-file (block | log-and-permit);
  decompress-layer (block | log-and-permit);
  default (block | log-and-permit);
  engine-not-ready (block | log-and-permit);
  out-of-resources (block | (log-and-permit);
  password-file (block | (log-and-permit);
  timeout (block | log-and-permit);
  too-many-requests (block | log-and-permit);
}
```

**Hierarchy Level** [edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Fallback options tell the system how to handle the errors returned by either the scan engine or the scan manager.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## fallback-options (Security Antivirus Sophos Engine)

**Syntax**

```
fallback-options {
  content-size (block | log-and-permit | permit);
  default (block | log-and-permit | permit);
  engine-not-ready (block | log-and-permit | permit);
  out-of-resources (block | log-and-permit | permit);
  timeout (block | log-and-permit | permit);
  too-many-requests (block | log-and-permit | permit);
}
```

**Hierarchy Level** [edit security utm feature-profile anti-virus sophos-engine profile *profile-name*]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Configure fallback options to instruct the system how to handle errors.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices

## fallback-settings (Security Web Filtering)

**Syntax**

```
fallback-settings {
  default (block | log-and-permit);
  server-connectivity (block | log-and-permit);
  timeout (block | log-and-permit);
  too-many-requests (block | log-and-permit);
}
```

**Hierarchy Level** [edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name*]
[edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.
Statement introduced in Release 11.4 of Junos OS for Enhanced Web Filtering.

**Description** Fallback settings tell the system how to handle errors.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## fallback-settings (Security Web Filtering Juniper Local)

**Syntax**

```
fallback-settings {
  default (block | log-and-permit);
  server-connectivity (block | log-and-permit);
  timeout (block | log-and-permit);
  too-many-requests (block | log-and-permit);
}
```

**Hierarchy Level** [edit security utm feature-profile web-filtering juniper–local profile *profile-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Fallback settings tell the system how to handle errors.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices

## fallback-settings (Security Web Filtering Websense Redirect)

**Syntax**

```
fallback-settings {
  default (block | log-and-permit);
  server-connectivity (block | log-and-permit);
  timeout (block | log-and-permit);
  too-many-requests (block | log-and-permit);
}
```

**Hierarchy Level** [edit security utm feature-profile web-filtering websense-redirect profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Fallback settings tell the system how to handle errors.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## false-positives

**Syntax**

```
false-positives {
  values [frequently occasionally rarely unknown];
}
```

**Hierarchy Level** [edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify a false-positives filter to add attack objects based on the frequency that the attack produces a false positive on your network.

**Options** **values**—Name of the false positives filter. You can select from the following false positives frequency:

- **frequently**—Frequently track false positives occurrence.
- **occasionally**—Occasionally track false positives occurrence.
- **rarely**—Rarely track false positives occurrence.
- **unknown**—By default, all compound attack objects are set to Unknown. As you fine-tune IDP to your network traffic, you can change this setting to help you track false positives.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## family (Security Forwarding Options)

**Syntax**

```
family {
  inet6 {
    mode (drop | flow-based | packet-based);
  }
  iso {
    mode packet-based;
  }
  mpls {
    mode packet-based;
  }
}
```

**Hierarchy Level** [edit security forwarding-options]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Determine the protocol family to be used for packet forwarding.



NOTE: Packet-based processing is not supported on the following SRX Series devices: SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- MPLS for Security Devices
- Device Configuration

Copyright © 2013, Juniper Networks, Inc.

## feature-profile

**Syntax**

```
feature-profile {
  anti-spam {
    address-blacklist list-name;
    address-whitelist list-name;
    sbl {
      profile profile-name {
        custom-tag-string [string];
        (sbl-default-server | no-sbl-default-server);
        spam-action (block | tag-header | tag-subject);
      }
    }
    traceoptions flag flag;
  }
  anti-virus {
    juniper-express-engine {
      pattern-update {
        email-notify {
          admin-email email-address;
          custom-message message;
          custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
          password password-string;
          port port-number;
          server address-or-url;
          username name;
        }
        url url;
      }
      profile profile-name {
        fallback-options {
          content-size (block | log-and-permit);
          default (block | log-and-permit);
          engine-not-ready (block | log-and-permit);
          out-of-resources (block | (log-and-permit);
          timeout (block | log-and-permit);
          too-many-requests (block | log-and-permit);
        }
        notification-options {
          fallback-block {
            administrator-email email-address;
            allow-email;
            custom-message message;
            custom-message-subject message-subject;
            display-host;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
          }
          fallback-non-block {
            custom-message message;
```


Copyright © 2013, Juniper Networks, Inc.

```
            custom-message-subject message-subject;
            (notify-mail-recipient | no-notify-mail-recipient);
          }
          virus-detection {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
          }
        }
        scan-options {
          content-size-limit value;
          (intelligent-prescreening | no-intelligent-prescreening);
          timeout value;
        }
        trickling {
          timeout value;
        }
      }
    }
    kaspersky-lab-engine {
      pattern-update {
        email-notify {
          admin-email email-address;
          custom-message message;
          custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
          password password-string;
          port port-number;
          server address-or-url;
          username name;
        }
        url url;
      }
      profile profile-name {
        fallback-options {
          content-size (block | log-and-permit);
          corrupt-file (block | log-and-permit);
          decompress-layer (block | log-and-permit);
          default (block | log-and-permit);
          engine-not-ready (block | log-and-permit);
          out-of-resources (block | (log-and-permit);
          password-file (block | (log-and-permit);
          timeout (block | log-and-permit);
          too-many-requests (block | log-and-permit);
        }
        notification-options {
          fallback-block {
            administrator-email email-address;
            allow-email;
            custom-message message;
            custom-message-subject message-subject;
            display-host;
```

```
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
          }
          fallback-non-block {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-recipient | no-notify-mail-recipient);
          }
          virus-detection {
            custom-message message;
            custom-message-subject message-subject;
            (notify-mail-sender | no-notify-mail-sender);
            type (message | protocol-only);
          }
        }
        scan-options {
          content-size-limit value;
          decompress-layer-limit value;
          (intelligent-prescreening | no-intelligent-prescreening);
          scan-extension filename;
          scan-mode (all | by-extension);
          timeout value;
        }
        trickling {
          timeout value;
        }
      }
    }
    mime-whitelist {
      exception listname;
      list listname {
        exception listname;
      }
    }
    sophos-engine {
      pattern-update {
        email-notify {
          admin-email email-address;
          custom-message message;
          custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
          password password-string;
          port port-number;
          server address-or-url;
          username name;
        }
        url url;
      }
      profile <name> {
        fallback-options {
          content-size (block | log-and-permit | permit);
          default (block | log-and-permit | permit);
          engine-not-ready (block | log-and-permit | permit);
```


Copyright © 2013, Juniper Networks, Inc.

```
            out-of-resources (block | log-and-permit | permit);
            timeout (block | log-and-permit | permit);
            too-many-requests (block | log-and-permit | permit);
          }
          notification-options {
            fallback-block {
              administrator-email email-address;
              allow-email;
              custom-message message;
              custom-message-subject message-subject;
              display-host;
              (notify-mail-sender | no-notify-mail-sender);
              type (message | protocol-only);
            }
            fallback-non-block {
              custom-message message;
              custom-message-subject message-subject;
              (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
              custom-message message;
              custom-message-subject message-subject;
              (notify-mail-sender | no-notify-mail-sender);
              type (message | protocol-only);
            }
          }
          scan-options {
            content-size-limit value;
            (no-uri-check | uri-check);
            timeout value;
          }
          trickling {
            timeout value;
          }
        }
        sxl-retry value;
        sxl-timeout seconds;
      }
      traceoptions flag flag;
      type (juniper-express-engine | kaspersky-lab-engine | sophos-engine);
      url-whitelist listname;
    }
    content-filtering {
      profile profile-name {
        block-command protocol-command-list;
        block-content-type (activex | exe | http-cookie | java-applet | zip);
        block-extension extension-list;
        block-mime {
          exception list-name;
          list list-name;
        }
        notification-options {
          custom-message message;
          (notify-mail-sender | no-notify-mail-sender);
          type (message | protocol-only);
        }
```

```
        permit-command protocol-command-list;
    }
    traceoptions flag flag;
}
web-filtering {
    juniper-enhanced {
        cache {
            size value;
            timeout value;
        }
        profile profile-name {
            category customurl-list name {
                action (block | log-and-permit | permit | quarantine);
            }
            custom-block-message value;
            custom-quarantine-message value;
            default (block | log-and-permit | permit | quarantine);
            fallback-settings {
                default (block | log-and-permit);
                server-connectivity (block | log-and-permit);
                timeout (block | log-and-permit);
                too-many-requests (block | log-and-permit);
            }
            no-safe-search;
            site-reputation-action {
                fairly-safe (block | log-and-permit | permit | quarantine);
                harmful (block | log-and-permit | permit | quarantine);
                moderately-safe (block | log-and-permit | permit | quarantine);
                suspicious (block | log-and-permit | permit | quarantine);
                very-safe (block | log-and-permit | permit | quarantine);
            }
            timeout value;
        }
        server {
            host host-name;
            port number;
        }
    }
    juniper-local {
        profile profile-name {
            custom-block-message value;
            default (block | log-and-permit | permit);
            fallback-settings {
                default (block | log-and-permit);
                server-connectivity (block | log-and-permit);
                timeout (block | log-and-permit);
                too-many-requests (block | log-and-permit);
            }
            timeout value;
        }
    }
    surf-control-integrated {
        cache {
            size value;
            timeout value;
        }
```


Copyright © 2013, Juniper Networks, Inc.

```
        profile profile-name {
          category customurl-list name {
            action (block | log-and-permit | permit);
          }
          custom-block-message value;
          default (block | log-and-permit | permit);
          fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
          }
          timeout value;
        }
        server {
          host host-name;
          port number;
        }
      }
      traceoptions flag flag;
      type (juniper-enhanced | juniper-local | surf-control-integrated | websense-redirect);
      url-blacklist listname;
      url-whitelist listname;
      websense-redirect {
        profile profile-name {
          account value;
          custom-block-message value;
          fallback-settings {
            default (block | log-and-permit);
            server-connectivity (block | log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
          }
          server {
            host host-name;
            port number;
          }
          sockets value;
          timeout value;
        }
      }
    }
  }
}
```

**Hierarchy Level** [edit security utm]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure UTM features, antivirus, antispam, content-filtering, and web-filtering by creating feature profiles.

**Options** The remaining statements are explained separately.

Copyright © 2013, Juniper Networks, Inc.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- Unified Threat Management
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

## fifo-max-size (Security IDP)

**Syntax** fifo-max-size *value*;

**Hierarchy Level** [edit security idp sensor-configuration flow]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Sets the maximum FIFO size (range: 1 through 65535).

**Options** The remaining statements are explained separately.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices

## fifo-max-size (IPS)

**Syntax** fifo-max-size *value*;

**Hierarchy Level** [edit security idp sensor-configuration ips]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Sets the maximum IPS FIFO size (range: 1 through 65535).

**Options** The remaining statements are explained separately.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## file (Security Log)

**Syntax**

```
file {
  files max-file-number;
  name file-name;
  path binary-log-file-path;
  size maximum-file-size;
}
```

**Hierarchy Level** [edit security log]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Configure security log file options for logs in binary format.

**Options**

- **files** ***number***—Specify the maximum number of binary log files.

  **Range:** 2 through 10 files.

- **name** ***name*** —Name of the file to log messages.
- **path** ***filepath***—Specify the path of the binary log file.
- **size** ***maximum-file-size***—Maximum size of each trace file, in megabytes (MB).

  **Range:** 1 KB through 10 MB

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- System Log Messages
- Security Logs

Copyright © 2013, Juniper Networks, Inc.

## filename-extension

**Syntax**

```
filename-extension object-name {
  value [value];
}
```

**Hierarchy Level** [edit security utm custom-objects]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** When scanning content, you can use a file extension list to define a set of file extensions that are used in file extension scan mode (scan-by-extension).

**Options**

- ***object-name***—Name of the extension-list object.
- **value *value***—Value of the extension-list object. You can configure multiple values separated by spaces and enclosed in square brackets.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Understanding UTM Custom Objects
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## filters

**Syntax**

```
filters {
  category {
    values [category-value];
  }
  direction {
    expression (and | or);
    values [any client-to-server exclude-any exclude-client-to-server exclude-server-to-client
      server-to-client];
  }
  false-positives {
    values [frequently occasionally rarely unknown];
  }
  performance {
    values [fast normal slow unknown];
  }
  products {
    values [product-value];
  }
  recommended;
  service {
    values [service-value];
  }
  severity {
    values [critical info major minor warning];
  }
  type {
    values [anomaly signature];
  }
}
```

**Hierarchy Level** [edit security idp dynamic-attack-group *dynamic-attack-group-name*]

**Release Information** Statement introduced in Release 9.3 of Junos OS. The **expression** option added in Release 11.4 of Junos OS.

**Description** To create a dynamic attack group, set the criteria using different types of filters.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## fin-no-ack

**Syntax** fin-no-ack;

**Hierarchy Level** [edit security screen ids-option *screen-name* tcp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable detection of an illegal combination of flags, and reject packets that have this combination.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Configuration Statement Hierarchy

## firewall-authentication (Security)

**Syntax**
```
firewall-authentication {
  traceoptions {
    flag flag;
  }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Define data-plane firewall authentication tracing options.

**Options**
- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple flag statements.
  - **all**—Enable all tracing operations.
  - **authentication**—Trace data-plane firewall authentication events.
  - **proxy**—Trace data-plane firewall authentication proxy events.
- **detail**—Display moderate amount of data.
- **extensive**—Display extensive amount of data.
- **terse**—Display minimum amount of data.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Firewall User Authentication for Security Devices
- Logical Systems for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## firewall-authentication (Security Policies)

**Syntax**

```
firewall-authentication {
  pass-through {
    access-profile profile-name;
    client-match user-or-group-name;
    ssl-termination-profile profile-name;
    web-redirect;
    web-redirect-to-https;
  }
  web-authentication {
    client-match user-or-group-name;
  }
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit]

**Release Information** Statement introduced in Junos OS Release 8.5. Support for the **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10.

**Description** Configure firewall authentication methods.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## first-update

**Syntax** first-update;

**Hierarchy Level** [edit security application-tracking]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Generate an AppTrack start message when a new session begins. (A final message is produced at session end with any option.) This option overrides the **first-update-interval** option if both are specified.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Tracking

Copyright © 2013, Juniper Networks, Inc.

## first-update-interval

**Syntax** first-update-interval *first-update-interval*;

**Hierarchy Level** [edit security application-tracking]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** For long-lived sessions being monitored by AppTrack, configure this value to issue the first update message after a specified number of minutes.



NOTE: The **first-update-interval** setting is disregarded if the **first-update** option is set to log the first message at session start.

**Options** ***minutes***—Maximum number of minutes after session start for the first update message to be sent. This value must be smaller than the **session-update-interval** setting.

**Default:** 1

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Tracking


Copyright © 2013, Juniper Networks, Inc.

## flood (Security ICMP)

**Syntax**

```
flood {
  threshold number;
}
```

**Hierarchy Level** [edit security screen ids-option *screen-name* icmp]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Configure the device to detect and prevent Internet Control Message Protocol (ICMP) floods. An ICMP flood occurs when ICMP echo requests are broadcast with the purpose of flooding a system with so much data that it first slows down, and then times out and is disconnected. The threshold defines the number of ICMP packets per second allowed to ping the same destination address before the device rejects further ICMP packets.

**Options**

**threshold *number*** —Number of ICMP packets per second allowed to ping the same destination address before the device rejects further ICMP packets.

**Range:** 1 through 1000000 per second

**Default:** 1000 per second



NOTE: For SRX Series devices the applicable range is 1 through 4000000 per second.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- flood (Security UDP) on page 594
- Security Configuration Statement Hierarchy

Copyright © 2013, Juniper Networks, Inc.

## flood (Security UDP)

**Syntax**

```
flood {
  threshold number;
}
```

**Hierarchy Level** [edit security screen ids-option *screen-name* udp]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Configure the device to detect and prevent UDP floods. UDP flooding occurs when an attacker sends UDP packets to slow down the system to the point that it can no longer process valid connection requests.

The threshold defines the number of UDP packets per second allowed to ping the same destination IP address/port pair. When the number of packets exceeds this value within any 1-second period, the device generates an alarm and drops subsequent packets for the remainder of that second.

**Options**

**threshold** ***number*** —Number of UDP packets per second allowed to ping the same destination address before the device rejects further UDP packets.

**Range:** 1 through 1000000 per second

**Default:** 1000 per second



NOTE: For SRX series devices the applicable range is 1 through 4000000 per second.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Configuration Statement Hierarchy
- flood (Security ICMP) on page 593


Copyright © 2013, Juniper Networks, Inc.

## flow (Security Flow)

**Syntax**

```
flow {
    aging {
        early-ageout seconds;
        high-watermark percent;
        low-watermark percent;
    }
    allow-dns-reply;
    bridge {
        block-non-ip-all;
        bpdu-vlan-flooding;
        bypass-non-ip-unicast;
        no-packet-flooding {
            no-trace-route;
        }
    }
    force-ip-reassembly;
    load distribution {
        session-affinity ipsec;
    }
    pending-sess-queue-length (high | moderate | normal);
    route-change-timeout seconds;
    syn-flood-protection-mode (syn-cookie | syn-proxy);
    tcp-mss {
        all-tcp mss value;
        gre-in {
            mss value;
        }
        gre-out {
            mss value;
        }
        ipsec-vpn {
            mss value;
        }
    }
    tcp-session {
        no-sequence-check;
        no-syn-check;
        no-syn-check-in-tunnel;
        rst-invalidate-session;
        rst-sequence-check;
        strict-syn-check;
        tcp-initial-timeout seconds;
        time-wait-state {
            (session-ageout | session-timeout seconds);
        }
    }
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
```

Copyright © 2013, Juniper Networks, Inc.

```
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
    packet-filter filter-name {
      destination-port port-identifier;
      destination-prefix address;
      interface interface-name;
      protocol protocol-identifier;
      source-port port-identifier;
      source-prefix address;
    }
    rate-limit messages-per-second;
  }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement modified in Release 9.5 of Junos OS.

**Description** Determine how the device manages packet flow. The device can regulate packet flow in the following ways:

- Enable or disable DNS replies when there is no matching DNS request.
- Set the initial session-timeout values.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- Processing Overview for Security Devices
- Logical Systems for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## flow (Security IDP)

**Syntax**

```
flow {
  (allow-icmp-without-flow | no-allow-icmp-without-flow);
  fifo-max-size value;
  hash-table-size value;
  (log-errors | no-log-errors);
  max-timers-poll-ticks value;
  reject-timeout value;
  (reset-on-policy | no-reset-on-policy);
  udp-anticipated-timeout value;
}
```

**Hierarchy Level** [edit security idp sensor-configuration]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Configure the IDP engine to manage the packet flow.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## force-ip-reassembly

**Syntax** force-ip-reassembly;

**Hierarchy Level** [edit security flow]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Reassemble all IP fragmented packets before forwarding.

This option is disabled by default. You can disable this option by deleting this flag from the CLI.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Flow-Based Processing for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## force-upgrade

**Syntax** force-upgrade;

**Hierarchy Level** [edit security dynamic-vpn]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Use this statement to force users to automatically upgrade the Access Manager when newer versions are available. If you include this statement in your configuration, it is automatically enabled. If the statement is not present in your configuration, the force upgrade option is not enabled.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Dynamic VPNs for Security Devices

## format (Security Log)

**Syntax** format (binary |sd-syslog | syslog)

**Hierarchy Level** [edit security log]

**Release Information** Statement introduced in a release of Junos OS prior to Release 10.0. Updated in Release 12.1 of Junos OS.

**Description** Set the default log format for event mode security logging on the device.

**Options**
- **binary**—Binary encoded text to conserve resources.
- **sd-syslog**—Structured system log file.
- **syslog**—Traditional system log file.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- System Log Messages
- Application Tracking


Copyright © 2013, Juniper Networks, Inc.

## format (Security Log Stream)

**Syntax** format (binary | sd-syslog | syslog | welf)

**Hierarchy Level** [edit security log stream *stream-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS. Updated in Release 12.1 of Junos OS.

**Description** Set the format for remote security message logging to **binary**, **syslog** (system log), **sd-syslog** (structured system log), or **welf**. Note that for the WELF format, the category must be set to **content-security** (see category (Security Logging)).

**Options**

- **binary**—Binary encoded text to conserve resources.
- **sd-syslog**—Structured system log file.
- **syslog**—Traditional system log file.
- **welf**—Web Trends Extended Log Format.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Log File Formats
- Application Tracking
- Master Administrator for Logical Systems on Security Devices

Copyright © 2013, Juniper Networks, Inc.

## forwarding-options (Security)

**Syntax**

```
forwarding-options {
  family {
    inet6 {
      mode (drop | flow-based | packet-based);
    }
    iso {
      mode packet-based;
    }
    mpls {
      mode packet-based;
    }
  }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Determine how the **inet6, iso**, and **mpls** protocol families manage security forwarding options.



NOTE: Packet-based processing is not supported on the following SRX Series devices: SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800.

**Options** The remaining statements are explained separately.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- MPLS for Security Devices
- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

## forwarding-process

**Syntax**

```
forwarding-process {
  application-services {
    maximize-alg-sessions;
    maximize-cp-sessions;
    maximize-idp-sessions {
      inline-tap;
      weight (equal | firewall | idp);
    }
    session-distribution-mode {
      hash-based;
    }
  }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Release 9.6 of Junos OS.

**Description** If you are deploying IDP policies, you can tune the device to increase IDP session capacity. By using the provided commands to change the way the system allocates resources, you can achieve a higher IDP session capacity.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Processing Overview for Security Devices
- IDP Policies for Security Devices

## fragment

**Syntax** fragment;

**Hierarchy Level** [edit security screen ids-option *screen-name* icmp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the device to detect and drop any ICMP frame with the More Fragments flag set or with an offset indicated in the **offset** field.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## from (Security NAT)

**Syntax**

```
from {
  interface [interface-name];
  routing-instance [routing-instance-name];
  zone [zone-name];
}
```

**Hierarchy Level**

[edit security nat destination rule-set *rule-set-name*]
[edit security nat source rule-set *rule-set-name*]
[edit security nat static rule-set *rule-set-name*]

**Release Information**

Statement modified in Junos OS Release 9.3.

**Description**

Specify the source of the packet among the routing instance, interface, or zone.

**Options**

- **interface [*interface-name*]** —Name of the interface.
- **routing-instance [*routing-instance-name*]** —Name of the routing instance.
- **zone [*zone-name*]** —Name of the zone.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

## from-zone (Security IDP Policy)

**Syntax**

from-zone (*zone-name* | any);

**Hierarchy Level**

[edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* match]
[edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match]

**Release Information**

Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Junos OS 10.0.

**Description**

Specify a source zone to be associated with the security policy. The default value is any.

**Options**

***zone-name***—Name of the source zone object.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- Application-Level Distributed Denial of Service
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## from-zone (Security Policies)

**Syntax**

```
from-zone zone-name to-zone zone-name {
  policy policy-name {
    description description;
    match {
      application {
        [application];
        any;
      }
      destination-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
      }
      source-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
      }
      source-identity {
        [role-name];
        any;
        authenticated-user;
        unauthenticated-user;
        unknown-user;
      }
    }
    scheduler-name scheduler-name;
    then {
      count {
        alarm {
          per-minute-threshold number;
          per-second-threshold number;
        }
      }
      deny;
      log {
        session-close;
        session-init;
      }
      permit {
        application-services {
          application-firewall {
            rule-set rule-set-name;
          }
          application-traffic-control {
            rule-set rule-set-name;
          }
          gprs-gtp-profile profile-name;
          gprs-sctp-profile profile-name;
          idp;
```

Copyright © 2013, Juniper Networks, Inc.

```
            redirect-wx | reverse-redirect-wx;
            ssl-proxy {
              profile-name profile-name;
            }
            uac-policy {
              captive-portal captive-portal;
            }
            utm-policy policy-name;
          }
          destination-address {
            drop-translated;
            drop-untranslated;
          }
          firewall-authentication {
            pass-through {
              access-profile profile-name;
              client-match user-or-group-name;
              ssl-termination-profile profile-name;
              web-redirect;
              web-redirect-to-https;
            }
            web-authentication {
              client-match user-or-group-name;
            }
          }
          services-offload;
          tcp-options {
            sequence-check-required;
            syn-check-required;
          }
          tunnel {
            ipsec-group-vpn group-vpn;
            ipsec-vpn vpn-name;
            pair-policy pair-policy;
          }
        }
        reject;
      }
    }
  }
```

**Hierarchy Level** [edit security policies]

**Release Information** Statement introduced in Junos OS Release 8.5. Support for the **services-offload** option added in Junos OS Release 11.4. Support for the **source-identity** option added in Junos OS Release 12.1. Support for the **description** option added in Junos OS Release 12.1. Support for the **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10.

**Description** Specify a source zone and destination zone to be associated with the security policy.


Copyright © 2013, Juniper Networks, Inc.

**Options**

- ***zone-name*** —Name of the source zone.
- **to-zone *zone-name***—Name of the destination zone.

The remaining statements are explained separately.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policy
- Security Policies for Security Devices
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## ftp (Security ALG)

**Syntax**

```
ftp {
  allow-mismatch-ip-address;
  disable;
  ftps-extension;
  line-break-extension;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement modified in Release 11.4 of Junos OS.

**Description** Specify the FTP ALG on the device.

**Options**

- **disable**—Disable the FTP ALG. By default, the FTP ALG is enabled. This option will enable or disable FTP ALG for both IPV4 and IPV6 mode.
- **ftps-extension**—Enable secure FTP and FTP SSL protocols.
- **line-break-extension**—Enable line-break-extension. This option will enable the FTP ALG to recognize the LF as line break in addition to the standard CR+LF (carriage return, followed by line feed).
- **traceoptions**—Configure FTP ALG tracing options. To specify more than one trace operation, include multiple flag statements.
  - **flag**—Trace operation to perform.
    - **all**—Trace all events.
    - **extensive**—(Optional) Display extensive amount of data.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Layer Gateways for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ftp (UTM Policy Anti-Virus)

**Syntax**

```
ftp {
  download-profile profile-name;
  upload-profile profile-name;
}
```

**Hierarchy Level** [edit security utm utm-policy *policy-name* anti-virus]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the antivirus FTP protocol and attach this policy to a security profile to implement it.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## ftp (UTM Policy Content Filtering)

**Syntax**

```
ftp {
  download-profile profile-name;
  upload-profile profile-name;
}
```

**Hierarchy Level** [edit security utm utm-policy *policy-name* content-filtering]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the content-filtering FTP protocol and attach this policy to a security profile to implement it.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM Content Filtering for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## functional-zone

**Syntax**

```
functional-zone {
  management {
    description text;
    host-inbound-traffic {
      protocols protocol-name {
        except;
      }
      system-services service-name {
        except;
      }
    }
    interfaces interface-name  {
      host-inbound-traffic {
        protocols protocol-name {
          except;
        }
        system-services service-name {
          except;
        }
      }
    }
    screen screen-name;
  }
}
```

**Hierarchy Level** [edit security zones]

**Release Information** Statement introduced in Junos OS Release 8.5. The **description** option added in Junos OS Release 12.1.

**Description** Configure a functional zone.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Zones and Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## gatekeeper

**Syntax**

```
gatekeeper {
    threshold rate;
}
```

**Hierarchy Level** [edit security alg h323 application-screen message-flood]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Limit the rate at which remote access server (RAS) requests to the gatekeeper are processed. Messages exceeding the threshold are dropped.

**Options** **threshold *rate***—Threshold measured in messages per second.

**Range:** 1 through 50000

**Default:** 1000

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Layer Gateways for Security Devices

## gateway (Security Group VPN Member IKE)

**Syntax**

```
gateway gateway-name {
    address [ip-address-or-hostname];
    ike-policy policy-name;
    local address ip-address;
    local-identity {
        (distinguished-name | hostname hostname | inet ip-address | user-at-hostname
            e-mail-address);
    }
}
```

**Hierarchy Level** [edit security group-vpn member ike]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure IKE gateway for group VPN member.

**Options** ***gateway-name*** —Name of the gateway.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## gateway (Security Group VPN Server IKE)

**Syntax**

```
gateway gateway-name {
  address ip-address-or-hostname;
  dynamic {
    (distinguished-name <container container-string> <wildcard wildcard-string> | hostname
      domain-name | inet ip-address | user-at-hostname e-mail-address);
  }
  ike-policy policy-name;
  local-identity {
    (distinguished-name | hostname hostname | inet ip-address | user-at-hostname
      e-mail-address);
  }
}
```

**Hierarchy Level** [edit security group-vpn server ike]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure IKE gateway for group VPN server.

**Options** ***gateway-name*** —Name of the gateway.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Group VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## gateway (Security IKE)

**Syntax**

```
gateway gateway-name {
  address [ip-address-or-hostname];
  dead-peer-detection {
    always-send;
    interval seconds;
    threshold number;
  }
  dynamic {
    connections-limit number;
    (distinguished-name <container container-string> <wildcard wildcard-string> | hostname
      domain-name | inet ip-address | inet6 ipv6-address | user-at-hostname e-mail-address);
    ike-user-type (group-ike-id | shared-ike-id);
  }
  external-interface external-interface-name;
  general-ikeid;
  ike-policy policy-name;
  local-identity {
    (distinguished-name | hostname hostname | inet ip-address | inet6 ipv6-address |
      user-at-hostname e-mail-address);
  }
  nat-keepalive seconds;
  no-nat-traversal;
  remote-identity {
    (distinguished-name <container container-string> <wildcard wildcard-string> | hostname
      hostname | inet ip-address | inet6 ipv6-address | user-at-hostname e-mail-address);
  }
  version (v1-only | v2-only);
  xauth {
    access-profile profile-name;
  }
}
```

**Hierarchy Level** [edit security ike]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS. The **inet6** option added in Release 11.1 of Junos OS.

**Description** Configure an IKE gateway.

**Options** *gateway-name* —Name of the gateway.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## gateway (Security IPsec VPN)

**Syntax** gateway *ip-address*;

**Hierarchy Level** [edit security ipsec vpn *vpn-name* ike]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the IP address of the peer.

**Options** *ip-address*—IP address of the peer.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- IPsec VPNs for Security Devices

## gateway (Security Manual SA)

**Syntax** gateway ***ip-address***;

**Hierarchy Level** [edit security ipsec vpn *vpn-name* manual]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS.

**Description** For a manual security association, specify the IPv4 or IPv6 address of the peer. (This statement is not supported on dynamic VPN implementations.)

**Options** ***ip-address*** —IPv4 or IPv6 address of the peer.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## general-ikeid

**Syntax** general-ikeid;

**Hierarchy Level** [edit security ike gateway *gateway-name*]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Accept general peer IKE ID.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IPsec VPNs for Security Devices

## global (Security IDP)

**Syntax**
```
global {
  (enable-all-qmodules | no-enable-all-qmodules);
  (enable-packet-pool | no-enable-packet-pool);
  gtp (decapsulation | no-decapsulation);
  memory-limit-percent value;
  (policy-lookup-cache | no-policy-lookup-cache);
}
```

**Hierarchy Level** [edit security idp sensor-configuration]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Configure the global rulebase IDP security policy.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## global (Security Policies)

**Syntax**

```
global {
  policy policy-name {
    description description;
    match {
      application {
        [application];
        any;
      }
      destination-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
      }
      source-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
      }
      source-identity {
        [role-name];
        any;
        authenticated-user;
        unauthenticated-user;
        unknown-user;
      }
    }
    scheduler-name scheduler-name;
    then {
      count {
        alarm {
          per-minute-threshold number;
          per-second-threshold number;
        }
      }
      deny;
      log {
        session-close;
        session-init;
      }
      permit {
        application-services {
          application-firewall {
            rule-set rule-set-name;
          }
          application-traffic-control {
            rule-set rule-set-name;
          }
          gprs-gtp-profile profile-name;
          gprs-sctp-profile profile-name;
          idp;
```


Copyright © 2013, Juniper Networks, Inc.

```
            redirect-wx | reverse-redirect-wx;
            ssl-proxy {
              profile-name profile-name;
            }
            uac-policy {
              captive-portal captive-portal;
            }
            utm-policy policy-name;
          }
          destination-address {
            drop-translated;
            drop-untranslated;
          }
          firewall-authentication {
            pass-through {
              access-profile profile-name;
              client-match user-or-group-name;
              web-redirect;
            }
            web-authentication {
              client-match user-or-group-name;
            }
          }
          services-offload;
          tcp-options {
            sequence-check-required;
            syn-check-required;
          }
        }
        reject;
      }
    }
}
```

**Hierarchy Level** [edit security policies]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Configure a global policy.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## gprs

**Syntax**

```
gprs {
    gtp {
        enable;
        profile profile-name {
            apn pattern-string {
                imsi-prefix imsi-prefix-digits {
                    action {
                        drop;
                        pass;
                        selection (ms|net|vrf);
                    }
                }
            }
            drop {
                aa-create-pdp (0 | 1 | 2 | all);
                aa-delete-pdp (0 | 1 | 2 | all);
                bearer-resource (0 | 1 | 2 | all);
                change-notification (0 | 1 | 2 | all);
                config-transfer (0 | 1 | 2 | all);
                context (0 | 1 | 2 | all);
                create-bearer (0 | 1 | 2 | all);
                create-data-forwarding (0 | 1 | 2 | all);
                create pdp (0 | 1 | 2 | all);
                create-session (0 | 1 | 2 | all);
                create-tnl-forwarding (0 | 1 | 2 | all);
                cs-paging (0 | 1 | 2 | all);
                data-record (0 | 1 | 2 | all);
                delete-bearer (0 | 1 | 2 | all);
                delete-command (0 | 1 | 2 | all);
                delete-data-forwarding (0 | 1 | 2 | all);
                delete-pdn (0 | 1 | 2 | all);
                delete-pdp (0 | 1 | 2 | all);
                delete-session (0 | 1 | 2 | all);
                detach (0 | 1 | 2 | all);
                downlink-notification (0 | 1 | 2 | all);
                echo (0 | 1 | 2 | all);
                error-indication (0 | 1 | 2 | all);
                failure-report (0 | 1 | 2 | all);
                fwd-access (0 | 1 | 2 | all);
                fwd-relocation (0 | 1 | 2 | all);
                fwd-srns-context (0 | 1 | 2 | all);
                g-pdu (0 | 1 | 2 | all);
                identification (0 | 1 | 2 | all);
                mbms-sess-start (0 | 1 | 2 | all);
                mbms-sess-stop (0 | 1 | 2 | all);
                mbms-sess-update (0 | 1 | 2 | all);
                modify-bearer (0 | 1 | 2 | all);
                modify-command (0 | 1 | 2 | all);
                node-alive (0 | 1 | 2 | all);
                note-ms-present (0 | 1 | 2 | all);
                pdu-notification (0 | 1 | 2 | all);
                ran-info (0 | 1 | 2 | all);
```


Copyright © 2013, Juniper Networks, Inc.

```
            redirection (0 | 1 | 2 | all);
            release-access (0 | 1 | 2 | all);
            relocation-cancel (0 | 1 | 2 | all);
            resume (0 | 1 | 2 | all);
            send-route (0 | 1 | 2 | all);
            sgsn-context (0 | 1 | 2 | all);
            stop-paging (0 | 1 | 2 | all);
            supported-extension (0 | 1 | 2 | all);
            suspend (0 | 1 | 2 | all);
            trace-session (0 | 1 | 2 | all);
            update-bearer (0 | 1 | 2 | all);
            update-pdn (0 | 1 | 2 | all);
            update-pdp (0 | 1 | 2 | all);
            ver-not-supported (0 | 1 | 2 | all);
          }
          gtp-in-gtp-denied;
          log {
            forwarded (basic | detail);
            prohibited (basic | detail);
            rate-limited {
              (basic | detail);
              frequency-number number;
            }
            state-invalid (basic | detail);
          }
          max-message-length number;
          min-message-length number;
          rate-limit limit;
          remove-ie {
            version v1 {
            number ie-number;
            release (R6 | R7 | R8 | R9);
            }
          }
          restart-path (all | create | echo);
          timeout (value);
        }
        traceoptions {
          file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
          }
          flag flag;
          no-remote-trace;
        }
      }
      sctp {
        log {
          configuration;
          decoding-error;
          dropped-packet;
          exceeding-rate-limit;
        }
```

```
profile profile-name {
  association-timeout time-in-minutes;
  drop {
    m3ua-service {
      isup;
      sccp;
      tup;
    }
    payload-protocol {
      all;
      asap;
      bicc;
      ddp-segment;
      ddp-stream;
      dua;
      enrp;
      h248;
      h323;
      iua;
      m2pa;
      m2ua;
      m3ua;
      qipc;
      reserved;
      simco;
      sua;
      tali;
      v5ua;
    }
  }
  handshake-timeout time-in-seconds;
  limit {
    rate {
      address ip-address {
        sccp rate-limit;
        ssp rate-limit;
        sst rate-limit;
      }
      sccp rate-limit;
      ssp rate-limit;
      sst rate-limit;
    }
  }
}
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
}
```


Copyright © 2013, Juniper Networks, Inc.

}

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure GPRS features.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- General Packet Radio Service for Security Devices

## gprs-gtp-profile

**Syntax** gprs-gtp-profile *profile-name*;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]

**Release Information** Statement introduced in Junos OS Release 11.1.

**Description** Specify the name of the GPRS tunneling protocol profile.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- General Packet Radio Service for Security Devices

## gprs-sctp-profile

**Syntax** gprs-sctp-profile *profile-name*;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]

**Release Information** Statement introduced in Junos OS Release 11.1.

**Description** Specify the name of the GPRS stream control protocol profile.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- General Packet Radio Service for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## gre-in

**Syntax**

```
gre-in {
  mss value;
}
```

**Hierarchy Level** [edit security flow tcp-mss]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable and specify the TCP maximum segment size (TCP MSS) for Generic Routing Encapsulation (GRE) packets that are coming out from an IPsec VPN tunnel. If the device receives a GRE-encapsulated TCP packet with the SYN bit and TCP MSS option set and the TCP MSS option specified in the packet exceeds the TCP MSS specified by the device, the device modifies the TCP MSS value accordingly. By default, a TCP MSS for GRE packets is not set.

**Options** mss *value* —TCP MSS for GRE packets. Value is optional.

**Range:** 64 through 63535 bytes

**Default:** 1320 bytes, if no value is specified

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Flow-Based Processing for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## gre-out

**Syntax**

```
gre-out {
  mss value;
}
```

**Hierarchy Level** [edit security flow tcp-mss]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable and specify the TCP maximum segment size (TCP MSS) for Generic Routing Encapsulation (GRE) packets that are going into an IPsec VPN tunnel. If the device receives a GRE-encapsulated TCP packet with the SYN bit and TCP MSS option set and the TCP MSS option specified in the packet exceeds the TCP MSS specified by the device, the device modifies the TCP MSS value accordingly. By default, a TCP MSS for GRE packets is not set.

**Options**

mss *value*—TCP MSS for GRE packets. Value is optional.

**Range:** 64 through 65,535 bytes

**Default:** 1320 bytes

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Flow-Based Processing for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## group (Security Group VPN)

**Syntax**

```
group name {
  activation-time-delay seconds;
  anti-replay-time-window seconds;
  description description;
  group-id number;
  ike-gateway gateway-name;
  ipsec-sa name {
    match-policy policy-name {
      destination ip-address/netmask;
      destination-port number;
      protocol number;
      source ip-address/netmask;
      source-port number;
    }
    proposal proposal-name;
  }
  no-anti-replay;
  server-address ip-address;
  server-member-communication {
    certificate certificate-id;
    communication-type (multicast | unicast);
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    heartbeat seconds;
    lifetime-seconds seconds;
    multicast-group address;
    multicast-outgoing-interface interface;
    number-of-retransmission number;
    retransmission-period seconds;
    sig-hash-algorithm (md5 | sha1);
  }
}
```

**Hierarchy Level** [edit security group-vpn server]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure group VPN on the group server.

**Options** *name*—Name of the group.

- **activation-time-delay** *seconds*—Time, in seconds, before a group member can use a new key when a member reregisters with the group server. When a member registers for the first time with the server (the member does not have a key), there is no delay. When the server sends a rekey message to the member, the member waits twice the **activation-time-delay** value before using the new key. Specify a value from 10 to 900. The default is 15 seconds.


Copyright © 2013, Juniper Networks, Inc.



NOTE: The lifetime-seconds values of all IPsec SA proposals and of the server-member-communication in the group must be at least 10 times the activation-time-delay value.

- **anti-replay-time-window** ***seconds***—Configure antireplay time in seconds. Specify a value from 60 to 360. The default is 100 seconds.
- **description** ***description***—Description of the group.
- **group-id** ***number***—Identifier for this group VPN. Specify a value from 1 to 65,535.
- **ike-gateway** ***gateway-name***—Define the group member for Phase 1 negotiation. There can be multiple instances of this option configured, one for each member of the group. When a group member sends its registration request to the server, the server checks to see that the member is configured for the group.
- **no-anti-replay**—Disable the antireplay mechanism.
- **server-address** ***ip-address***—(Required) IP address of the group server.



NOTE: We recommend that you use the loopback address of the device for server-address.

The remaining statements are explained separately.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Group VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## group-members

**Syntax** group-members [*attack-or-attack-group-name*];

**Hierarchy Level** [edit security idp custom-attack-group *custom-attack-group-name*]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the group members in a custom group. The members can be predefined attacks, predefined attack groups, custom attacks, or custom dynamic groups.

Use custom groups for the following tasks:

- To define a specific set of attacks to which you know your network is vulnerable.
- To group your custom attack objects.
- To define a specific set of informational attack objects that you use to keep you aware of what is happening on your network.

**Options** ***attack-or-attack-group-name***—Name of the attack object or group attack object.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## group-vpn

**Syntax**

```
group-vpn {
    co-location;
    member {
        ike {
            gateway gateway-name {
                address [ip-address-or-hostname];
                ike-policy policy-name;
                local-address ip-address;
                local-identity {
                    (distinguished-name | hostname hostname | inet ip-address | user-at-hostname
                        e-mail-address);
                }
            }
            policy policy-name {
                certificate {
                    local-certificate certificate-id;
                    peer-certificate-type [pkcs7 | x509-signature);
                }
                description description;
                mode (aggressive | main);
                pre-shared-key (ascii-text key | hexadecimal key);
                proposal-set (basic | compatible | standard);
                proposals [proposal-name];
            }
            proposal proposal-name {
                authentication-algorithm (md5 | sha-256 | sha1);
                authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
                description description;
                dh-group (group1 | group14 | group2 | group5);
                encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
                lifetime-seconds seconds;
            }
        }
        ipsec {
            vpn vpn-name {
                group id;
                group-vpn-external-interface interface;
                heartbeat-threshold number;
                ike-gateway gateway-name;
            }
        }
    }
    server {
        group name {
            activation-time-delay seconds;
            anti-replay-time-window seconds;
            description description;
            group-id number;
            ike-gateway gateway-name;
            ipsec-sa name {
                match-policy policy-name {
                    destination ip-address/netmask;
```

Copyright © 2013, Juniper Networks, Inc.

```
            destination-port number;
            protocol number;
            source ip-address/netmask;
            source-port number;
          }
          proposal proposal-name;
        }
        no-anti-replay;
        server-address ip-address;
        server-member-communication {
          certificate certificate-id;
          communication-type (multicast | unicast);
          encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
          heartbeat seconds;
          lifetime-seconds seconds;
          multicast-group address;
          multicast-outgoing-interface interface;
          number-of-retransmission number;
          retransmission-period seconds;
          sig-hash-algorithm (md5 | sha1);
        }
      }
      ike {
        gateway gateway-name {
          address ip-address-or-hostname;
          dynamic {
            (distinguished-name <container container-string> <wildcard wildcard-string> |
              hostname domain-name | inet ip-address | user-at-hostname e-mail-address);
          }
          ike-policy policy-name;
          local-identity {
            (distinguished-name | hostname hostname | inet ip-address | user-at-hostname
              e-mail-address);
          }
        }
        policy policy-name {
          certificate {
            local-certificate certificate-id;
            peer-certificate-type [pkcs7 | x509-signature);
          }
          description description;
          mode (aggressive | main);
          pre-shared-key (ascii-text key | hexadecimal key);
          proposal-set (basic | compatible | standard);
          proposals [proposal-name];
        }
        proposal proposal-name {
          authentication-algorithm (md5 | sha-256 | sha1);
          authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
          description description;
          dh-group (group1 | group14 | group2 | group5);
          encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
        }
      }
      ipsec {
        proposal proposal-name {
```


Copyright © 2013, Juniper Networks, Inc.

```
            authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
            description description;
            encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
            lifetime-seconds seconds;
          }
        }
        traceoptions {
          file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
          }
          flag flag;
          no-remote-trace;
        }
      }
    }
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure group VPNs.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Group VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## gtp

**Syntax**

```
gtp {
    enable;
    profile profile-name {
        apn pattern-string {
            imsi-prefix imsi-prefix-digits {
                action {
                    drop;
                    pass;
                    selection (ms|net|vrf);
                }
            }
        }
        drop {
            aa-create-pdp (0 | 1 | 2 | all);
            aa-delete-pdp (0 | 1 | 2 | all);
            bearer-resource (0 | 1 | 2 | all);
            change-notification (0 | 1 | 2 | all);
            config-transfer (0 | 1 | 2 | all);
            context (0 | 1 | 2 | all);
            create-bearer (0 | 1 | 2 | all);
            create-data-forwarding (0 | 1 | 2 | all);
            create pdp (0 | 1 | 2 | all);
            create-session (0 | 1 | 2 | all);
            create-tnl-forwarding (0 | 1 | 2 | all);
            cs-paging (0 | 1 | 2 | all);
            data-record (0 | 1 | 2 | all);
            delete-bearer (0 | 1 | 2 | all);
            delete-command (0 | 1 | 2 | all);
            delete-data-forwarding (0 | 1 | 2 | all);
            delete-pdn (0 | 1 | 2 | all);
            delete-pdp (0 | 1 | 2 | all);
            delete-session (0 | 1 | 2 | all);
            detach (0 | 1 | 2 | all);
            downlink-notification (0 | 1 | 2 | all);
            echo (0 | 1 | 2 | all);
            error-indication (0 | 1 | 2 | all);
            failure-report (0 | 1 | 2 | all);
            fwd-access (0 | 1 | 2 | all);
            fwd-relocation (0 | 1 | 2 | all);
            fwd-srns-context (0 | 1 | 2 | all);
            g-pdu (0 | 1 | 2 | all);
            identification (0 | 1 | 2 | all);
            mbms-sess-start (0 | 1 | 2 | all);
            mbms-sess-stop (0 | 1 | 2 | all);
            mbms-sess-update (0 | 1 | 2 | all);
            modify-bearer (0 | 1 | 2 | all);
            modify-command (0 | 1 | 2 | all);
            node-alive (0 | 1 | 2 | all);
            note-ms-present (0 | 1 | 2 | all);
            pdu-notification (0 | 1 | 2 | all);
            ran-info (0 | 1 | 2 | all);
            redirection (0 | 1 | 2 | all);
```


Copyright © 2013, Juniper Networks, Inc.

```
        release-access (0 | 1 | 2 | all);
        relocation-cancel (0 | 1 | 2 | all);
        resume (0 | 1 | 2 | all);
        send-route (0 | 1 | 2 | all);
        sgsn-context (0 | 1 | 2 | all);
        stop-paging (0 | 1 | 2 | all);
        supported-extension (0 | 1 | 2 | all);
        suspend (0 | 1 | 2 | all);
        trace-session (0 | 1 | 2 | all);
        update-bearer (0 | 1 | 2 | all);
        update-pdn (0 | 1 | 2 | all);
        update-pdp (0 | 1 | 2 | all);
        ver-not-supported (0 | 1 | 2 | all);
      }
      gtp-in-gtp-denied;
      log {
        forwarded (basic | detail);
        prohibited (basic | detail);
        rate-limited {
          (basic | detail);
          frequency-number number;
        }
        state-invalid (basic | detail);
      }
      max-message-length number;
      min-message-length number;
      rate-limit limit;
      remove-ie {
        version v1 {
        number ie-number;
        release (R6 | R7 | R8 | R9);
        }
      }
      restart-path (all | create | echo);
      timeout (value);
    }
    traceoptions {
      file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
      }
      flag flag;
      no-remote-trace;
    }
}
```

**Hierarchy Level** [edit security gprs]

**Release Information** Statement introduced in Release 10.0 of Junos OS. The **restart-path** option added in Release 11.4 of Junos OS. New GTP message types added in Release 11.4 of Junos OS. Support for GTPv2 added in Release 11.4 of Junos OS.

Copyright © 2013, Juniper Networks, Inc.

**Description** Use the GTP commands to enable the GTP service, configure GTP objects, set traceoptions, remove GTP inspection object configurations, and obtain configuration information.

A Juniper Networks security device provides firewall protection for the following types of GPRS interfaces:

- Gn—The Gn interface is the connection between a Serving GPRS Support Node (SGSN) and a Gateway GPRS Support Node (GGSN) within the same Public Land Mobile Network (PLMN).
- Gp—The Gp interface is the connection between two PLMNs.
- Gi—The Gi interface is the connection between a GGSN and the Internet or destination networks connected to a PLMN.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- General Packet Radio Service for Security Devices

## gtp-in-gtp-denied

**Syntax** gtp-in-gtp-denied;

**Hierarchy Level** [edit security gprs gtp profile *profile-name*]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Select this option to enable the security device to detect and drop a GTP packet that contains another GTP packet in its message body.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- General Packet Radio Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## h323

**Syntax**

```
h323 {
  application-screen {
    message-flood {
      gatekeeper {
        threshold rate;
      }
    }
    unknown-message {
      permit-nat-applied;
      permit-routed;
    }
  }
  disable;
  dscp-rewrite {
    code-point string;
  }
  endpoint-registration-timeout value-in-seconds;
  media-source-port-any;
  traceoptions {
    flag flag <detail | extensive | terse>;
  }
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the H.323 Application Layer Gateway (ALG) on the device. H.323 is a control-signaling protocol used to exchange messages between H.323 endpoints.

**Options** **disable**—Disable the H.323 ALG. By default, H.323 ALG is enabled.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- H.323 ALGs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## handshake-timeout

**Syntax** handshake-timeout *time-in-seconds*;

**Hierarchy Level** [edit security gprs sctp profile *profile-name*]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Set the handshake time for Stream Control Transmission Protocol (SCTP).

**Options** ***time-in-seconds***—Number of seconds of handshake time that elapse before the session is terminated. **Range:** 10 to 30 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- General Packet Radio Service for Security Devices

## hash-based

**Syntax** hash-based;

**Hierarchy Level** [edit security forwarding-process application-services session-distribution-mode]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Tune the device to hash based to alter the load distribution on a central point and to forward cache-missed packets to a selected SPU instead of forwarding the packet to a central point. Note that you must reboot the device for the configuration to take effect.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Flow-Based Processing for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## hash-table-size (Security IDP)

**Syntax** hash-table-size *value*;

**Hierarchy Level** [edit security idp sensor-configuration flow]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Sets the packet flow hash table size (range: 1024 through 1000000).

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices

## header-length

**Syntax**
```
header-length {
  match (equal | greater-than | less-than | not-equal);
  value header-length;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the number of bytes in the TCP header.

**Options**
- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***header-length***—Match the number of bytes in the TCP header.

  **Range:** 0 through 15 bytes

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## high-availability (Security IDP)

**Syntax**
```
high-availability {
  no-policy-cold-synchronization;
}
```

**Hierarchy Level** [edit security idp sensor-configuration]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Configures high availability (chassis cluster) for IDP.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices

## high-watermark

**Syntax** high-watermark *percent*;

**Hierarchy Level** [edit security flow aging]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Sets the point at which the aggressive aging-out process begins.

**Options** ***percent*** —Percentage of session-table capacity at which aggressive aging-out starts.
**Range:** 1 through 100 percent
**Default:** 100 percent

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Flow-Based Processing for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## history

**Syntax**

```
routing-engine
  {
    history
    {
      level;
      resource <cpu | memory |open-files-count |process-count | storage | temperature>;
      {
        level ;
      }
    }
  }
```

**Hierarchy Level** [edit snmp health-monitor routing-engine history]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Enable or disable history logging support for the routing engine.

**Options**

- **level**—Specifies the history logging level. The following levels are available:
  - **any**—Log all events.
  - **moderate-threshold**—Log moderate and above threshold events.
  - **high-threshold** —Log high and above threshold events.
  - **critical-threshold** —Log critical events only.
  - **none**—Disable logging.



NOTE: If a resource-specific history configuration is not available, the global configuration is used.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Device and Routing Operations Monitoring

Copyright © 2013, Juniper Networks, Inc.

## hit-rate-threshold

**Syntax** hit-rate-threshold *number*;

**Hierarchy Level** [edit security idp application-ddos *application-name* context *context-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure context hit rate thresholds to start bot client classifications for application-level distributed denial-of-service (DDoS) protection. The value is measured in number of contexts seen in tick interval (one tick is equal to 60 seconds). The context is an application protocol context such as: http-url and dns-cname. When the threshold is reached, the system will begin client classification using time-binding, if time-binding parameters are configured.

If time-binding is not configured, the system will skip bot client classification, and the configured policy actions are taken. This could result in valid clients being applied with configured policy actions. Time-binding configuration (count and period) should be used for bot client classification. However, this feature can be used as an Application Layer screen to deny resource access for all clients when context **hit-rate-threshold** is exceeded.

The context hit rate is the number of hits in tick interval for the same context type, for example: http-url for a specific application-level DDoS protected application.

**Options** *number*—Context hit rate threshold from bot client.

**Range:**

- SRX3400– 1 to 250,000,000
- SRX3600–1 to 500,000,000
- SRX5600/5800–1 to 2,500,000,000

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service


Copyright © 2013, Juniper Networks, Inc.

## host (Security IDP Sensor Configuration)

**Syntax** host *ip-address* <port *number*>;

**Hierarchy Level** [edit security idp sensor-configuration packet-log]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the IP address and port number of the server where the packet capture object will be sent.

**Options**
- **host *ip-address***—The IP address of the server where the packet capture object will be sent.
- **port *number***—The port number of the server where the packet capture object will be sent.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## host (Security Log)

**Syntax**
```
host {
  ip-address;
  port port-number;
}
```

**Hierarchy Level** [edit security log stream *stream-name*]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** You can specify the IP address of the server to which the security logs will be streamed.

**Options**
- ***ip-address***—Specify IP address of the host.
- **port *port-number***—Specify UDP port number.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- System Log Messages
- Security Logs
- CLI Statements and Commands

Copyright © 2013, Juniper Networks, Inc.

## host (Security Web Filtering)

**Syntax** host *host-name*;

**Hierarchy Level** [edit security utm feature-profile web-filtering surf-control-integrated server]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name* server]
[edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name* server]

**Release Information** Statement introduced in Release 9.5 of Junos OS.
Statement introduced in Release 11.4 of Junos OS for Enhanced Web Filtering.

**Description** Set server host parameters by entering the server name or IP address.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

## host-address-base

**Syntax** host-address-base *ip-address*;

**Hierarchy Level** [edit security nat source pool *pool-name*]

**Release Information** Statement introduced in Junos OS Release 9.2.

**Description** Specify the base address of the original source IP address range. This is used for IP shifting.

**Options** ***ip-address*** —IP address.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## host-inbound-traffic

**Syntax**

```
host-inbound-traffic {
  protocols protocol-name {
    except;
  }
  system-services service-name {
    except;
  }
}
```

**Hierarchy Level** [edit security zones functional-zone management],
[edit security zones functional-zone management interfaces *interface-name*],
[edit security zones security-zone *zone-name*],
[edit security zones security-zone *zone-name* interfaces *interface-name*]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Control the type of traffic that can reach the device from interfaces bound to the zone.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- Security Zones and Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## host (SSH Known Hosts)

**Syntax**

```
host hostname {
    dsa-key dsa-key;
    ecdsa-sha2-nistp256-key ecdsa-sha2-nistp256-key;
    ecdsa-sha2-nistp384-key ecdsa-sha2-nistp384-key;
    ecdsa-sha2-nistp521-key ecdsa-sha2-nistp521-key;
    rsa-key rsa-key;
    rsa1-key rsa1-key;
}
```

**Hierarchy Level** [edit security ssh-known-hosts]

**Release Information** Statement modified in Junos OS Release 8.5.

**Description** Configure the type of base-64 encoded host key.

**Options**

- ***hostname***—Name of the SSH known host.
- **dsa-key *dsa-key***—Digital Signature Algorithm (DSA) for SSH version 2
- **ecdsa-sha2-nistp256-key *ecdsa-sha2-nistp256-key***—Elliptic Curve Digital Signature Algorithm (ECDSA)
- **ecdsa-sha2-nistp384-key *ecdsa-sha2-nistp384-key***—Elliptic Curve Digital Signature Algorithm (ECDSA)
- **ecdsa-sha2-nistp521-key *ecdsa-sha2-nistp521-key***—Elliptic Curve Digital Signature Algorithm (ECDSA)
- **rsa-key *rsa-key***—RSA public key algorithm, which supports encryption and digital signatures for SSH version 1 and SSH version 2
- **rsa1-key *rsa1-key***—RSA public key algorithm, which supports encryption and digital signatures for SSH version 1

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

## hostname

**Syntax** hostname *domain-name*;

**Hierarchy Level** [edit security group-vpn server ike gateway *gateway-name* dynamic]
[edit security ike gateway *gateway-name* dynamic]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn server** hierarchy added in Release 10.2 of Junos OS.

**Description** Unique name by which a network-attached device is known on a network.

**Options** ***domain-name***—A fully qualified domain name (FQDN).

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

## http-profile (Security Antivirus)

**Syntax** http-profile *profile-name*;

**Hierarchy Level** [edit security utm utm-policy *policy-name* anti-virus]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the antivirus HTTP protocol and attach this policy to a security profile to implement it.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## http-profile (Security Content Filtering)

**Syntax** http-profile *profile-name*;

**Hierarchy Level** [edit security utm utm-policy *policy-name* content-filtering]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the content-filtering HTTP protocol and attach this policy to a security profile to implement it.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices

## http-profile (Security Web Filtering)

**Syntax** http-profile *profile-name*;

**Hierarchy Level** [edit security utm utm-policy *policy-name* web-filtering]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the web-filtering HTTP protocol and attach this policy to a security profile to implement it.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## icmp (Security IDP Custom Attack)

**Syntax** icmp;

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type chain protocol-binding]
[edit security idp custom-attack *attack-name* attack-type signature protocol-binding]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Allow IDP to match the attack for specified ICMP.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## icmp (Security IDP Signature Attack)

**Syntax**

```
icmp {
  code {
    match (equal | greater-than | less-than | not-equal);
    value code-value;
  }
  data-length {
    match (equal | greater-than | less-than | not-equal);
    value data-length;
  }
  identification {
    match (equal | greater-than | less-than | not-equal);
    value identification-value;
  }
  sequence-number {
    match (equal | greater-than | less-than | not-equal);
    value sequence-number;
  }
  type {
    match (equal | greater-than | less-than | not-equal);
    value type-value;
  }
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Allow IDP to match the ICMP header information for the signature attack.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## icmp (Security Screen)

**Syntax**

```
icmp {
  flood {
    threshold number;
  }
  fragment;
  ip-sweep {
    threshold number;
  }
  large;
  ping-death;
}
```

**Hierarchy Level** [edit security screen ids-option *screen-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure ICMP intrusion detection service (IDS) options.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Configuration Statement Hierarchy

## icmpv6 (Security IDP)

**Syntax** icmpv6;

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type chain protocol-binding]
[edit security idp custom-attack *attack-name* attack-type signature protocol-binding]

**Release Information** Statement introduced in Junos OS Release 9.3.

**Description** Specify that the attack is for ICMPv6 packets only.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## identification (Security ICMP Headers)

**Syntax**

```
identification {
  match (equal | greater-than | less-than | not-equal);
  value identification-value;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol icmp]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify a unique value used by the destination system to associate requests and replies.

**Options**

- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***identification-value***—Match a decimal value.

  **Range:** 0 through 65,535

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## identification (Security IP Headers)

**Syntax**

```
identification {
  match (equal | greater-than | less-than | not-equal);
  value identification-value;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol ipv4]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify a unique value used by the destination system to reassemble a fragmented packet.

**Options**

- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***identification-value***—Match a decimal value.

  **Range:** 0 through 65,535

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## idle-time

**Syntax** idle-time *seconds*;

**Hierarchy Level** [edit security ipsec vpn *vpn-name* ike]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the maximum amount of idle time to delete a security association (SA).

**Options** ***seconds*** —Maximum amount of idle time.
**Range:** 60 through 999999 seconds
**Default:** To be disabled

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

## idp (Application Services)

**Syntax** idp;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]

**Release Information** Statement introduced in Junos OS Release 11.1.

**Description** Configure Intrusion Detection and Prevention (IDP) for application services.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## idp (Security)

**Syntax**

```
idp {
  active-policy policy-name;
  application-ddos application-name {
    connection-rate-threshold number;
    context context-name {
      exclude-context-values [value];
      hit-rate-threshold number;
      max-context-values number;
      time-binding-count number;
      time-binding-period seconds;
      value-hit-rate-threshold number;
    }
    service service-name;
  }
  custom-attack attack-name {
    attack-type {
      anomaly {
        direction (any | client-to-server | server-to-client);
        service service-name;
        shellcode (all | intel | no-shellcode | sparc);
        test test-condition;
      }
      chain {
        expression boolean-expression;
        member member-name {
          attack-type {
            (anomaly ...same statements as in [edit security idp custom-attack attack-name
              attack-type anomaly] hierarchy level | signature ...same statements as in [edit
              security idp custom-attack attack-name attack-type signature] hierarchy
              level);
          }
        }
        order;
        protocol-binding {
          application application-name;
          icmp;
          icmpv6;
          ip {
            protocol-number transport-layer-protocol-number;
          }
          ipv6 {
            protocol-number transport-layer-protocol-number;
          }
          nested-application nested-application-name;
          rpc {
            program-number rpc-program-number;
          }
          tcp {
            minimum-port port-number <maximum-port port-number>;
          }
          udp {
            minimum-port port-number <maximum-port port-number>;
```


Copyright © 2013, Juniper Networks, Inc.

```
        }
    }
    reset;
    scope (session | transaction);
}
signature {
    context context-name;
    direction (any | client-to-server | server-to-client);
    negate;
    pattern signature-pattern;
    protocol {
        icmp {
            code {
                match (equal | greater-than | less-than | not-equal);
                value code-value;
            }
            data-length {
                match (equal | greater-than | less-than | not-equal);
                value data-length;
            }
            identification {
                match (equal | greater-than | less-than | not-equal);
                value identification-value;
            }
            sequence-number {
                match (equal | greater-than | less-than | not-equal);
                value sequence-number;
            }
            type {
                match (equal | greater-than | less-than | not-equal);
                value type-value;
            }
        }
        ipv4 {
            destination {
                match (equal | greater-than | less-than | not-equal);
                value ip-address-or-hostname;
            }
            identification {
                match (equal | greater-than | less-than | not-equal);
                value identification-value;
            }
            ip-flags {
                (df | no-df);
                (mf | no-mf);
                (rb | no-rb);
            }
            protocol {
                match (equal | greater-than | less-than | not-equal);
                value transport-layer-protocol-id;
            }
            source {
                match (equal | greater-than | less-than | not-equal);
                value ip-address-or-hostname;
            }
            tos {
```

```
        match (equal | greater-than | less-than | not-equal);
        value type-of-service-in-decimal;
      }
      total-length {
        match (equal | greater-than | less-than | not-equal);
        value total-length-of-ip-datagram;
      }
      ttl {
        match (equal | greater-than | less-than | not-equal);
        value time-to-live;
      }
    }
    ipv6 {
      destination {
        match (equal | greater-than | less-than | not-equal);
        value ip-address-or-hostname;
      }
      flow-label {
        match (equal | greater-than | less-than | not-equal);
        value flow-label-value;
      }
      hop-limit {
        match (equal | greater-than | less-than | not-equal);
        value hop-limit-value;
      }
      next-header {
        match (equal | greater-than | less-than | not-equal);
        value next-header-value;
      }
      payload-length {
        match (equal | greater-than | less-than | not-equal);
        value payload-length-value;
      }
      source {
        match (equal | greater-than | less-than | not-equal);
        value ip-address-or-hostname;
      }
      traffic-class {
        match (equal | greater-than | less-than | not-equal);
        value traffic-class-value;
      }
    tcp {
      ack-number {
        match (equal | greater-than | less-than | not-equal);
        value acknowledgement-number;
      }
      data-length {
        match (equal | greater-than | less-than | not-equal);
        value tcp-data-length;
      }
      destination-port {
        match (equal | greater-than | less-than | not-equal);
        value destination-port;
      }
      header-length {
        match (equal | greater-than | less-than | not-equal);
```


Copyright © 2013, Juniper Networks, Inc.

```
            value header-length;
        }
        mss {
            match (equal | greater-than | less-than | not-equal);
            value maximum-segment-size;
        }
        option {
            match (equal | greater-than | less-than | not-equal);
            value tcp-option;
        }
        sequence-number {
            match (equal | greater-than | less-than | not-equal);
            value sequence-number;
        }
        source-port {
            match (equal | greater-than | less-than | not-equal);
            value source-port;
        }
        tcp-flags {
            (ack | no-ack);
            (fin | no-fin);
            (psh | no-psh);
            (r1 | no-r1);
            (r2 | no-r2);
            (rst | no-rst);
            (syn | no-syn);
            (urg | no-urg);
        }
        urgent-pointer {
            match (equal | greater-than | less-than | not-equal);
            value urgent-pointer;
        }
        window-scale {
            match (equal | greater-than | less-than | not-equal);
            value window-scale-factor;
        }
        window-size {
            match (equal | greater-than | less-than | not-equal);
            value window-size;
        }
    }
    udp {
        data-length {
            match (equal | greater-than | less-than | not-equal);
            value data-length;
        }
        destination-port {
            match (equal | greater-than | less-than | not-equal);
            value destination-port;
        }
        source-port {
            match (equal | greater-than | less-than | not-equal);
            value source-port;
        }
    }
}
```

```
        protocol-binding {
          application application-name;
          icmp;
          icmpv6;
          ip {
            protocol-number transport-layer-protocol-number;
          }
          ipv6 {
            protocol-number transport-layer-protocol-number;
          }
          nested-application nested-application-name;
          rpc {
            program-number rpc-program-number;
          }
          tcp {
            minimum-port port-number <maximum-port port-number>;
          }
          udp {
            minimum-port port-number <maximum-port port-number>;
          }
        }
        regexp regular-expression;
        shellcode (all | intel | no-shellcode | sparc);
      }
    }
    recommended-action (close | close-client | close-server | drop | drop-packet | ignore |
      none);
    severity (critical | info | major | minor | warning);
    time-binding {
      count count-value;
      scope (destination | peer | source);
    }
  }
  custom-attack-group custom-attack-group-name {
    group-members [attack-or-attack-group-name];
  }
  dynamic-attack-group dynamic-attack-group-name {
    filters {
      category {
        values [category-value];
      }
      direction {
        expression (and | or);
        values [any client-to-server exclude-any exclude-client-to-server
          exclude-server-to-client server-to-client];
      }
      false-positives {
        values [frequently occasionally rarely unknown];
      }
      performance {
        values [fast normal slow unknown];
      }
      products {
        values [product-value];
      }
      recommended;
```


Copyright © 2013, Juniper Networks, Inc.

```
    service {
      values [service-value];
    }
    severity {
      values [critical info major minor warning];
    }
    type {
      values [anomaly signature];
    }
  }
}
idp-policy policy-name {
  rulebase-ddos {
    rule rule-name {
      description text;
      match {
        application (application-name | any | default);
        application-ddos <application-name>;
        destination-address ([address-name] | any | any-ipv4 | any-ipv6);
        destination-except [address-name];
        from-zone (zone-name | any);
        source-address ([address-name] | any | any-ipv4 | any-ipv6);
        source-except [address-name];
        to-zone (zone-name | any);
      }
      then {
        action {
          (close-server | drop-connection | drop-packet | no-action);
        }
        ip-action {
          (ip-block | ip-close | ip-connection-rate-limit connections-per-second | ip-notify);
          log;
          log-create;
          refresh-timeout;
          timeout seconds;
        }
        notification {
          log-attacks {
            alert;
          }
        }
      }
    }
  }
  rulebase-exempt {
    rule rule-name {
      description text;
      match {
        attacks {
          custom-attack-groups [attack-group-name];
          custom-attacks [attack-name];
          dynamic-attack-groups [attack-group-name];
          predefined-attack-groups [attack-group-name];
          predefined-attacks [attack-name];
        }
        destination-address ([address-name] | any | any-ipv4 | any-ipv6);
```

Copyright © 2013, Juniper Networks, Inc.

```
        destination-except [address-name];
        from-zone (zone-name | any );
        source-address ([address-name] | any | any-ipv4 | any-ipv6);
        source-except [address-name];
        to-zone (zone-name | any);
      }
    }
  }
  rulebase-ips {
    rule rule-name {
      description text;
      match {
        application (application-name | any | default);
        attacks {
          custom-attack-groups [attack-group-name];
          custom-attacks [attack-name];
          dynamic-attack-groups [attack-group-name];
          predefined-attack-groups [attack-group-name];
          predefined-attacks [attack-name];
        }
        destination-address ([address-name] | any | any-ipv4 | any-ipv6);
        destination-except [address-name];
        from-zone (zone-name | any );
        source-address ([address-name] | any | any-ipv4 | any-ipv6);
        source-except [address-name];
        to-zone (zone-name | any);
      }
      terminal;
      then {
        action {
          class-of-service {
            dscp-code-point number;
            forwarding-class forwarding-class;
          }
          (close-client | close-client-and-server | close-server |drop-connection |
            drop-packet | ignore-connection | mark-diffserv value | no-action |
            recommended);
        }
        ip-action {
          (ip-block | ip-close | ip-notify);
          log;
          log-create;
          refresh-timeout;
          target (destination-address | service | source-address | source-zone |
            source-zone-address | zone-service);
          timeout seconds;
        }
        notification {
          log-attacks {
            alert;
          }
          packet-log {
            post-attack number;
            post-attack-timeout seconds;
            pre-attack number;
          }
```


Copyright © 2013, Juniper Networks, Inc.

```
            }
            severity (critical | info | major | minor | warning);
          }
        }
      }
    }
    security-package {
      automatic {
        download-timeout minutes;
        enable;
        interval hours;
        start-time start-time;
      }
      install {
        ignore-version-check;
      }
      source-address address;
      url url-name;
    }
    sensor-configuration {
      application-ddos {
        statistics {
          interval minutes;
        }
      }
      application-identification {
        max-packet-memory value;
        max-tcp-session-packet-memory value;
        max-udp-session-packet-memory value;
      }
      detector {
        protocol-name protocol-name {
          tunable-name  tunable-name {
            tunable-value protocol-value;
          }
        }
      }
      flow {
        (allow-icmp-without-flow | no-allow-icmp-without-flow);
        fifo-max-size value;
        hash-table-size value;
        (log-errors | no-log-errors);
        max-timers-poll-ticks value;
        reject-timeout value;
        (reset-on-policy | no-reset-on-policy);
        udp-anticipated-timeout value;
      }
      global {
        (enable-all-qmodules | no-enable-all-qmodules);
        (enable-packet-pool | no-enable-packet-pool);
        gtp (decapsulation | no-decapsulation);
        memory-limit-percent value;
        (policy-lookup-cache | no-policy-lookup-cache);
      }
      high-availability {
        no-policy-cold-synchronization;
```

Copyright © 2013, Juniper Networks, Inc.

```
    }
    ips {
      content-decompression-max-memory-kb value;
      content-decompression-max-ratio value;
      (detect-shellcode | no-detect-shellcode);
      fifo-max-size value;
      (ignore-regular-expression | no-ignore-regular-expression);
      log-supercede-min minimum-value;
      pre-filter-shellcode;
      (process-ignore-s2c | no-process-ignore-s2c);
      (process-override | no-process-override);
      process-port port-number;
    }
    log {
      cache-size size;
      suppression {
        disable;
        (include-destination-address | no-include-destination-address);
        max-logs-operate value;
        max-time-report value;
        start-log value;
      }
    }
    packet-log {
      host ip-address <port number>;
      max-sessions percentage;
      source-address ip-address;
      total-memory percentage;
    }
    re-assembler {
      (ignore-memory-overflow | no-ignore-memory-overflow);
      (ignore-reassembly-memory-overflow | no-ignore-reassembly-memory-overflow);
      ignore-reassembly-overflow;
      max-flow-mem value;
      max-packet-mem value;
    }
    ssl-inspection {
      cache-prune-chunk-size number;
      key-protection;
      maximum-cache-size number;
      session-id-cache-timeout seconds;
      sessions number;
    }
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag all;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
```


Copyright © 2013, Juniper Networks, Inc.

}

**Hierarchy Level** [edit security]

**Release Information** Statement modified in Release 9.3 of Junos OS. The **expression** option added in Release 11.4 of Junos OS.

**Description** Configure Intrusion Detection and Prevention (IDP) to selectively enforce various IDP attack detection and prevention techniques on the network.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application-Level Distributed Denial of Service
- Master Administrator for Logical Systems on Security Devices

## idp (Security Alarms)

**Syntax** idp;

**Hierarchy Level** [edit security alarms potential-violation]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Configure alarms for IDP attack.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## idp-policy (Security)

**Syntax**

```
idp-policy policy-name {
  rulebase-ddos {
    rule rule-name {
      description text;
      match {
        application (application-name | any | default);
        application-ddos <application-name>;
        destination-address ([address-name] | any | any-ipv4 | any-ipv6);
        destination-except [address-name];
        from-zone (zone-name | any);
        source-address ([address-name] | any | any-ipv4 | any-ipv6);
        source-except [address-name];
        to-zone (zone-name | any);
      }
      then {
        action {
          (close-server | drop-connection | drop-packet | no-action);
        }
        ip-action {
          (ip-block | ip-close | ip-connection-rate-limit connections-per-second | ip-notify);
          log;
          log-create;
          refresh-timeout;
          timeout seconds;
        }
        notification {
          log-attacks {
            alert;
          }
        }
      }
    }
  }
  rulebase-exempt {
    rule rule-name {
      description text;
      match {
        attacks {
          custom-attack-groups [attack-group-name];
          custom-attacks [attack-name];
          dynamic-attack-groups [attack-group-name];
          predefined-attack-groups [attack-group-name];
          predefined-attacks [attack-name];
        }
        destination-address ([address-name] | any | any-ipv4 | any-ipv6);
        destination-except [address-name];
        from-zone (zone-name | any );
        source-address ([address-name] | any | any-ipv4 | any-ipv6);
        source-except [address-name];
        to-zone (zone-name | any);
      }
    }
```


Copyright © 2013, Juniper Networks, Inc.

```
    }
    rulebase-ips {
      rule rule-name {
        description text;
        match {
          application (application-name | any | default);
          attacks {
            custom-attack-groups [attack-group-name];
            custom-attacks [attack-name];
            dynamic-attack-groups [attack-group-name];
            predefined-attack-groups [attack-group-name];
            predefined-attacks [attack-name];
          }
          destination-address ([address-name] | any | any-ipv4 | any-ipv6);
          destination-except [address-name];
          from-zone (zone-name | any );
          source-address ([address-name] | any | any-ipv4 | any-ipv6);
          source-except [address-name];
          to-zone (zone-name | any);
        }
        terminal;
        then {
          action {
            class-of-service {
              dscp-code-point number;
              forwarding-class forwarding-class;
            }
            (close-client | close-client-and-server | close-server |drop-connection | drop-packet
              | ignore-connection | mark-diffserv value | no-action | recommended);
          }
          ip-action {
            (ip-block | ip-close | ip-notify);
            log;
            log-create;
            refresh-timeout;
            target (destination-address | service | source-address | source-zone |
              source-zone-address | zone-service);
            timeout seconds;
          }
          notification {
            log-attacks {
              alert;
            }
            packet-log {
              post-attack number;
              post-attack-timeout seconds;
              pre-attack number;
            }
          }
          severity (critical | info | major | minor | warning);
        }
      }
    }
  }
```

Copyright © 2013, Juniper Networks, Inc.

**Hierarchy Level** [edit security idp]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Configure a security IDP policy.

**Options** ***policy-name***—Name of the IDP policy.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- Application-Level Distributed Denial of Service
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ids-option

**Syntax**

```
ids-option screen-name {
    alarm-without-drop;
    description text;
    icmp {
      flood {
        threshold number;
      }
      fragment;
      ip-sweep {
        threshold number;
      }
      large;
      ping-death;
    }
    ip {
      bad-option;
      block-frag;
      loose-source-route-option;
      record-route-option;
      security-option;
      source-route-option;
      spoofing;
      stream-option;
      strict-source-route-option;
      tear-drop;
      timestamp-option;
      unknown-protocol;
    }
    limit-session {
      destination-ip-based number;
      source-ip-based number;
    }
    tcp {
      fin-no-ack;
      land;
      port-scan {
        threshold number;
      }
      syn-ack-ack-proxy {
        threshold number;
      }
      syn-fin;
      syn-flood {
        alarm-threshold number;
        attack-threshold number;
        destination-threshold number;
        source-threshold number;
        timeout seconds;
        white-list name {
          destination-address destination-address;
          source-address source-address;
        }
```

```
        }
        syn-frag;
        tcp-no-flag;
        tcp-sweep {
          threshold threshold number;
        }
        winnuke;
      }
      udp {
        flood {
          threshold number;
        }
        udp-sweep {
          threshold threshold number;
        }
      }
    }
}
```

**Hierarchy Level** [edit security screen]

**Release Information** Statement introduced in Release 8.5 of Junos OS. The **description** option added in Release 12.1 of Junos OS.

**Description** Define screens for intrusion detection service (IDS).

**Options** **description** ***text***—Descriptive text about screen.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Configuration Statement Hierarchy

## ignore-memory-overflow

**Syntax** (ignore-memory-overflow | no-ignore-memory-overflow);

**Hierarchy Level** [edit security idp sensor-configuration re-assembler]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Enable the TCP reassembler to ignore the memory overflow to prevent the dropping of IDP custom applications. By default this feature is enabled.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ignore-reassembly-overflow

**Syntax** ignore-reassembly-overflow

**Hierarchy Level** [edit security idp sensor-configuration re-assembler]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Enable the TCP reassembler to ignore the global reassembly overflow to prevent the dropping of application traffic. This feature is enabled by default.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## ignore-reassembly-memory-overflow | no-ignore-reassembly-memory-overflow

**Syntax** (ignore-reassembly-memory-overflow | no-ignore-reassembly-memory-overflow);

**Hierarchy Level** [edit security idp sensor-configuration re-assembler]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Ignores or accepts the packet reassembly memory overflow.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## ignore-regular-expression

**Syntax** (ignore-regular-expression | no-ignore-regular-expression);

**Hierarchy Level** [edit security idp sensor-configuration ips]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Enable regular expression to detect intrusion attempts. By default this setting is disabled.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ike (Security)

**Syntax**

```
ike {
  gateway gateway-name {
    address [ip-address-or-hostname];
    dead-peer-detection {
      always-send;
      interval seconds;
      threshold number;
    }
    dynamic {
      connections-limit number;
      (distinguished-name <container container-string> <wildcard wildcard-string> |
        hostname domain-name | inet ip-address | inet6 ipv6-address | user-at-hostname
        e-mail-address);
      ike-user-type (group-ike-id | shared-ike-id);
    }
    external-interface external-interface-name;
    general-ikeid;
    ike-policy policy-name;
    local-identity {
      (distinguished-name | hostname hostname | inet ip-address | inet6 ipv6-address |
        user-at-hostname e-mail-address);
    }
    nat-keepalive seconds;
    no-nat-traversal;
    remote-identity {
      (distinguished-name <container container-string> <wildcard wildcard-string> |
        hostname hostname | inet ip-address | inet6 ipv6-address | user-at-hostname
        e-mail-address);
    }
    version (v1-only | v2-only);
    xauth {
      access-profile profile-name;
    }
  }
  policy policy-name {
    certificate {
      local-certificate certificate-id;
      peer-certificate-type (pkcs7 | x509-signature);
    }
    description description;
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposal-set (basic | compatible | standard);
    proposals [proposal-name];
  }
  proposal proposal-name {
    authentication-algorithm (md5 | sha-256 | sha1);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    description description;
    dh-group (group1 | group14 | group2 | group5);
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    lifetime-seconds seconds;
```

Copyright © 2013, Juniper Networks, Inc.

```
    }
    respond-bad-spi <max-responses>;
    traceoptions {
      file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
      }
      flag flag;
      no-remote-trace;
      rate-limit messages-per-second;
    }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement modified in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS. The **inet6** option added in Release 11.1 of Junos OS.

**Description** Define Internet Key Exchange (IKE) configuration.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- ALG for IKE and ESP for Security Devices
- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- IPsec VPNs for Security Devices
- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ike (Security Group VPN Member)

**Syntax**

```
ike {
  gateway gateway-name {
    address [ip-address-or-hostname];
    ike-policy policy-name;
    local-address ip-address;
    local-identity {
      (distinguished-name | hostname hostname | inet ip-address | user-at-hostname
        e-mail-address);
    }
  }
  policy policy-name {
    certificate {
      local-certificate certificate-id;
      peer-certificate-type [pkcs7 | x509-signature);
    }
    description description;
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposal-set (basic | compatible | standard);
    proposals [proposal-name];
  }
  proposal proposal-name {
    authentication-algorithm (md5 | sha-256 | sha1);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    description description;
    dh-group (group1 | group14 | group2 | group5);
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    lifetime-seconds seconds;
  }
}
```

**Hierarchy Level** [edit security group-vpn member]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure IPsec group VPN on the group member.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Group VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## ike (Security Group VPN Server)

**Syntax**

```
ike {
  gateway gateway-name {
    address ip-address-or-hostname;
    dynamic {
      (distinguished-name <container container-string> <wildcard wildcard-string> |
        hostname domain-name | inet ip-address | user-at-hostname e-mail-address);
    }
    ike-policy policy-name;
    local-identity {
      (distinguished-name | hostname hostname | inet ip-address | user-at-hostname
        e-mail-address);
    }
  }
  policy policy-name {
    certificate {
      local-certificate certificate-id;
      peer-certificate-type [pkcs7 | x509-signature);
    }
    description text;
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposal-set (basic | compatible | standard);
    proposals [proposal-name];
  }
  proposal proposal-name {
    authentication-algorithm (md5 | sha-256 | sha1);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    description description;
    dh-group (group1 | group14 | group2 | group5);
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
  }
}
```

**Hierarchy Level** [edit security group-vpn server]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure Phase 1 security association (SA) with a member on the group server. The gateway is the group member.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Group VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ike (Security IPsec VPN)

**Syntax**

```
ike {
  gateway gateway-name;
  idle-time seconds;
  install-interval seconds;
  ipsec-policy ipsec-policy-name;
  no-anti-replay;
  proxy-identity {
    local ip-prefix;
    remote ip-prefix;
    service (any | service-name);
  }
}
```

**Hierarchy Level** [edit security ipsec vpn *vpn-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS.

**Description** Define an IKE-keyed IPsec VPN.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## ike-phase1-failures

**Syntax**

```
ike-phase1-failures {
  threshold value;
}
```

**Hierarchy Level** [edit security alarms potential-violation]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Raise a security alarm after exceeding a specified number of Internet Key Exchange (IKE) Phase 1 failures.

**Default** Multiple IKE phase 1 failures do not cause an alarm to be raised.

**Options** *failures*—Number of IKE phase 1 failures up to which an alarm is not raised. When the configured number is exceeded, an alarm is raised.

**Range:** 1 through 1000000000.

**Default:** 20

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ike-phase2-failures

**Syntax**

```
ike-phase2-failures {
    threshold value;
}
```

**Hierarchy Level** [edit security alarms potential-violation]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Raise a security alarm after exceeding a specified number of Internet Key Exchange (IKE) phase 2 failures.

**Default** Multiple IKE phase 2 failures do not cause an alarm to be raised.

**Options** *failures*—Number of IKE phase 2 failures up to which an alarm is not raised. When the configured number is exceeded, an alarm is raised.

**Range:** 1 through 1000000000.

**Default:** 20

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## ike-policy (Security Gateway)

**Syntax** ike-policy *policy-name*;

**Hierarchy Level** [edit security group-vpn member ike gateway *gateway-name*]
[edit security group-vpn server ike gateway *gateway-name*]
[edit security ike gateway *gateway-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

**Description** Specify the IKE policy to be used for the gateway.

**Options** ***policy-name*** —IKE policy name.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

## ike-user-type

**Syntax** ike-user-type (group-ike-id | shared-ike-id);

**Hierarchy Level** [edit security ike gateway *gateway-name* dynamic]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the type of IKE user for a remote access connection.

**Options**
- **group-ike-id**—E-mail address or fully qualified domain name (FQDN) shared for a group of remote access users so that each one does not need a separate IKE profile configured.
- **shared-ike-id**—E-mail address shared for a large number of remote access users so that each one does not need a separate IKE profile configured.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## imap-profile (Security UTM Policy Antivirus)

**Syntax** imap-profile *profile-name*;

**Hierarchy Level** [edit security utm utm-policy *policy-name* anti-virus]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the antivirus IMAP protocol and attach this policy to a security profile to implement it.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## imap-profile (Security UTM Policy Content Filtering)

**Syntax** imap-profile *profile-name*;

**Hierarchy Level** [edit security utm utm-policy *policy-name* content-filtering]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the content-filtering IMAP protocol and attach this policy to a security profile to implement it.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## inactive-media-timeout (Security MGCP)

**Syntax** inactive-media-timeout *value-in-seconds*;

**Hierarchy Level** [edit security alg mgcp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the maximum amount of time that the temporary openings in the firewall (pinholes) remain open for media if no activity is detected.

**Options** ***value-in-seconds***—Maximum amount of time that the pinholes remain open.
**Range:** 10 through 2550 seconds
**Default:** 120 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- MGCP ALGs for Security Devices

## inactive-media-timeout (Security SCCP)

**Syntax** inactive-media-timeout *value-in-seconds*;

**Hierarchy Level** [edit security alg sccp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the maximum amount of time that the temporary openings in the firewall (pinholes) remain open for media if no activity is detected.

**Options** ***value-in-seconds***—Maximum amount of time that the pinholes remain open.
**Range:** 10 through 600 seconds
**Default:** 120 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- SCCP ALGs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## inactive-media-timeout (Security SIP)

**Syntax** inactive-media-timeout *value-in-seconds*;

**Hierarchy Level** [edit security alg sip]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the maximum amount of time that the temporary openings in the firewall (pinholes) remain open for media if no activity is detected.

**Options** ***value-in-seconds***—Maximum amount of time that the pinholes remain open.
**Range:** 0 through 2550 seconds
**Default:** 120 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- SIP ALGs for Security Devices

## inactivity-timeout (Security Persistent NAT)

**Syntax** inactivity-timeout *seconds*;

**Hierarchy Level** [edit security nat source rule-set *ruleset* rule *rule* then source-nat interface persistent-nat]
[edit security nat source rule-set *ruleset* rule *rule* then source-nat pool persistent-nat]

**Release Information** Statement introduced in Junos OS Release 9.6.

**Description** The amount of time, in seconds, that the persistent NAT binding remains in the Juniper Networks device's memory when all the sessions of the binding entry are gone. When the configured timeout is reached, the binding is removed from memory.

**Options** *seconds*—Number of seconds.
**Range:** 60 through 7200 seconds
**Default:** 300 seconds (5 minutes)

**Required Privilege Level** **security**—To view this statement in the configuration.
**security-control**—To add this statement to the configuration

**Related Documentation**
- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## include-destination-address

**Syntax** (include-destination-address | no-include-destination-address);

**Hierarchy Level** [edit security idp sensor-configuration log suppression]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** When log suppression is enabled, multiple occurrences of events with the same source, service, and matching attack object generate a single log record with a count of occurrences. If you enable this option, log suppression will only combine log records for events with a matching source as well. The IDP Sensor does not consider destination when determining matching events for log suppression. By default this setting is disabled.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## inet (Security Dynamic Peer)

**Syntax** inet *ip-address*;

**Hierarchy Level** [edit security group-vpn server ike gateway *gateway-name* dynamic]
[edit security ike gateway *gateway-name* dynamic]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn server** hierarchy added in Release 10.2 of Junos OS.

**Description** Specify IP address to identify the dynamic peer. (This statement is not supported on dynamic VPN implementations.)

**Options** ***ip-address***—IP address.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## inet (Security Static NAT)

**Syntax**

```
inet {
  routing-instance (default | routing-instance-name);
}
```

**Hierarchy Level** [edit security nat static rule-set *rule-set-name* rule *rule-name* then static-nat]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify the translated IPV4 address of the static NAT rule.

**Options**

- **routing-instance** ***routing-instance-name*** —Use the user-defined static NAT routing-instance to perform static NAT.
- **default**—Default routing-instance. By default, the **routing-instance** is the same as the **from routing-instance**.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

## inet6 (Security Forwarding Options)

**Syntax**

```
inet6 {
  mode (drop | flow-based | packet-based);
}
```

**Hierarchy Level** [edit security forwarding-options family]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable packet-based or flow-based processing of IPv6 traffic. By default, the device drops IPv6 traffic.



NOTE: Packet-based processing is not supported on the following SRX Series devices: SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800.

**Options** The **mode** statement is described separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Layer 2 Bridging and Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## inet6 (Security IKE Gateway)

**Syntax** inet6 *ipv6-address*;

**Hierarchy Level** [edit security ike gateway *gateway-name* dynamic]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Specify an IPv6 address to identify the dynamic peer. (This statement is not supported on dynamic VPN implementations.)

**Options** ***ipv6-address***—IPv6 address.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

## inline-tap

**Syntax** inline-tap;

**Hierarchy Level** [edit security forwarding-process application-services maximize-idp-sessions]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Enable IDP inline tap mode. The inline tap feature provides passive, inline detection of application layer threats for traffic matching security policies which have the IDP application service enabled. When a device is in inline tap mode, packets pass through firewall inspection and are also copied to the independent IDP module.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Processing Overview for Security Devices
- IDP Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## install

**Syntax**

```
install {
  ignore-version-check;
}
```

**Hierarchy Level** [edit security idp security-package]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Configures the **install** command.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## install-interval

**Syntax** install-interval *seconds*;

**Hierarchy Level** [edit security ipsec vpn *vpn-name* ike]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the maximum number of seconds to allow for the installation of a rekeyed outbound security association (SA) on the device.

**Options** ***seconds*** —Maximum amount of idle time.

**Range:** 0 through 10 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## intelligent-prescreening

**Syntax** intelligent-prescreening;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* scan-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Enables intelligent prescreening.

Intelligent prescreening tells the antivirus module to begin scanning a file much earlier. In this case, the scan engine uses the first packet or the first several packets to determine if a file could possibly contain malicious code. The scan engine does a quick check on these first packets and if the scan engine finds that it is unlikely that the file is infected, it then determines that it is safe to bypass the normal scanning procedure.

You can disable intelligent prescreening with the **no-intelligent-prescreening** statement.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## interface (Security NAT ARP Proxy)

**Syntax**

```
interface interface-name {
  address ip-address {
    to ip-address;
  }
}
```

**Hierarchy Level** [edit security nat proxy-arp]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify the interface on which the ARP proxy is to be configured. It should be a logical interface.

**Options** *interface-name*—Name of the logical interface.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

## interface (Security NAT NDP Proxy)

**Syntax**

```
interface interface-name {
  address ip-address {
    to ip-address;
  }
}
```

**Hierarchy Level** [edit security nat proxy-ndp]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify the interface on which the NDP proxy is to be configured. It should be a logical interface.

**Options** *interface-name*—Name of the logical interface.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## interface (Security Source NAT)

**Syntax**

```
interface {
  port-overloading {
    off;
  }
}
```

**Hierarchy Level** [edit security nat source]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Enable interface NAT with or without port overloading.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

## interface (Security Source NAT Rule Set)

**Syntax**

```
interface {
  persistent-nat {
    address-mapping;
    inactivity-timeout seconds;
    max-session-number value;
    permit (any-remote-host | target-host | target-host-port);
  }
}
```

**Hierarchy Level** [edit security nat source rule-set *rule-set-name* rule *rule-name* then source-nat]

**Release Information** Statement introduced in Junos OS Release 9.6.

**Description** Enable interface NAT with or without port overloading.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## interface (Security Dynamic VPN)

**Syntax** interface [ *interface-names* ];

**Hierarchy Level** [edit security dynamic-vpn]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify a list of interfaces to set the interfaces that allow access to dynamic VPN.

**Options** *interface-names* —Names of one or more Interfaces that accept dynamic VPN client access, separated by spaces.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Dynamic VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## interfaces (Security Zones)

**Syntax**

```
interfaces interface-name {
  host-inbound-traffic {
    protocols protocol-name {
      except;
    }
    system-services service-name {
      except;
    }
  }
}
```

**Hierarchy Level** [edit security zones functional-zone management],
[edit security zones security-zone *zone-name*]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the set of interfaces that are part of the zone.

**Options** ***interface-name*** —Name of the interface.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- Security Zones and Interfaces for Security Devices
- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

## interval (Security Antivirus)

**Syntax** interval *value*;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine pattern-update]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]
[edit security utm feature-profile anti-virus sophos-engine pattern-update]

**Release Information** Statement introduced in Release 9.5 of Junos OS for Juniper Express engine and Kaspersky Lab engine. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** Set the pattern data files auto-update interval. You can choose to leave the default interval value or you can change it by using this command. You can also force a manual update, if necessary.



NOTE: The data files used with Sophos are not a typical virus pattern files, they are small file that helps guide virus scanning logic. The full virus pattern database is stored on an external Sophos server called the Sophos Extensible List (SXL) server.

**Options** *value*—Pattern data files auto-update interval in minutes.

**Range:** 10 through 10,080 minutes (10 minutes through 7 days)

**Default:** For Juniper Express engine and Kaspersky Lab engine, 60 minutes; for Sophos engine, 1440 minutes (every 24 hours)

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- Unified Threat Management

Copyright © 2013, Juniper Networks, Inc.

## interval (Security IDP)

**Syntax** interval *hours*;

**Hierarchy Level** [edit security idp security-package automatic]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify the amount of time that the device waits before updating the signature database. User should insert a default value.

**Options** ***hours***—Number of hours that the device waits.
**Range:** 24 through 336 hours

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## interval (Security IKE)

**Syntax** interval *seconds*;

**Hierarchy Level** [edit security ike gateway *gateway-name* dead-peer-detection]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the amount of time that the peer waits for traffic from its destination peer before sending a dead-peer-detection (DPD) request packet.

**Options** ***seconds*** —Number of seconds that the peer waits before sending a DPD request packet.
**Range:** 0 through 60 seconds
**Default:** 10 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ip (Security IDP Custom Attack)

**Syntax**

```
ip {
  protocol-number transport-layer-protocol-number;
}
```

**Hierarchy Level**

[edit security idp custom-attack *attack-name* attack-type chain protocol-binding]
[edit security idp custom-attack *attack-name* attack-type signature protocol-binding]

**Release Information**

Statement introduced in Release 9.3 of Junos OS.

**Description**

Allow IDP to match the attack for a specified IP protocol type.

**Options**

**protocol-number *transport-layer-protocol-number***—Transport Layer protocol number.

**Range:** 0 through 139

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## ip (Security Screen)

**Syntax**

```
ip {
    bad-option;
    block-frag;
    loose-source-route-option;
    record-route-option;
    security-option;
    source-route-option;
    spoofing;
    stream-option;
    strict-source-route-option;
    tear-drop;
    timestamp-option;
    unknown-protocol;
}
```

**Hierarchy Level** [edit security screen ids-option *screen-name* ]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure IP layer IDS options.

**Options**

- **bad-option**—Detect and drop any packet with an incorrectly formatted IP option in the IP packet header. The device records the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
- **block-frag**—Enable IP packet fragmentation blocking.
- **loose-source-route-option**—Detect packets where the IP option is 3 (loose source routing), and record the event in the screen counters list for the ingress interface. This option specifies a partial route list for a packet to take on its journey from source to destination. The packet must proceed in the order of addresses specified, but it is allowed to pass through other devices in between those specified. The type 0 routing header of the loose source route option is the only related header defined in IPv6 .
- **record-route-option**—Detect packets where the IP option is 7 (record route), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
- **security-option**—Detect packets where the IP option is 2 (security), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
- **source-route-option**—Detect packets, and record the event in the screen counters list for the ingress interface.
- **spoofing**—Prevent spoofing attacks. Spoofing attacks occur when unauthorized agents attempt to bypass firewall security by imitating valid client IP addresses. Using the spoofing option invalidates such false source IP address connections.

  The default behavior is to base spoofing decisions on individual interfaces.


Copyright © 2013, Juniper Networks, Inc.

- **stream-option**—Detect packets where the IP option is 8 (stream ID), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
- **strict-source-route-option**—Detect packets where the IP option is 9 (strict source routing), and record the event in the screen counters list for the ingress interface. This option specifies the complete route list for a packet to take on its journey from source to destination. The last address in the list replaces the address in the destination field. Currently, this screen option is applicable only to IPv4.
- **tear-drop**—Block the teardrop attack. Teardrop attacks occur when fragmented IP packets overlap and cause the host attempting to reassemble the packets to crash. The teardrop option directs the device to drop any packets that have such a discrepancy.
- **timestamp-option**—Detect packets where the IP option list includes option 4 (Internet timestamp), and record the event in the screen counters list for the ingress interface. Currently, this screen option is applicable only to IPv4.
- **unknown-protocol**—Discard all received IP frames with protocol numbers greater than 137 for IPv4 and 139 for IPv6. Such protocol numbers are undefined or reserved.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Configuration Statement Hierarchy

Copyright © 2013, Juniper Networks, Inc.

## ipv4 (Security IDP Signature Attack)

**Syntax**

```
ipv4 {
  destination {
    match (equal | greater-than | less-than | not-equal);
    value ip-address-or-hostname;
  }
  identification {
    match (equal | greater-than | less-than | not-equal);
    value identification-value;
  }
  ip-flags {
    (df | no-df);
    (mf | no-mf);
    (rb | no-rb);
  }
  protocol {
    match (equal | greater-than | less-than | not-equal);
    value transport-layer-protocol-id;
  }
  source {
    match (equal | greater-than | less-than | not-equal);
    value ip-address-or-hostname;
  }
  tos {
    match (equal | greater-than | less-than | not-equal);
    value type-of-service-in-decimal;
  }
  total-length {
    match (equal | greater-than | less-than | not-equal);
    value total-length-of-ip-datagram;
  }
  ttl {
    match (equal | greater-than | less-than | not-equal);
    value time-to-live;
  }
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Allow IDP to match the IP header information for the signature attack.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ip-action (Security Application-Level DDoS)

**Syntax**

```
ip-action {
    (ip-block | ip-close | ip-connection-rate-limit connections-per-second | ip-notify);
    log;
    log-create;
    refresh-timeout;
    timeout seconds;
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* then]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Specify the actions you want IDP to take against future connections that use the same IP address.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## ip-action (Security IDP Rulebase IPS)

**Syntax**

```
ip-action {
   (ip-block | ip-close | ip-notify);
   log;
   log-create;
   refresh-timeout;
   target (destination-address | service | source-address | source-zone | source-zone-address
      | zone-service);
   timeout seconds;
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify the actions you want IDP to take against future connections that use the same IP address.

**Options** The remaining statements are explained separately.



NOTE: For ICMP flows, the destination port is 0; therefore, any ICMP flow matching source port, source address, and destination address is blocked.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ip-block

**Syntax** ip-block;

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* then ip-action]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then ip-action]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Release 10.0 of Junos OS.

**Description** Block future connections of any session that matches the IP action. If there is an IP action match with multiple rules, then the most severe IP action of all the matched rules is applied. The highest IP action priority (that is, the most severe action) is Drop/Block, then Close, then Notify.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- Application-Level Distributed Denial of Service
- IDP Application Identification for Security Devices

## ip-close

**Syntax** ip-close;

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* then ip-action]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then ip-action]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Release 10.0 of Junos OS.

**Description** Close future connections of any new sessions that match the IP action by sending RST packets to the client and server.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- Application-Level Distributed Denial of Service
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## ip-connection-rate-limit

**Syntax** ip-connection-rate-limit *connections-per-second*;

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* then ip-action]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** When a match is made in a rulebase-ddos rule you can set the **then** action to ip-connection-rate-limit, which will rate limit future connections based on a connections per second limit that you set. This can be used to reduce the number of attacks from a client.

**Options** ***value***—Defines the connection rate limit per second on the matched host.

**Range:** 1 to the maximum connections per second capability of the device.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- Application-Level Distributed Denial of Service
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ip-flags

**Syntax**

```
ip-flags {
   (df | no-df);
   (mf | no-mf);
   (rb | no-rb);
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol ipv4]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify that IDP looks for a pattern match whether or not the IP flag is set.

**Options**

- **df | no-df**—When set, the df (Don't Fragment) indicates that the packet cannot be fragmented for transmission. When unset, it indicates that the packet can be fragmented.
- **mf | no-mf**—When set, the mf (More Fragments) indicates that the packet contains more fragments. When unset, it indicates that no more fragments remain.
- **rb | no-rb**—When set, the rb (Reserved Bit) indicates that the bit is reserved.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## ip-notify

**Syntax** ip-notify;

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* then ip-action]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then ip-action]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Release 10.0 of Junos OS.

**Description** Do not take any action against future traffic, but do log the event.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- Application-Level Distributed Denial of Service
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## ip-sweep

**Syntax**

```
ip-sweep {
  threshold number;
}
```

**Hierarchy Level** [edit security screen ids-option *screen-name* icmp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the device to detect and prevent an IP Sweep attack. An IP Sweep attack occurs when an attacker sends ICMP echo requests (pings) to multiple destination addresses. If a target host replies, the reply reveals the target's IP address to the attacker. If the device receives 10 ICMP echo requests within the number of microseconds specified in this statement, it flags this as an IP Sweep attack, and rejects the 11th and all further ICMP packets from that host for the remainder of the second.

**Options**

**threshold *number***—Maximum number of microseconds during which up to 10 ICMP echo requests from the same host are allowed into the device. More than 10 requests from a host during this period triggers an IP Sweep attack response on the device during the remainder of the second.

**Range:** 1000 through 1,000,000 microseconds

**Default:** 5000 microseconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Configuration Statement Hierarchy


Copyright © 2013, Juniper Networks, Inc.

## ipc

**Syntax**

```
ipc {
  traceoptions flag flag;
}
```

**Hierarchy Level** [edit security utm]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure traceoptions for IPC.

**Options**

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Enable trace for all IPC trace options.
  - **basic**—Trace basic IPC related information.
  - **connection-manager**—Trace IPC connection manager information.
  - **connection-status**—Trace IPC connection status information.
  - **detail**—Trace IPC related detailed information.
  - **pfe**—Trace communication with PFE.
  - **utm-realtime**—Trace IPC realtime-thread information.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM Basics for Security Devices
- Unified Threat Management

Copyright © 2013, Juniper Networks, Inc.

## ips

**Syntax**

```
ips {
  content-decompression-max-memory-kb value;
  content-decompression-max-ratio value;
  (detect-shellcode | no-detect-shellcode);
  fifo-max-size value;
  (ignore-regular-expression | no-ignore-regular-expression);
  log-supercede-min minimum-value;
  pre-filter-shellcode;
  (process-ignore-s2c | no-process-ignore-s2c);
  (process-override | no-process-override);
  process-port port-number;
}
```

**Hierarchy Level** [edit security idp sensor-configuration]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Configure IPS security policy sensor settings.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ipsec (Security)

**Syntax**

```
ipsec {
  policy policy-name {
    description description;
    perfect-forward-secrecy keys (group1 | group14 | group2 | group5);
    proposal-set (basic | compatible | standard);
    proposals [proposal-name];
  }
  proposal proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
    description description;
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    lifetime-kilobytes kilobytes;
    lifetime-seconds seconds;
    protocol (ah | esp);
  }
  traceoptions {
    flag flag;
  }
  vpn vpn-name {
    bind-interface interface-name;
    df-bit (clear | copy | set);
    establish-tunnels (immediately | on-traffic);
    ike {
      gateway gateway-name;
      idle-time seconds;
      install-interval seconds;
      ipsec-policy ipsec-policy-name;
      no-anti-replay;
      proxy-identity {
        local ip-prefix;
        remote ip-prefix;
        service (any | service-name);
      }
    }
    manual {
      authentication {
        algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
      }
      encryption {
        algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
        key (ascii-text key | hexadecimal key);
      }
      external-interface external-interface-name;
      gateway ip-address;
      protocol (ah | esp);
      spi spi-value;
    }
    vpn-monitor {
      destination-ip ip-address;
      optimized;
      source-interface interface-name;
```

```
    }
  }
  vpn-monitor-options {
    interval seconds;
    threshold number;
  }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Define IP Security (IPsec) configuration.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- IPsec VPNs for Security Devices
- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ipsec (Security Group VPN Member)

**Syntax**

```
ipsec {
  vpn vpn-name {
    group id;
    group-vpn-external-interface interface;
    heartbeat-threshold number;
    ike-gateway gateway-name;
  }
}
```

**Hierarchy Level** [edit security group-vpn member]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure IPsec proposal for Phase 2 exchange on the group member.

**Options** **vpn *vpn-name***—Name of the VPN.

- **group *id***—Identifier configured for the group VPN.
- **group-vpn-external-interface *interface***—MPLS-facing interface used by the group member to connect to the group VPN.
- **heartbeat-threshold *number***—Threshold for receiving heartbeats from the group VPN server.
- **ike-gateway *gateway-name***—Name of the IKE gateway for the group VPN.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Group VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## ipsec (Security Group VPN Server)

**Syntax**

```
ipsec {
  proposal proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
    description description;
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    lifetime-seconds seconds;
  }
}
```

**Hierarchy Level** [edit security group-vpn server]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure IPsec proposal for Phase 2 exchange on the group server.

**Options** **proposal *proposal-name***—Name of the proposal. The proposal name can be up to 32 alphanumeric characters long.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Group VPNs for Security Devices

## ipsec-group-vpn (Security Policies)

**Syntax** ipsec-group-vpn *group-vpn*;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit tunnel]

**Release Information** Statement introduced in Junos OS Release 10.2.

**Description** Specify group VPN tunnel for the traffic configured by the scope policy on a group member.

**Options** ***group-vpn*** —Name of the group VPN tunnel configured on the group member.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ipsec-policy (Security)

**Syntax** ipsec-policy *ipsec-policy-name*;

**Hierarchy Level** [edit security ipsec vpn *vpn-name* ike]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the IPsec policy name.

**Options** ***ipsec-policy-name*** —Name of the IPsec policy.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## ipsec-sa

**Syntax**

```
ipsec-sa name {
  match-policy policy-name {
    destination ip-address/netmask;
    destination-port number;
    protocol number;
    source ip-address/netmask;
    source-port number;
  }
  proposal proposal-name;
}
```

**Hierarchy Level** [edit security group-vpn server group *name*]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the group SAs to be downloaded to members. There can be multiple group SAs downloaded to group members.

**Options** **ipsec-sa *name***—Define the group SAs to be downloaded to members.

- **match-policy *policy-name***—Configure the group policy with source address, source port, destination address, destination port, and protocol.

  Use **0.0.0.0** to specify any source or destination. Use **0** to specify any source port, destination port, or protocol.

- **proposal *proposal-name***—Specify the name of the IPsec proposal configured with the **proposal** configuration statement at the [**edit security group-vpn server ipsec**] hierarchy.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Group VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ipsec-vpn (Security Dynamic VPNs)

**Syntax** ipsec-vpn *vpn-name*;

**Hierarchy Level** [edit security dynamic-vpn clients *vpn-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Use this statement to specify which IPsec VPN configuration the dynamic VPN feature should use to secure traffic.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Dynamic VPNs for Security Devices

## ipsec-vpn (Security Flow)

**Syntax**
```
ipsec-vpn {
    mss value;
}
```

**Hierarchy Level** [edit security flow tcp-mss]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the TCP maximum segment size (TCP MSS) for the TCP packets that are about to go into an IPsec VPN tunnel. This value overrides the value specified in the **all-tcp-mss** statement.

**Options** **mss *value***—TCP MSS value for TCP packets entering an IPsec VPN tunnel. Value is optional.

**Range:** 64 through 65,535 bytes

**Default:** 1320 bytes

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## ipsec-vpn (Security Policies)

**Syntax** ipsec-vpn *vpn-name*;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit tunnel]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Define IPsec name for VPN.

**Options** ***vpn-name*** —Name of the IPsec.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## ipv6 (Security IDP)

**Syntax** ipv6;

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type chain protocol-binding]
[edit security idp custom-attack *attack-name* attack-type signature protocol-binding]

**Release Information** Statement introduced in Junos OS Release 9.3.

**Description** Specify that the attack is for all IPv6 packets only.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## iso (Security Forwarding Options)

**Syntax**

```
iso {
  mode packet-based;
}
```

**Hierarchy Level** [edit security forwarding-options family]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable the forwarding of IS-IS traffic. By default, the device drops IS-IS traffic.



NOTE: Junos OS security processing is not applied to IS-IS packets forwarded by the device.



NOTE: Packet-based processing is not supported on the following SRX Series devices: SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

Copyright © 2013, Juniper Networks, Inc.

## juniper-enhanced

**Syntax**

```
juniper-enhanced {
  cache {
    size value;
    timeout value;
  }
  profile profile-name {
    category customurl-list name {
      action (block | log-and-permit | permit | quarantine);
    }
    custom-block-message value;
    custom-quarantine-message value;
    default (block | log-and-permit | permit | quarantine);
    fallback-settings {
      default (block | log-and-permit);
      server-connectivity (block | log-and-permit);
      timeout (block | log-and-permit);
      too-many-requests (block | log-and-permit);
    }
    no-safe-search;
    site-reputation-action {
      fairly-safe (block | log-and-permit | permit | quarantine);
      harmful (block | log-and-permit | permit | quarantine);
      moderately-safe (block | log-and-permit | permit | quarantine);
      suspicious (block | log-and-permit | permit | quarantine);
      very-safe (block | log-and-permit | permit | quarantine);
      }
    timeout value;
  }
  server {
    host host-name;
    port number;
  }
}
```

**Hierarchy Level** [set security utm feature-profile web-filtering]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Configure the UTM Enhanced Web Filtering feature.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## juniper-express-engine

**Syntax**

```
juniper-express-engine {
  pattern-update {
    email-notify {
      admin-email email-address;
      custom-message message;
      custom-message-subject message-subject;
    }
    interval value;
    no-autoupdate;
    proxy {
      password password-string;
      port port-number;
      server address-or-url;
      username name;
    }
    url url;
  }
  profile profile-name {
    fallback-options {
      content-size (block | log-and-permit);
      default (block | log-and-permit);
      engine-not-ready (block | log-and-permit);
      out-of-resources (block | (log-and-permit);
      timeout (block | log-and-permit);
      too-many-requests (block | log-and-permit);
    }
    notification-options {
      fallback-block {
        administrator-email email-address;
        allow-email;
        custom-message message;
        custom-message-subject message-subject;
        display-host;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
      fallback-non-block {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-recipient | no-notify-mail-recipient);
      }
      virus-detection {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
    }
    scan-options {
      content-size-limit value;
      (intelligent-prescreening | no-intelligent-prescreening);
      timeout value;
```

Copyright © 2013, Juniper Networks, Inc.

```
    }
    trickling {
      timeout value;
    }
  }
}
```

**Hierarchy Level** [edit security utm feature-profile anti-virus]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure the UTM express antivirus feature.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

## juniper-local

**Syntax**

```
juniper-local {
  profile profile-name {
    custom-block-message value;
    default (block | log-and-permit | permit);
    fallback-settings {
      default (block | log-and-permit);
      server-connectivity (block | log-and-permit);
      timeout (block | log-and-permit);
      too-many-requests (block | log-and-permit);
    }
    timeout value;
  }
}
```

**Hierarchy Level** [set security utm feature-profile web-filtering]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure the UTM web-filtering local feature.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## kaspersky-lab-engine

**Syntax**

```
kaspersky-lab-engine {
  pattern-update {
    email-notify {
      admin-email email-address;
      custom-message message;
      custom-message-subject message-subject;
    }
    interval value;
    no-autoupdate;
    proxy {
      password password-string;
      port port-number;
      server address-or-url;
      username name;
    }
    url url;
  }
  profile profile-name {
    fallback-options {
      content-size (block | log-and-permit);
      corrupt-file (block | log-and-permit);
      decompress-layer (block | log-and-permit);
      default (block | log-and-permit);
      engine-not-ready (block | log-and-permit);
      out-of-resources (block | (log-and-permit);
      password-file (block | (log-and-permit);
      timeout (block | log-and-permit);
      too-many-requests (block | log-and-permit);
    }
    notification-options {
      fallback-block {
        administrator-email email-address;
        allow-email;
        custom-message message;
        custom-message-subject message-subject;
        display-host;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
      fallback-non-block {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-recipient | no-notify-mail-recipient);
      }
      virus-detection {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
    }
    scan-options {
```

Copyright © 2013, Juniper Networks, Inc.

```
        content-size-limit value;
        decompress-layer-limit value;
        (intelligent-prescreening | no-intelligent-prescreening);
        scan-extension filename;
        scan-mode (all | by-extension);
        timeout value;
      }
      trickling {
        timeout value;
      }
    }
}
```

**Hierarchy Level** [edit security utm feature-profile anti-virus]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure the UTM full file-based antivirus feature.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## key-generation-self-test

**Syntax** key-generation-self-test;

**Hierarchy Level** [edit security alarms potential-violation]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Raise a security alarm when the device or switch detects a key generation self-test failure. Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt data. The self-tests run without operator intervention.

**Default** No alarm is raised upon failure of a key generation self-test.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## key-protection (Security)

**Syntax** key-protection;

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Enabling key protection provides improved security. When key protection is enabled, persistent keys are encrypted when not in use.

Enabling or disabling of this option requires rebooting the device.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## key-protection (Security IDP Sensor Configuration)

**Syntax** key-protection;

**Hierarchy Level** [edit security idp sensor-configuration ssl-inspection]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Enable secure key handling. This option is off by default.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## land

**Syntax** land;

**Hierarchy Level** [edit security screen ids-option *screen-name* tcp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable prevention of Land attacks by combining the SYN flood defense with IP spoofing protection. Land attacks occur when an attacker sends spoofed IP packets with headers containing the target's IP address for the source and destination IP addresses. The attacker sends these packets with the SYN flag set to any available port. The packets induce the target to create empty sessions with itself, filling its session table and overwhelming its resources.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Configuration Statement Hierarchy

## large

**Syntax** large;

**Hierarchy Level** [edit security screen ids-option *screen-name* icmp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure the device to detect and drop any ICMP frame with an IP length greater than 1024 bytes.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Reconnaissance Deterrence for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## lifetime-kilobytes

**Syntax** lifetime-kilobytes *kilobytes*;

**Hierarchy Level** [edit security ipsec proposal *proposal-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the lifetime (in kilobytes) of an IPsec security association (SA).

**Options** ***kilobytes*** —Lifetime of the IPsec security association (SA).
**Range:** 64 through 1048576 kilobytes

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IPsec VPNs for Security Devices

## lifetime-seconds (Security Group VPN)

**Syntax** lifetime-seconds *seconds*;

**Hierarchy Level** [edit security group-vpn member ike proposal *proposal-name*]
[edit security group-vpn server ipsec proposal *proposal-name*]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Specify the lifetime (in seconds) of an IKE or IPsec security association (SA) for group VPN. When the SA expires, it is replaced by a new SA and security parameter index (SPI) or terminated.

**Options** ***seconds***—Lifetime of the IKE or IPsec SA.
**Range:** 180 through 86,400 seconds
**Default:** 3600 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## lifetime-seconds (Security IKE)

**Syntax** lifetime-seconds *seconds*;

**Hierarchy Level** [edit security ike proposal *proposal-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Default value modified in Release 10.2.

**Description** Specify the lifetime (in seconds) of an IKE security association (SA). When the SA expires, it is replaced by a new SA and security parameter index (SPI) or terminated.

**Options** ***seconds***—Lifetime of the IKE SA.
**Range:** 180 through 86,400 seconds
**Default:** 28,800 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IPsec VPNs for Security Devices

## lifetime-seconds (Security IPsec)

**Syntax** lifetime-seconds ***seconds*** ;

**Hierarchy Level** [edit security ipsec proposal ***proposal-name*** ]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Default value modified in Release 10.2.

**Description** Specify the lifetime (in seconds) of an IPsec security association (SA). When the SA expires, it is replaced by a new SA and security parameter index (SPI) or terminated.

**Options** ***seconds***—Lifetime of the IPsec SA.
**Range:** 180 through 86,400 seconds
**Default:** 3600 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## limit (Security Log)

**Syntax** limit *value*;

**Hierarchy Level** [edit security log cache]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Specify the number of security log entries to be kept in memory.

**Options** Once the maximum value limit is reached, new entries will not be added until the cache size drops.

**Range:** 0 through 4,294,967,295

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- System Log Messages
- Security Logs
- CLI Statements and Commands

Copyright © 2013, Juniper Networks, Inc.

## limit (Security SCTP)

**Syntax**

```
limit {
  rate {
    address ip-address {
      sccp rate-limit;
      ssp rate-limit;
      sst rate-limit;
    }
    sccp rate-limit;
    ssp rate-limit;
    sst rate-limit;
  }
}
```

**Hierarchy Level** [edit security gprs sctp profile *profile-name*]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Set the rate limit for local Services Processing Unit (SPU) packets. Four categories can be set.

- **address *ip-address***—To set Signalling Connection Control Part (SCCP), Subsystem-Prohibited (SSP), and Subsystem Status Test (SST) messages rate limit to an IP address.
- **sccp *rate-limit***—To set the SCCP messages rate limit.
- **ssp *rate-limit***—To set the SSP messages rate limit.
- **sst *rate-limit***—To set the SST messages rate limit.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- General Packet Radio Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## limit (UTM Policy)

**Syntax** limit *value*;

**Hierarchy Level** [edit security utm utm-policy *policy-name* traffic-options sessions-per-client]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle to limit sessions.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM Content Filtering for Security Devices
- Unified Threat Management
- UTM Basics for Security Devices

## limit-session

**Syntax**

```
limit-session {
    destination-ip-based number;
    source-ip-based number;
}
```

**Hierarchy Level** [edit security screen ids-option *screen-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Limit the number of concurrent sessions the device can initiate from a single source IP address or the number of sessions it can direct to a single destination IP address.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Configuration Statement Hierarchy

Copyright © 2013, Juniper Networks, Inc.

## list (Security Antivirus Mime Whitelist)

**Syntax**

```
list listname {
    exception listname;
}
```

**Hierarchy Level** [edit security utm feature-profile anti-virus mime-whitelist]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure the antivirus scanner to use MIME bypass lists (custom objects). If you want to have exceptions to the whitelist, create a mime-pattern list with the **exception** statement in addition to the **list** statement.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## list (Security Content Filtering Block Mime)

**Syntax**

```
list list-name;
```

**Hierarchy Level** [edit security utm feature-profile content-filtering profile *profile-name* block-mime]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure the content filter to use MIME block lists (custom objects).

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM Content Filtering for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## load-distribution

**Syntax**

```
load distribution {
  session-affinity ipsec;
}
```

**Hierarchy Level** [edit security flow]

**Release Information** Statement introduced in Junos OS Release 11.4R5.

**Description** Enable load distribution for a data flow.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IPsec VPNs for Security Devices

## local (Certificates)

**Syntax**

```
local name {
  certificate;
  load-key-file url;
}
```

**Hierarchy Level** [edit security certificates]

**Release Information** Statement introduced before Release 12.1 of Junos OS.

**Description** Configure local X.509 certificate.

**Options**
- *name*—Name of this local configuration.
- *certificate*—Certificate and private key string.
- **load-key-file** ***url***—File that contains a certificate and private key in Privacy-Enhanced Mail (PEM) format.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## local (Security IPsec)

**Syntax** local *ip-prefix*;

**Hierarchy Level** [edit security ipsec vpn *vpn-name* ike proxy-identity]

**Release Information** Statement modified in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS.

**Description** Specify the local IPv4 or IPv6 address and subnet mask for the proxy identity.

**Options** ***ip-prefix*** —IPv4 or IPv6 address and subnet mask.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IPsec VPNs for Security Devices

## local-address (Security Group VPN)

**Syntax** local–address *ip-address*;

**Hierarchy Level** [edit security group-vpn member ike gateway *gateway-name*]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the IP address the member uses when accessing the group server.

**Options** *ip-address*—IPv4 address.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## local-authentication-table

**Syntax** local-authentication-table (disable | priority *priority*);

**Hierarchy Level** [edit security user-identification authentication-source]

**Release Information** Statement introduced in Release 12.1 of Junos OS.

**Description** An authentication table created on the SRX Series device using the **request security user-identification local-authentication-table add** command.

**Options**

- **disable**—Disable the local authentication table. Remove the keyword to re-enable the table.
- **priority *priority***—A unique value between 1 and 65535 that determines the sequence for searching multiple tables to retrieve a user role. Each table is given a unique priority value. The lower the value, the higher the priority. A table with priority 120 is searched before a table with priority 200. The default priority value of the local-authentication-table is 100.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Understanding User Role Firewalls
- Understanding the User Identification Table
- *Unified Access Control Solution Guide for SRX Series Services Gateways*

Copyright © 2013, Juniper Networks, Inc.

## local-certificate (Security)

**Syntax** local-certificate *certificate-id*;

**Hierarchy Level** [edit security group-vpn member ike policy *policy-name* certificate]
[edit security group-vpn server ike policy *policy-name* certificate]
[edit security ike policy *policy-name* certificate]

**Release Information** Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

**Description** Specify a particular certificate when the local device has multiple loaded certificates. (This statement is not supported on dynamic VPN implementations.)



NOTE: The device deletes existing IKE and IPsec SAs when you update the **local-certificate** configuration in the IKE policy.

**Options** ***certificate-id*** —Name of the specific certificate to be used.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## local-identity

**Syntax**

```
local-identity {
  (distinguished-name | hostname hostname | inet ip-address | inet6 ipv6-address |
    user-at-hostname e-mail-address);
}
```

**Hierarchy Level**

[edit security group-vpn member ike gateway *gateway-name*]
[edit security group-vpn server ike gateway *gateway-name*]
[edit security ike gateway *gateway-name*]

**Release Information**

Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS. The **inet6** option added in Release 11.1 of Junos OS. The **inet6** option is not supported on the **group-vpn** hierarchies.

**Description**

Specify the local IKE identity to send in the exchange with the destination peer to establish communication. If you do not configure a local-identity, the device uses the IPv4 or IPv6 address corresponding to the local endpoint by default. (The **distinguished-name** option is not supported on dynamic VPN implementations.)



NOTE: For Network Address Translation Traversal (NAT-T), both local identity and remote identity must be configured.

**Options**

- **distinguished-name**—Specify identity as the distinguished name (DN) from the certificate. If there is more than one certificate on the device, use the **security ike gateway** *gateway-name* **policy** *policy-name* **certificate local-certificate** *certificate-id*statement to specify a certificate.
- **hostname** *hostname*—Specify identity as a fully qualified domain name (FQDN).
- **inet** *ip-address*—Specify identity as an IPv4 address.
- **inet6** *ipv6-address*—Specify identity as an IPv6 address.
- **user-at-hostname** *e-mail-address*—Specify identity as an e-mail address.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## log (Security)

**Syntax**

```
log {
  cache {
    exclude exclude-name {
      destination-address destination-address;
      destination-port destination-port;
      event-id event-id;
      failure;
      interface-name interface-name;
      policy-name policy-name;
      process process-name;
      protocol protocol;
      source-address source-address;
      source-port source-port;
      success;
      user-name user-name;
    }
    limit value;
  }
  disable;
  event-rate rate;
  file {
    files max-file-number;
    name file-name;
    path binary-log-file-path;
    size maximum-file-size;
  }
  format (binary | sd-syslog | syslog);
  mode (event | stream);
  rate-cap rate-cap-value;
  source-address source-address;
  stream stream-name {
    category (all | content-security);
    format (binary | sd-syslog | syslog | welf);
    host {
      ip-address;
      port port-number;
    }
    severity (alert | critical | debug | emergency | error | info | notice | warning);
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
  utc-time-stamp;
}
```


Copyright © 2013, Juniper Networks, Inc.

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Release 9.2 of Junos OS

**Description** You can set the mode of logging (event for traditional system logging or stream for streaming security logs through a revenue port to a server). You can also specify all the other parameters for security logging.

**Options**

- **disable**—Disable the security logging for the device.
- **event-rate** ***rate***—Limits the rate (0 through 1500) at which logs will be streamed per second.
- **rate-cap** ***rate-cap-value***—Limits the rate (0 through 5000) at which data plane logs will be generated per second.
- **source-address** ***source-address***—Specify a source IP address or IP address used when exporting security logs.
- **utc-time-stamp**— Specify to use UTC time for security log timestamps.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Log File Formats
- Application Tracking
- Master Administrator for Logical Systems on Security Devices

Copyright © 2013, Juniper Networks, Inc.

## log (Security GTP)

**Syntax**

```
log {
  forwarded (basic | detail);
  prohibited (basic | detail);
  rate-limited {
    (basic | detail);
    frequency-number number;
  }
  state-invalid (basic | detail);
}
```

**Hierarchy Level** [edit security gprs gtp profile *profile-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS. Support for GTPv2 added in Release 11.4 of Junos OS.

**Description** Configure GTP logs to be viewed from the console or syslog.



NOTE: By default, all logs are disabled on the device.

**Options**

- **forwarded**—A packet that the security device transmitted because it was valid.
- **prohibited**—A packet that the security device dropped because it was invalid.
- **rate-limited**—A packet that the security device dropped because it exceeded the maximum rate limit of the destination GSN.
  - **frequency-number *number***—Logging frequency over threshold set by rate-limit (2–500).
- **state-invalid**—A packet that the security device dropped because it failed stateful inspection.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- General Packet Radio Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## log (Security IDP)

**Syntax**

```
log {
  cache-size size;
  suppression {
    disable;
    (include-destination-address | no-include-destination-address);
    max-logs-operate value;
    max-time-report value;
    start-log value;
  }
}
```

**Hierarchy Level** [edit security idp sensor-configuration]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Configure IDP security policy logs.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## log (Security IDP Policy)

**Syntax**

```
log;
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* then ip-action]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then ip-action]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Release 10.0 of Junos OS.

**Description** Log the information about the IP action against the traffic that matches a rule.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- Application-Level Distributed Denial of Service
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## log (Security Policies)

**Syntax**

```
log {
  session-close;
  session-init;
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Enable traffic to which the policy applies to be logged at the beginning or end of a session.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## log (Security SCTP)

**Syntax**

```
log {
  configuration;
  decoding-error;
  dropped-packet;
  exceeding-rate-limit;
}
```

**Hierarchy Level** [edit security gprs sctp]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure Stream Control Transmission Protocol (SCTP) logs to be viewed from the console or system log. Four categories of SCTP packet logging can be set.

- **configuration**—To log the CLI configuration.
- **decoding-error**—To log the decoding errors.
- **dropped-packet**—To log the dropped packets and out of resource errors.
- **exceeding-rate-limit**—To log the exceeding rate limit.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- General Packet Radio Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## log-attacks

**Syntax**

```
log-attacks {
  alert;
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* then notification]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then notification]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Release 10.0 of Junos OS.

**Description** Enable the log attacks to create a log record that appears in the log viewer.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## log-create

**Syntax** log-create;

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* then ip-action]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then ip-action]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Generate a log event on installing the ip-action filter.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## log-errors

**Syntax** (log-errors | no-log-errors);

**Hierarchy Level** [edit security idp sensor-configuration flow]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Enable the error log to generate the result of success or failure about the flow. A flow-related error is when IDP receives a packet that does not fit into expected flow. By default error log is enabled.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## log-supercede-min

**Syntax** log-supercede-min *minimum-value*;

**Hierarchy Level** [edit security idp sensor-configuration ips]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify the amount of time to supersede the IPS sensor logs.

**Options** *minimum-value*—Minimum time to supersede the log.
**Range:** 0 through 65,535 seconds
**Default:** 1 second

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## low-watermark

**Syntax** low-watermark *percent*;

**Hierarchy Level** [edit security flow aging]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Set the point at which the aggressive aging-out process ends.

**Options** ***percent*** —Percentage of session-table capacity at which aggressive aging-out ends.
**Range:** 0 through 100 percent
**Default:** 100 percent

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Flow-Based Processing for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## management (Security Zones)

**Syntax**

```
management {
  description text;
  host-inbound-traffic {
    protocols protocol-name {
      except;
    }
    system-services service-name {
      except;
    }
  }
  interfaces interface-name  {
    host-inbound-traffic {
      protocols protocol-name {
        except;
      }
      system-services service-name {
        except;
      }
    }
  }
  screen screen-name;
}
```

**Hierarchy Level** [edit security zones functional-zone]

**Release Information** Statement introduced in Junos OS Release 8.5.The **description** option added in Junos OS Release 12.1.

**Description** Specify the host for out-of-band management interfaces. You can set firewall options in this zone to protect the management interface from different types of attacks. Because this zone cannot be specified in policies, traffic entering from this zone can only be traffic originating from the device itself and cannot originate from any other zone.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Zones and Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## manual (Security IPsec)

**Syntax**

```
manual {
  authentication {
    algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
    key (ascii-text key | hexadecimal key );
  }
  encryption {
    algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    key (ascii-text key | hexadecimal key );
  }
  external-interface external-interface-name;
  gateway ip-address;
  protocol (ah | esp);
  spi spi-value ;
}
```

**Hierarchy Level** [edit security ipsec vpn *vpn-name*]

**Release Information** Statement modified in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS.

**Description** Define a manual IPsec security association (SA). (This statement is not supported on dynamic VPN implementations.)

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## mapped-port (Security Static NAT)

**Syntax** mapped-port *lower-port-range* to *upper-port-range*;

**Hierarchy Level** [edit security nat static rule-set *rule-set-name* rule *rule-name* then static-nat prefix]
[edit security nat static rule-set *rule-set-name* rule *rule-name* then static-nat prefix-name]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify a destination port or port range to allow static NAT to map ports.

**Options**
- **lower-port-range**—Specify the lower limit of the port range.
- **upper-port-range**—Specify the upper limit of the port range.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## application-firewall

**Syntax**

```
application-firewall {
  rule-sets rule-set-name {
    default-rule {
      (deny | permit | reject);
    }
    rule rule-name {
      match {
        dynamic-application [system-application];
        dynamic-application-groups [system-application-group];
        ssl-encryption (any | yes | no);
      }
      then {
        (deny | permit | reject);
      }
    }
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Junos OS Release 11.1. Updated with the **ssl-encryption** and **reject** options in Junos OS Release 12.1X44-D10.

**Description** Specify the rule set and rule specifications and trace options to be used for appllication firewall implementations.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Firewall

Copyright © 2013, Juniper Networks, Inc.

## match (Security Destination NAT)

**Syntax**

```
match {
  (destination-address <ip-address> | destination-address-name <address-name>);
  destination-port port-number;
  protocol [protocol-name-or-number];
  source-address [ip-address];
  source-address-name [address-name];
}
```

**Hierarchy Level** [edit security nat destination rule-set *rule-set-name* rule *rule-name*]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify the destination rules to be used as match criteria.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## match (Security IDP Policy)

**Syntax**

```
match {
  attacks {
    custom-attack-groups [attack-group-name];
    custom-attacks [attack-name];
    dynamic-attack-groups [attack-group-name];
    predefined-attack-groups [attack-group-name];
    predefined-attacks [attack-name];
  }
  destination-address ([address-name] | any | any-ipv4 | any-ipv6);
  destination-except [address-name];
  from-zone (zone-name | any );
  source-address ([address-name] | any | any-ipv4 | any-ipv6);
  source-except [address-name];
  to-zone (zone-name | any);
}
```

**Hierarchy Level**

[edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name*]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name*]

**Release Information**

Statement introduced in Release 9.2 of Junos OS.

**Description**

Specify the rules to be used as match criteria.

**Options**

The remaining statements are explained separately.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## match (Security Policies)

**Syntax**

```
match {
  application {
    [application];
    any;
  }
  destination-address {
    [address];
    any;
    any-ipv4;
    any-ipv6;
  }
  source-address {
    [address];
    any;
    any-ipv4;
    any-ipv6;
  }
  source-identity {
    [role-name];
    any;
    authenticated-user;
    unauthenticated-user;
    unknown-user;
  }
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name*]

**Release Information** Statement introduced in Junos OS Release 8.5. Statement updated with **source-identity** option in Junos OS Release 12.1.

**Description** Configure security policy match criteria.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## match (Security Rulebase DDoS)

**Syntax**

```
match {
  application (application-name | any | default);
  application-ddos <application-name>;
  destination-address ([address-name] | any | any-ipv4 | any-ipv6);
  destination-except [address-name];
  from-zone (zone-name | any);
  source-address ([address-name] | any | any-ipv4 | any-ipv6);
  source-except [address-name];
  to-zone (zone-name | any);
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Specify the rules to be used as match criteria for application-level DDoS protection.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## match (Security Source NAT)

**Syntax**

```
match {
  (destination-address <ip-address> | destination-address-name <address-name>);
  destination-port port-number;
  protocol [(protocol-name | protocol-number)];
  source-address [ip-address];
  source-address-name [address-name];
}
```

**Hierarchy Level** [edit security nat source rule-set *rule-set-name* rule *rule-name*]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify the source rules to be used as match criteria.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

## match (Security Static NAT)

**Syntax**

```
match {
  (destination-address ip-address | destination-address-name address-name);
  destination-port lower-port-range to upper-port-range;
}
```

**Hierarchy Level** [edit security nat static rule-set *rule-set-name* rule *rule-name*]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify the static rules to be used as match criteria.

**Options** The remaining statement is explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## max-context-values

**Syntax** max-context-values *number*;

**Hierarchy Level** [edit security idp application-ddos *application-name* context *context-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** (Optional) Configures the top *n* context values that should be monitored, reported, or both, for application-level DDoS protection.

**Options** ***number***—Monitor top *n* context values only.
**Range:** 1 to 10,000

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application-Level Distributed Denial of Service

## max-flow-mem

**Syntax** max-flow-mem *value*;

**Hierarchy Level** [edit security idp sensor-configuration re-assembler]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Define the maximum TCP flow memory which IDP sensor can handle.

**Options** ***value***—Maximum TCP flow memory in kilobytes.
**Range:** 64 through 4,294,967,295 kilobytes
**Default:** 1024 kilobytes

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## max-logs-operate

**Syntax** max-logs-operate *value*;

**Hierarchy Level** [edit security idp sensor-configuration log suppression]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** When log suppression is enabled, IDP must cache log records so that it can identify when multiple occurrences of the same event occur. This setting specifies how many log records are tracked simultaneously by IDP.

**Options** ***value***—Maximum number of log records are tracked by IDP.

**Range:** 256 through 65536 records

**Default:** 16384 records

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## max-message-length

**Syntax** max-message-length *number*;

**Hierarchy Level** [edit security gprs gtp profile *profile-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS. Support for GTPv2 added in Release 11.4 of Junos OS.

**Description** Set the maximum message payload length (in bytes) the security device accepts for a GTP message. The default maximum message length is 65,535 bytes. The message length range is from 1 through 65,535 bytes.

**Options** ***number***—Set the maximum message payload length in bytes.

**Range:** 1 through 65535 bytes.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- General Packet Radio Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## max-packet-mem

**Syntax** max-packet-mem *value*;

**Hierarchy Level** [edit security idp sensor-configuration re-assembler]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Define the maximum TCP packet memory that the IDP sensor can handle.

**Options** *value*—Maximum TCP packet memory.
**Range:** 64 through 4,294,967,295 kilobytes (KB)
**Default:** 262144 KB

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## max-packet-memory

**Syntax** max-packet-memory *value*;

**Hierarchy Level** [edit security idp sensor-configuration application-identification]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify the maximum memory length of a packet in bytes.

**Options** *value*—Maximum memory length in bytes.
**Range:** 0 through 200,000,000 bytes
**Default:** 100,000,000 bytes

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## max-session-number

**Syntax** max-session-number *number*;

**Hierarchy Level** [edit security nat source rule-set *ruleset* rule *rule* then source-nat interface persistent-nat]
[edit security nat source rule-set *ruleset* rule *rule* then source-nat pool persistent-nat]

**Release Information** Statement introduced in Junos OS Release 9.6.

**Description** The maximum number of the sessions with which a persistent NAT binding can be associated. For example, if the **max-session-number** of the persistent NAT rule is 65,536, then a 65,537th session cannot be established if that session uses the persistent NAT binding created from the persistent NAT rule.

**Options** *number*—Maximum number of sessions.

**Range:** 8 through 65,536

**Default:** 30 sessions

**Required Privilege Level** **security**—To view this statement in the configuration.
**security-control**—To add this statement to the configuration

**Related Documentation**
- Network Address Translation for Security Devices

## max-sessions (Security Packet Log)

**Syntax** max-sessions *percentage*;

**Hierarchy Level** [edit security idp sensor-configuration packet-log]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the maximum number of sessions actively conducting pre-attack packet captures on a device at one time. This value is expressed as a percentage of the maximum number of IDP sessions for the device.

**Options** ***percentage***—Maximum number of packet capture sessions expressed as a percentage of the IDP session capacity for the device.

**Range:** 1 to 100 percent

**Default:** 10

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## max-tcp-session-packet-memory

**Syntax** max-tcp-session-packet-memory *value*;

**Hierarchy Level** [edit security idp sensor-configuration application-identification]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify the maximum number of TCP sessions that IDP maintains. If the sensor reaches the maximum, it drops all new TCP sessions.

**Options** ***value***—Maximum number of TCP sessions.
**Range:** 0 through 60000

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## max-time-report

**Syntax** max-time-report *value*;

**Hierarchy Level** [edit security idp sensor-configuration log suppression]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** When log suppression is enabled, IDP maintains a count of multiple occurrences of the same event. After the specified number of seconds has passed, IDP writes a single log entry containing the count of occurrences.

**Options** ***value***—Time after which IDP writes a single log entry containing the count of occurrences.
**Range:** 1 through 60 seconds
**Default:** 5 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## max-timers-poll-ticks

**Syntax** max-timers-poll-ticks *value*;

**Hierarchy Level** [edit security idp sensor-configuration flow]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify the time at which timer ticks at regular interval.

**Options** *value*—Maximum amount of time at which the timer ticks.
**Range:** 0 through 1000 ticks
**Default:** 1000 ticks

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## max-udp-session-packet-memory

**Syntax** max-udp-session-packet-memory *value*;

**Hierarchy Level** [edit security idp sensor-configuration application-identification]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify the maximum number of UDP sessions that IDP maintains. If the sensor reaches the maximum, it drops all new UDP sessions.

**Options** *value*—Maximum number of UDP sessions.
**Range:** 0 through 20000

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## maximize-idp-sessions

**Syntax**

```
maximize-idp-sessions {
  inline-tap;
  weight (equal | firewall | idp);
}
```

**Hierarchy Level** [edit security forwarding-process application-services]

**Release Information** Statement introduced in Release 9.6 of Junos OS.

**Description** If you are deploying IDP policies, you can tune the device to increase IDP session capacity. By using the provided commands to change the way the system allocates resources, you can achieve a higher IDP session capacity. See weight for information about the options provided.



NOTE: The IDP session capacity is restricted to 100000 sessions per SPU.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Processing Overview for Security Devices
- IDP Policies for Security Devices

## maximum-cache-size

**Syntax** maximum-cache-size *number*;

**Hierarchy Level** [edit security idp sensor-configuration ssl-inspection]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Maximum SSL session ID cache size.

**Options** ***maximum-cache-size***—Maximum number of SSL session ID cache size.

**Range:** 1 through 5000000 sessions

**Default:** 5000000

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## maximum-call-duration (Security)

**Syntax** maximum-call-duration *value-in-minutes*;

**Hierarchy Level** [edit security alg mgcp],
[edit security alg sip]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the time at which the SIP call ends. The media session is released after the call has ended.

**Options** ***value-in-minutes***—Maximum amount of time at which the call ends and releases the media sessions.

**Range:** 3 through 7200 minutes

**Default:** 720 minutes

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- MGCP ALGs for Security Devices
- SIP ALGs for Security Devices

## maximum-capture-size (Datapath Debug)

**Syntax** maximum-capture-size *maximum-capture-size*;

**Hierarchy Level** [edit security datapath-debug]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Specifies maximum packet capture length.

**Options**
- **maximum-capture-size** ***maximum-capture-size***—Specify the maximum packet capture length.

  **Range:** 68 through 10,000 bytes

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- System Log Messages
- Security Logs
- CLI Statements and Commands


Copyright © 2013, Juniper Networks, Inc.

## maximum-message-length

**Syntax** maximum-message-length *number*;

**Hierarchy Level** [edit security alg dns]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** Specify the maximum DNS message length.

**Options** **number**—Maximum length in bytes of a single DNS message.
**Range:** 512 through 8192 bytes.
**Default:** 512 bytes.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Layer Gateways for Security Devices

## imsi-prefix

**Syntax**
```
imsi-prefix imsi-prefix-digits {
  action {
    drop;
    pass;
    selection (ms|net|vrf);
  }
}
```

**Hierarchy Level** [edit security gprs gtp profile *profile-name* apn *pattern-string*]

**Release Information** Statement introduced in Release 10.0 of Junos OS. Support for GTPv2 added in Release 11.4 of Junos OS. Option mcc-mnc replaced with imsi-prefix in Junos OS Release 12.1X44-D10.

**Description** Specify an International Mobile Station Identity (IMSI) prefix for filtering GTP packets.

You can also filter GTP packets based on the combination of an IMSI prefix and an access point name (APN).

**Options** *imsi-prefix-digits*—Specify an IMSI prefix.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- General Packet Radio Service for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## media-source-port-any

**Syntax** media-source-port-any;

**Hierarchy Level** [edit security alg h323]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Allow media traffic from any port number. By default, this feature is disabled, which allows a temporary opening in the firewall (pinhole) for media traffic to be opened.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- H.323 ALGs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## member (Security Group VPN)

**Syntax**

```
member {
  ike {
    gateway gateway-name {
      address [ip-address-or-hostname];
      ike-policy policy-name;
      local-address ip-address;
      local-identity {
        (distinguished-name | hostname hostname | inet ip-address | user-at-hostname
          e-mail-address);
      }
    }
    policy policy-name {
      certificate {
        local-certificate certificate-id;
        peer-certificate-type [pkcs7 | x509-signature);
      }
      description description;
      mode (aggressive | main);
      pre-shared-key (ascii-text key | hexadecimal key);
      proposal-set (basic | compatible | standard);
      proposals [proposal-name];
    }
    proposal proposal-name {
      authentication-algorithm (md5 | sha-256 | sha1);
      authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
      description description;
      dh-group (group1 | group14 | group2 | group5);
      encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
      lifetime-seconds seconds;
    }
  }
  ipsec {
    vpn vpn-name {
      group id;
      group-vpn-external-interface interface;
      heartbeat-threshold number;
      ike-gateway gateway-name;
    }
  }
}
```

**Hierarchy Level** [edit security group-vpn]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure group VPN member.

**Options** Configure group VPN member. You configure the following on the group member:

- Phase 1 IKE SA with the group server. The IKE gateway is the group server.

Copyright © 2013, Juniper Networks, Inc.

NOTE: We recommend that you do not change the default value for lifetime-seconds for the IKE proposal on the member. Increasing the value might cause the member device to continue to use the existing Phase 1 IKE SA key even in the event of a crash; this can delay the recovery process.

- IPsec group VPN.

NOTE: A scope policy must also be configured on the group member. To configure a scope policy, use the policies configuration statement at the [edit security] hierarchy and specify the IPsec group VPN for the ipsec-group-vpn option.

The remaining statements are explained separately.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPNs for Security Devices

## member (Security IDP)

**Syntax**

```
member member-name {
  attack-type {
    (anomaly ...same statements as in [edit security idp custom-attack attack-name
      attack-type anomaly] hierarchy level | signature ...same statements as in [edit security
      idp custom-attack attack-name attack-type signature] hierarchy level);
  }
}
```

**Hierarchy Level**
[edit security idp custom-attack *attack-name* attack-type chain]

**Release Information**
Statement introduced in Release 9.3 of Junos OS.

**Description**
Create the list of member attacks.

**Options**
*member-name*—Name of the member list.

The remaining statements are explained separately.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## message-flood (Security H323)

**Syntax**

```
message-flood {
  gatekeeper {
    threshold rate;
  }
}
```

**Hierarchy Level** [edit security alg h323 application-screen]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Limit the rate per second at which remote access server (RAS) requests to the gatekeeper are processed. Messages exceeding the threshold are dropped. This feature is disabled by default.

**Options**

**gatekeeper threshold *rate***—Maximum number of RAS connection requests per second allowed per gateway.

**Range:** 1 through 65,535

**Default:** 1000

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- H.323 ALGs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## message-flood (Security MGCP)

**Syntax**

```
message-flood {
    threshold rate;
}
```

**Hierarchy Level** [edit security alg mgcp application-screen]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Limits the rate per second at which message requests to the Media Gateway are processed. Messages exceeding the threshold are dropped by the Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG). This feature is disabled by default.

**Options**

**threshold *rate*** —Number of connection requests per second allowed per Media Gateway.

**Range:** 2 through 50000

**Default:** 1000

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- MGCP ALGs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## mgcp

**Syntax**

```
mgcp {
  application-screen {
    connection-flood {
      threshold rate;
    }
    message-flood {
      threshold rate;
    }
    unknown-message {
      permit-nat-applied;
      permit-routed;
    }
  }
  disable;
  dscp-rewrite {
    code-point string;
  }
  inactive-media-timeout value-in-seconds;
  maximum-call-duration value-in-minutes;
  traceoptions {
    flag flag <extensive>;
  }
  transaction-timeout value-in-seconds;
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Specify the Media Gateway Control Protocol (MGCP) ALG on the device. MGCP is a text-based Application Layer protocol that can be used for call setup and call control.

**Options** **disable**—Disable the MGCP ALG. By default, the MGCP ALG is enabled.

NOTE: By default, the MGCP ALG is disabled for SRX Series devices.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- MGCP ALGs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## mime-pattern

**Syntax**

```
mime-pattern object-name {
  value [value];
}
```

**Hierarchy Level** [edit security utm custom-objects]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** The gateway device uses MIME (Multipurpose Internet Mail Extension) types to decide which traffic may bypass various types of scanning.

**Options**

- ***object-name***—Name of the MIME object.
- **value *value***—Value of the MIME object. You can configure multiple values separated by spaces and enclosed in square brackets.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Content Filtering for Security Devices
- Unified Threat Management


Copyright © 2013, Juniper Networks, Inc.

## mime-whitelist

**Syntax**

```
mime-whitelist {
  exception listname;
  list listname {
    exception listname;
  }
}
```

**Hierarchy Level** [edit security utm feature-profile anti-virus]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Statement updated in 11.1 for Sophos antivirus support.

**Description** Configure the antivirus scanner to use MIME bypass lists and exception lists. You can use your own custom object lists, or you can use the default list that ships with the device called junos-default-bypass-mime.



WARNING: When you configure the MIME whitelist feature, be aware that, because header information in HTTP traffic can be spoofed, you cannot always trust HTTP headers to be legitimate. When a Web browser is determining the appropriate action for a given file type, it detects the file type without checking the MIME header contents. However, the MIME whitelist feature does refer to the MIME encoding in the HTTP header. For these reasons, it is possible in certain cases for a malicious website to provide an invalid HTTP header. For example, a network administrator might inadvertently add a malicious website to a MIME whitelist, and, because the site is in the whitelist, it will not be blocked by Sophos even though Sophos has identified the site as malicious in its database. Internal hosts would then be able to reach this site and could become infected.

**Options** The remaining statements are explained separately.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- Unified Threat Management

Copyright © 2013, Juniper Networks, Inc.

## min-message-length

**Syntax** min-message-length *number*;

**Hierarchy Level** [edit security gprs gtp profile *profile-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS. Support for GTPv2 added in Release 11.4 of Junos OS.

**Description** Set the minimum message payload length (in bytes) the security device accepts for a GTP message. The default minimum message length is 0 bytes. The message length range is from 0 through 65,535 bytes.

**Options** *number*—Set the minimum message payload length in bytes.

**Range:** 0 through 65535 bytes.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- General Packet Radio Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## mode (Security Forwarding Options)

**Syntax** mode (drop | flow-based | packet-based);

**Hierarchy Level** [edit security forwarding-options family inet6]

**Release Information** Support on SRX Series and J Series devices for flow-based mode for family inet6 added in Release 10.2 of Junos OS.

**Description** Specify forwarding options for IPv6 traffic.

**Options**

- **drop**—Drop IPv6 packets. This is the default setting.
- **flow-based**—Perform flow-based packet forwarding.
- **packet-based**—Perform simple packet forwarding.



NOTE: **Packet-based processing is not supported on the following SRX Series devices: SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800.**

If you change the forwarding option mode for IPv6, you might have to perform a reboot to initialize the configuration change. Table 5 on page 761 summarizes device status upon configuration change.

### Table 5: Device Status Upon Configuration Change

| Configuration Change | Commit Warning | Reboot Required | Impact on Existing Traffic Before Reboot | Impact on New Traffic Before Reboot |
|---|---|---|---|---|
| Drop to flow-based | Yes | Yes | Dropped | Dropped |
| Drop to packet-based | No | No | Packet-based | Packet-based |
| Flow-based to packet-based | Yes | Yes | None | Flow sessions created |
| Flow-based to drop | Yes | Yes | None | Flow sessions created |
| Packet-based to flow-based | Yes | Yes | Packet-based | Packet-based |
| Packet-based to drop | No | No | Dropped | Dropped |

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

Copyright © 2013, Juniper Networks, Inc.

## mode (Security IKE Policy)

**Syntax** mode (aggressive | main);

**Hierarchy Level** [edit security group-vpn member ike policy *policy-name*]
[edit security group-vpn server ike policy *policy-name*]
[edit security ike policy *policy-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

**Description** Define the mode used for Internet Key Exchange (IKE) Phase 1 negotiations. Use aggressive mode only when you need to initiate an IKE key exchange without ID protection, as when a peer unit has a dynamically assigned IP address. (The **main** option is not supported on dynamic VPN implementations.)



NOTE:

- IKEv2 protocol does not negotiate using mode configuration.
- The device deletes existing IKE and IPsec SAs when you update the mode configuration in the IKE policy.

**Options**

- **aggressive**—Aggressive mode.
- **main**—Main mode. Main mode is the recommended key-exchange method because it conceals the identities of the parties during the key exchange.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## mode (Security Log)

**Syntax** mode (event | stream)

**Hierarchy Level** [edit security log]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Set the mode of logging (event for traditional system logging or stream for streaming security logs through a revenue port to a server).

**Options**

- **event**— Process security logs in the control plane.
- **stream**—Process security logs directly in the forwarding plane.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- System Log Messages
- Security Logs
- CLI Statements and Commands

Copyright © 2013, Juniper Networks, Inc.

## mpls (Security Forwarding Options)

**Syntax**

```
mpls {
  mode packet-based;
}
```

**Hierarchy Level** [edit security forwarding-options family]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Enable the forwarding of MPLS traffic. By default, the device drops MPLS traffic.



CAUTION: Because MPLS operates in packet mode, security services are not available.



NOTE: Packet-based processing is not supported on the following SRX Series devices: SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- MPLS for Security Devices
- Device and Routing Operations Monitoring
- Troubleshooting for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## msrpc

**Syntax**

```
msrpc {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Specify the Microsoft (MS) remote procedure call (RPC) ALG on the device.

**Options**

- **disable**—Disable the Microsoft RPC ALG. By default, the Microsoft RPC ALG is enabled.
- **traceoptions**—Configure Microsoft RPC ALG tracing options.
  - **flag**—Trace operation to perform.
    - **all**—Trace all events.
    - ***extensive***—Display extensive amount of data.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- RPC ALGs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## mss (Security IDP)

**Syntax**

```
mss {
  match (equal | greater-than | less-than | not-equal);
  value maximum-segment-size;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the maximum segment size (MSS) in the TCP header.

**Options**

- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***maximum-segment-size***—Match the maximum segment size value.

  **Range:** 0 through 65,535

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## nat

**Syntax**

```
nat {
    destination {
        pool pool-name {
            address ip-address {
                (port port-number | to ip-address);
            }
            description text;
            routing-instance routing-instance-name;
        }
        rule-set rule-set-name {
            description text;
            from {
                interface [interface-name];
                routing-instance [routing-instance-name];
                zone [zone-name];
            }
            rule rule-name {
                description text;
                match {
                    (destination-address <ip-address> | destination-address-name <address-name>);
                    destination-port port-number;
                    protocol [protocol-name-or-number];
                    source-address [ip-address];
                    source-address-name [address-name];
                }
                then {
                    destination-nat (off | pool pool-name);
                }
            }
        }
    }
    proxy-arp {
        interface interface-name {
            address ip-address {
                to ip-address;
            }
        }
    }
    proxy-ndp {
        interface interface-name {
            address ip-address {
                to ip-address;
            }
        }
    }
    source {
        address-persistent;
        interface {
            port-overloading {
                off;
            }
        }
```

```
pool pool-name {
  address ip-address {
    to ip-address;
  }
  description text;
  host-address-base ip-address;
  overflow-pool (interface | pool-name);
  port {
    (no-translation | port-overloading-factor number | range port-low <to port-high>);
  }
  routing-instance routing-instance-name;
}
pool-default-port-range lower-port-range to upper-port-range;
pool-utilization-alarm {
  clear-threshold value;
  raise-threshold value;
}
port-randomization {
  disable;
}
rule-set rule-set-name {
  description text;
  from {
    interface [interface-name];
    routing-instance [routing-instance-name];
    zone [zone-name];
  }
  rule rule-name {
    description text;
    match {
      (destination-address <ip-address> | destination-address-name <address-name>);
      destination-port port-number;
      protocol [protocol-name-or-number];
      source-address [ip-address];
      source-address-name [address-name];
    }
    then {
      source-nat {
        interface {
          persistent-nat {
            address-mapping;
            inactivity-timeout seconds;
            max-session-number value;
            permit (any-remote-host | target-host | target-host-port);
          }
        }
        off;
        pool {
          persistent-nat {
            address-mapping;
            inactivity-timeout seconds;
            max-session-number number;
            permit (any-remote-host | target-host | target-host-port);
          }
          pool-name;
        }
```


Copyright © 2013, Juniper Networks, Inc.

```
            }
          }
        }
        to {
          interface [interface-name];
          routing-instance [routing-instance-name];
          zone [zone-name];
        }
      }
    }
    static {
      rule-set rule-set-name {
        description text;
        from {
          interface [interface-name];
          routing-instance [routing-instance-name];
          zone [zone-name];
        }
        rule rule-name {
          description text;
          match {
            (destination-address ip-address | destination-address-name address-name);
          }
          then {
            static-nat {
              inet {
                routing-instance (default | routing-instance-name);
              }
              prefix {
                address-prefix;
                routing-instance (default | routing-instance-name);
              }
              prefix-name {
                address-prefix-name;
                routing-instance (default | routing-instance-name);
              }
            }
          }
        }
      }
    }
    traceoptions {
      file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
      }
      flag flag;
      no-remote-trace;
    }
  }
```

**Hierarchy Level** [edit security]

Copyright © 2013, Juniper Networks, Inc.

**Release Information** Statement modified in Release 9.6 of Junos OS. The **description** option added in Release 12.1 of Junos OS.

**Description** Configure Network Address Translation (NAT) for SRX Series devices.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Layer Gateways for Security Devices
- Logical Systems for Security Devices
- Device and Routing Operations Monitoring
- Troubleshooting for Security Devices

## nat-keepalive

**Syntax** nat-keepalive *seconds*;

**Hierarchy Level** [edit security ike gateway *gateway-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the interval at which NAT keepalive packets can be sent so that NAT translation continues.

**Options** ***seconds*** —Maximum interval in seconds at which NAT keepalive packets can be sent.
**Range:** 1 through 300 seconds
**Default:** 5 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## negate

**Syntax** negate;

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Select negate to exclude the specified pattern from being matched.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## nested-application (Security IDP)

**Syntax** nested-application *nested-application-name*;

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type chain protocol-binding]
[edit security idp custom-attack *attack-name* attack-type signature protocol-binding]

**Release Information** Statement introduced in Junos OS Release 9.3.

**Description** Specify the nested application name.

**Options** *nested-application-name*—Name of the nested application.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## no-anti-replay (Security)

**Syntax** no-anti-replay;

**Hierarchy Level** [edit security ipsec vpn *vpn-name* ike]
[edit security group-vpn server group *group-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchy added in Release 10.2 of Junos OS.

**Description** Disable the antireplay checking feature of IPsec. By default, antireplay checking is enabled.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

## no-autoupdate

**Syntax** no-autoupdate;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine pattern-update]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]
[edit security utm feature-profile anti-virus sophos-engine pattern-update]

**Release Information** Statement introduced in Release 9.5 of Junos OS for Juniper Express engine and Kaspersky Lab engine. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** Turn off automatic data file (pattern file) update for the Kaspersky Lab, Juniper Express, or Sophos engines.



NOTE: The data files used with Sophos are not a typical virus pattern files, they are small file that helps guide virus scanning logic. The full virus pattern database is stored on an external Sophos server called the Sophos Extensible List (SXL) server.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- Unified Threat Management


Copyright © 2013, Juniper Networks, Inc.

## no-intelligent-prescreening

**Syntax** no-intelligent-prescreening;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* scan-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Disables intelligent prescreening.

Intelligent prescreening tells the antivirus module to begin scanning a file much earlier. In this case, the scan engine uses the first packet or the first several packets to determine if a file could possibly contain malicious code. The scan engine does a quick check on these first packets and if the scan engine finds that it is unlikely that the file is infected, it then determines that it is safe to bypass the normal scanning procedure.

You can enable intelligent prescreening with the **intelligent-prescreening** statement.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## no-nat-traversal

**Syntax** no-nat-traversal;

**Hierarchy Level** [edit security ike gateway *gateway-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Disables UDP encapsulation of IPsec Encapsulating Security Payload (ESP) packets, otherwise known as Network Address Translation Traversal (NAT-T). NAT-T is enabled by default.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## no-notify-mail-recipient

**Syntax** no-notify-mail-recipient;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options fallback-non-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options fallback-non-block]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options fallback-non-block]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** Do not notify the e-mail recipient about errors returned by the antivirus scan engine when a fallback-non-block action occurs.

You can specify that the e-mail recipient is to be notified with the **notify-mail-recipient** statement.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

## no-notify-mail-sender (Security Content Filtering Notification Options)

**Syntax** no-notify-mail-sender;

**Hierarchy Level** [edit security utm feature-profile content-filtering profile *profile-name* notification-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Do not notify the e-mail sender.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM Content Filtering for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## no-notify-mail-sender (Security Fallback Block)

**Syntax** no-notify-mail-sender;

**Hierarchy Level**
[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options fallback-block]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** Do not notify the e-mail sender about errors returned by the antivirus scan engine when a fallback action occurs.

You can specify that the e-mail sender is to be notified with the **notify-mail-sender** statement.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## no-notify-mail-sender (Security Virus Detection)

**Syntax** no-notify-mail-sender;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options virus-detection]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options virus-detection]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** Do not notify the e-mail sender when a virus is detected by the antivirus engine.

You can specify that the e-mail sender is to be notified with the **notify-mail-sender** statement.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

## no-policy-cold-synchronization

**Syntax** no-policy-cold-synchronization

**Hierarchy Level** [edit security idp sensor-configuration high-availability]

**Release Information** Statement introduced in Junos OS Release 11.1.

**Description** Disable policy cold synchronization functionality. This prevents the SRX Series devices from waiting for the IPS policy to be loaded on all service PICs, and there by forfeits IPS service protection during the ISSU (In-service software upgrade) operation/window.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## no-sbl-default-server

**Syntax** no-sbl-default-server;

**Hierarchy Level** [edit security utm feature-profile anti-spam sbl profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Disable the default SBL server lookup.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

## no-sequence-check

**Syntax** no-sequence-check;

**Hierarchy Level** [edit security flow tcp-session]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify that the device does not check sequence numbers in TCP segments during stateful inspection. By default, the device monitors the sequence numbers in TCP segments. The device detects the window scale specified by source and destination hosts in a session and adjusts a window for an acceptable range of sequence numbers according to their specified parameters. The device then monitors the sequence numbers in packets sent between these hosts. If the device detects a sequence number outside this range, it drops the packet.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Flow-Based Processing for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## no-syn-check

**Syntax** no-syn-check;

**Hierarchy Level** [edit security flow tcp-session]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Disable checking of the TCP SYN bit before creating a session. By default, the device checks that the SYN bit is set in the first packet of a session. If the bit is not set, the device drops the packet.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Reconnaissance Deterrence for Security Devices

## no-syn-check-in-tunnel

**Syntax** no-syn-check-in-tunnel;

**Hierarchy Level** [edit security flow tcp-session]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Disable checking of the TCP SYN bit before creating a session for tunneled packets. By default, the device checks that the SYN bit is set in the first packet of a VPN session. If the bit is not set, the device drops the packet.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Reconnaissance Deterrence for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## no-uri-check

**Syntax** no-uri-check;

**Hierarchy Level** [edit security utm feature-profile anti-virus sophos-engine profile *profile-name* scan-options]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Do not perform Sophos antivirus Uniform Resource Identifier (URI) checking. URI checking is performed by analyzing HTTP traffic URI content against a remote Sophos database server to identify malware or malicious content. URI checking is on by default.

You can enable Sophos antivirus URI checking with the **uri-check** statement.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

## non-cryptographic-self-test

**Syntax** non-cryptographic-self-test;

**Hierarchy Level** [edit security alarms potential-violation]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Raise a security alarm when the device or switch detects a noncryptographic self-test failure. The self-tests run without operator intervention.

**Default** No alarm is raised upon failure of a noncryptographic self-test.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## notification

**Syntax**

```
notification {
  log-attacks {
    alert;
  }
  packet-log {
    post-attack number;
    post-attack-timeout seconds;
    pre-attack number;
  }
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Added packet capture support in Release 10.2 of Junos OS.

**Description** Configure the logging options against the action. When attacks are detected, you can choose to log an attack and create log records with attack information and send that information to the log server.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## notification (Security IDP Policy)

**Syntax**

```
notification {
  log-attacks {
  alert;
  }
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* then]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Configures notifications and logging options.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service

Copyright © 2013, Juniper Networks, Inc.

## notification-options (Security Antivirus)

**Syntax**

```
notification-options {
  fallback-block {
    administrator-email email-address;
    allow-email;
    custom-message message;
    custom-message-subject message-subject;
    display-host;
    (notify-mail-sender | no-notify-mail-sender);
    type (message | protocol-only);
  }
  fallback-non-block {
    custom-message message;
    custom-message-subject message-subject;
    (notify-mail-recipient | no-notify-mail-recipient);
  }
  virus-detection {
    custom-message message;
    custom-message-subject message-subject;
    (notify-mail-sender | no-notify-mail-sender);
    type (message | protocol-only);
  }
}
```

**Hierarchy Level**

[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name*]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name*]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name*]

**Release Information**

Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description**

There are multiple notification options you can configure to trigger when a virus is detected.

**Options**

The remaining statements are explained separately.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## notification-options (Security Content Filtering)

**Syntax**

```
notification-options {
  custom-message message;
  (notify-mail-sender | no-notify-mail-sender);
  type (message | protocol-only);
}
```

**Hierarchy Level** [edit security utm feature-profile content-filtering profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** You can configure a message notification to trigger when a content filter is matched.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices

## notify-mail-recipient

**Syntax** notify-mail-recipient;

**Hierarchy Level**
[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options fallback-non-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options fallback-non-block]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options fallback-non-block]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** Notify the e-mail recipient about errors returned by the antivirus scan engine when a fallback-non-block action occurs.

You can specify that the e-mail recipient is not to be notified with the **no-notify-mail-recipient** statement.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## notify-mail-sender (Security Content Filtering Notification Options)

**Syntax** notify-mail-sender;

**Hierarchy Level** [edit security utm feature-profile content-filtering profile *profile-name* notification-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Notify the e-mail sender.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices

## notify-mail-sender (Security Fallback Block)

**Syntax** notify-mail-sender;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options fallback-block]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** E-mail notification is used to notify the sender or the recipient about the errors returned by either the scan engine or the scan manager when a fallback action occurs.

You can specify that the sender is not to be notified with the **no-notify-mail-sender** statement.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## notify-mail-sender (Security Virus Detection)

**Syntax** notify-mail-sender;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options virus-detection]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options virus-detection]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** E-mail notification is used to notify the sender or the recipient about the detected viruses or the scanning errors. When a virus is detected, an e-mail is sent to the sender upon virus detection.

You can specify that the sender is not to be notified with the **no-notify-mail-sender** statement.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

## number

**Syntax** number *ie-number*

**Hierarchy Level** [edit security gprs gtp profile *profile-name* remove-ie version *v1*]

**Release Information** Statement introduced in Release 12.1 of Junos OS.

**Description** Specify the user-configured IE number. IE removal by IE number supports all IEs, ranging from 1 to 255.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- General Packet Radio Service for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## optimized

**Syntax** optimized;

**Hierarchy Level** [edit security ipsec vpn *vpn-name* vpn-monitor]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify that the device uses traffic patterns as evidence of peer liveliness. If enabled, ICMP requests are suppressed. This feature is disabled by default. (This statement is not supported on dynamic VPN implementations.)

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

## option (Security IDP)

**Syntax**
```
option {
  match (equal | greater-than | less-than | not-equal);
  value tcp-option;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the TCP option type (kind field in the TCP header).

**Options** **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

**value** ***tcp-option***—Match the option value.
**Range:** 0 through 255

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## order (Security IDP)

**Syntax** order;

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type chain]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Create a compound attack object that must match each member signature or protocol anomaly in the order you specify. If you do not specify an ordered match, the compound attack object still must match all members, but the attacks or protocol anomalies can appear in random order.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## out-of-resources

**Syntax** out-of-resources (block | (log-and-permit);

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* fallback-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Virus scanning requires a great deal of memory and CPU resources. Due to resource constraints, memory allocation requests can be denied by the system. When out-of-resources occurs, scanning is aborted. The default action is block.

**Options**
- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## out-of-resources (Security Antivirus Sophos Engine)

**Syntax** default (block | log-and-permit | permit);

**Hierarchy Level** [edit security utm feature-profile anti-virus sophos-engine profile *profile-name* fallback-options]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Virus scanning requires a great deal of memory and CPU resources. Due to resource constraints, memory allocation requests can be denied by the system. When out-of-resources occurs, scanning is aborted.

**Options**
- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

## over-limit

**Syntax** over-limit (block | log-and-permit);

**Hierarchy Level** [edit security utm utm-policy *policy-name* traffic-options sessions-per-client]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle to limit sessions and configure an action to occur when the limit is exceeded.

**Options**
- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## overflow-pool

**Syntax** overflow-pool (interface | *pool-name*);

**Hierarchy Level** [edit security nat source pool *pool-name*]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify a source pool to use when the current address pool is exhausted. Currently the statement is applicable for IPv4 addresses only.



NOTE: The length of the IPv6 prefix must be 96 when the pool is used for NAT-PT.

**Options**

- **interface** — Allow the interface pool to support overflow.
- ***pool-name*** — Name of the source address pool.



NOTE: The source pool must have Port Address Translation (PAT) enabled. PAT is not supported when the address is an IPv6 prefix address.

**Required Privilege Level** security — To view this statement in the configuration.
security-control — To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## packet-filter

**Syntax**

```
packet-filter packet-filter-name {
  action-profile (profile-name | default);
  destination-port (port-range | protocol-name);
  destination-prefix destination-prefix;
  interface logical-interface-name;
  protocol (protocol-number | protocol-name;
  source-port (port-range | protocol- name);
  source-prefix source-prefix;
  }
```

**Hierarchy Level** [edit security datapath-debug]

**Release Information** Command introduced in Release 9.6 of Junos OS; Support for IPv6 addresses for the **destination-prefix** and **source-prefix** options added in Release 10.4 of Junos OS. Support for IPv6 filter for the **interface** option added in Release 10.4 of Junos OS

**Description** Sets packet filter for taking the datapath-debug action. A maximum of four filters are supported at the same time.

**Options**

- **action-profile (*profile-name* | default)**— Identify the action profile to use. You can specify the name of the action profile to use or select default action profile.
- **destination-port (*port-range* | *protocol name*)**— Specify a destination port to match TCP/UDP destination port.
- **destination-prefix *destination-prefix***— Specify a destination IPv4/IPv6 address prefix.
- **interface *logical-interface-name***— Specify a logical interface name.
- **protocol (*protocol-number* | *protocol-name***— Match IP protocol type.
- **source-port (*port-range* | *protocol-name***— Match TCP/UDP source port.
- **source-prefix *source-prefix***— Specify a source IP address prefix.

**Required Privilege Level** security—To view this statement in the configuration
security-control—To add this statement to the configuration.

**Related Documentation**

- [edit security flow] Hierarchy Level on page 325


Copyright © 2013, Juniper Networks, Inc.

## packet-log (Security IDP Policy)

**Syntax**

```
packet-log {
    post-attack number;
    post-attack-timeout seconds;
    pre-attack number;
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then notification]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** In response to a rule match, capture the packets received before and after the attack for further offline analysis of attacker behavior. You can configure the number of pre-attack and post-attack packets to be captured for this attack, and limit the duration of post-attack packet capture by specifying a timeout value.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## packet-log (Security IDP Sensor Configuration)

**Syntax**

```
packet-log {
  host ip-address <port number>;
  max-sessions percentage;
  source-address ip-address;
  total-memory percentage;
}
```

**Hierarchy Level** [edit security idp sensor-configuration]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the sensor for packet capture. This configuration defines the amount of memory to be allocated for packet capture and the maximum number of sessions that can generate packet capture data for the device at one time. The configuration also identifies the source address and host address for transmission of the completed packet capture object.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## pair-policy

**Syntax** pair-policy *pair-policy* ;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit tunnel]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Link the policy that you are configuring with another policy that references the same VPN tunnel so that both policies share one proxy ID and one security association (SA). Policy pairing is useful when you want to allow bidirectional traffic over a policy-based VPN that is using source or destination address translation with a dynamic IP address pool or destination address translation with a mapped IP (MIP) or dynamic IP (DIP) address pool.

Without policy pairing, the device derives a different proxy ID from the outbound and inbound policies. Two proxy IDs causes a problem for the remote peer with a single proxy ID for the VPN tunnel.

Pairing two policies solves the proxy ID problem for the remote peer and conserves SA resources. The single proxy ID is derived from the policy you configured last.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## pass-through

**Syntax**

```
pass-through {
  access-profile profile-name;
  client-match user-or-group-name;
  ssl-termination-profile profile-name;
  web-redirect;
  web-redirect-to-https;
}
```

**Hierarchy Level**

[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit firewall-authentication]

**Release Information**

Statement introduced in Junos OS Release 8.5. Support for **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10.

**Description**

Configure pass-through firewall user authentication. The user needs to use an FTP, Telnet, or HTTP client to access the IP address of the protected resource in another zone. Subsequent traffic from the user or host is allowed or denied based on the result of this authentication. Once authenticated, the firewall proxies the connection.

**Options**

- **access-profile** *profile-name* —(Optional) Specify the name of the access profile.
- **client-match** *user-or-group* —(Optional) Specify the name of the users or user groups in a profile who are allowed access by this policy. If you do not specify any users or user groups, any user who is successfully authenticated is allowed access.
- **ssl-termination-profile** *profile-name* —(Optional) Specify the SSL termination profile used for SSL offloading.
- **web-redirect**—(Optional) Enable redirecting an HTTP request to the device and redirecting the client system to a webpage for authentication. Including this statement allows users an easier authentication process because they need to know only the name or IP address of the resource they are trying to access.
- **web-redirect-to-https**—(Optional) Redirect unauthenticated HTTP requests to the internal HTTPS Web server of the device.



NOTE: If **web-redirect-to-https** is set, then you must specify the SSL termination profile used for SSL offloading.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## password (Security Antivirus)

**Syntax** password *password-string*;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine pattern-update proxy]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update proxy]
[edit security utm feature-profile anti-virus sophos-engine pattern-update proxy]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Set the password for the proxy server.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

## password-file

**Syntax** password-file (block | (log-and-permit);

**Hierarchy Level** [edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* fallback-options]

**Description** Password protected file is the error returned by the scan engine when the scanned file is protected by a password. The default action is log-and-permit.

**Options**
- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## pattern (Security IDP)

**Syntax** pattern *signature-pattern*;

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the pattern IDP should match. You construct the attack pattern just as you would when creating a new signature attack object.

**Options** ***signature-pattern***—Specify the signature pattern.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## pattern-update (Security Antivirus)

**Syntax**

```
pattern-update {
  email-notify {
    admin-email email-address;
    custom-message message;
    custom-message-subject message-subject;
  }
  interval value;
  no-autoupdate;
  proxy {
    password password-string;
    port port-number;
    server address-or-url;
    username name;
  }
  url url;
}
```

**Hierarchy Level**

[edit security utm feature-profile anti-virus juniper-express-engine]
[edit security utm feature-profile anti-virus kaspersky-lab-engine]
[edit security utm feature-profile anti-virus sophos-engine]

**Release Information**

Statement introduced in Release 9.5 of Junos OS for Juniper Express engine and Kaspersky Lab engine. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description**

Updates to the pattern file are added as new viruses are discovered. You can configure the security device to regularly update the pattern file automatically, or you can update the file manually.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## peer-certificate-type

**Syntax** peer-certificate-type (pkcs7 | x509-signature);

**Hierarchy Level** [edit security group-vpn member ike policy *policy-name* certificate]
[edit security group-vpn server ike policy *policy-name* certificate]
[edit security ike policy *policy-name* certificate]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

**Description** Specify a preferred type of certificate (PKCS7 or X509). (This statement is not supported on dynamic VPN implementations.)

**Options**
- **pkcs7**—Public-Key Cryptography Standard #7.
- **x509-signature**—X509 is an ITU-T standard for public key infrastructure.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPNs for Security Devices

## pending-sess-queue-length

**Syntax** pending-sess-queue-length (high | moderate | normal);

**Hierarchy Level** [edit security flow]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Configure the maximum queued length per pending session.

**Options**
- **high**— Allow the maximum number of queued sessions.
- **moderate**—Allow more queued sessions than the normal number.
- **normal**—Allow the normal number of queued session.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Flow-Based Processing for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## perfect-forward-secrecy (Security IPsec)

**Syntax** perfect-forward-secrecy keys (group1 | group14 | group2 | group5);

**Hierarchy Level** [edit security ipsec policy *policy-name*]

**Release Information** Statement modified in Release 8.5 of Junos OS. Support for group 14 is added in Release 11.1 of Junos OS.

**Description** Specify Perfect Forward Secrecy (PFS) as the method that the device uses to generate the encryption key. PFS generates each new encryption key independently from the previous key.



NOTE: The device deletes existing IPsec SAs when you update the perfect-forward-secrecy configuration in the IPsec policy.

**Options**

- **group1**—Diffie-Hellman Group 1.
- **group14**—Diffie-Hellman Group 14. (This option is not supported on dynamic VPN implementations.)
- **group2**—Diffie-Hellman Group 2.
- **group5**—Diffie-Hellman Group 5.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## performance

**Syntax**

```
performance {
  values [fast normal slow unknown];
}
```

**Hierarchy Level** [edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify a performance filter to add attack objects based on the performance level that is vulnerable to the attack.

**Options** **values**—Name of the performance filter. You can select from the following performance level:

- **fast**—Fast track performance level.
- **normal**—Normal track performance level.
- **slow**—Slow track performance level.
- **unknown**—By default, all compound attack objects are set to Unknown. As you fine-tune IDP to your network traffic, you can change this setting to help you track performance level.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## permit (Security Persistent NAT)

**Syntax** permit ( any-remote-host | target-host | target-host-port );

**Hierarchy Level** [edit security nat source rule-set *ruleset* rule *rule* then source-nat interface persistent-nat]
[edit security nat source rule-set *ruleset* rule *rule* then source-nat pool persistent-nat]

**Release Information** Statement introduced in Junos OS Release 9.6. Support for IPv6 addresses added in Junos OS Release 11.2.

**Description** Configure persistent NAT mappings.

**Options**

- **any-remote-host**—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. (The reflexive transport address is the public IP address and port created by the NAT device closest to the STUN server.) Any external host can send a packet to the internal host by sending the packet to the reflexive transport address.
- **target-host**—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. An external host can send a packet to an internal host by sending the packet to the reflexive transport address. The internal host must have previously sent a packet to the external host's IP address.
- **target-host-port**—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. An external host can send a packet to an internal host by sending the packet to the reflexive transport address. The internal host must have previously sent a packet to the external host's IP address and port.



NOTE: **The target-host-port configuration is not supported for NAT64 when configured with IPv6 address.**

**Required Privilege Level** **security**—To view this statement in the configuration.
**security-control**—To add this statement to the configuration

**Related Documentation**

- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## permit (Security Policies)

**Syntax**

```
permit {
  application-services {
    application-firewall {
      rule-set rule-set-name;
    }
    application-traffic-control {
      rule-set rule-set-name;
    }
    gprs-gtp-profile profile-name;
    gprs-sctp-profile profile-name;
    idp;
    redirect-wx | reverse-redirect-wx;
    ssl-proxy {
      profile-name profile-name;
    }
    uac-policy {
      captive-portal captive-portal;
    }
    utm-policy policy-name;
  }
  destination-address {
    drop-translated;
    drop-untranslated;
  }
  firewall-authentication {
    pass-through {
      access-profile profile-name;
      client-match user-or-group-name;
      ssl-termination-profile profile-name;
      web-redirect;
      web-redirect-to-https;
    }
    web-authentication {
      client-match user-or-group-name;
    }
  }
  services-offload;
  tcp-options {
    sequence-check-required;
    syn-check-required;
  }
  tunnel {
    ipsec-group-vpn group-vpn;
    ipsec-vpn vpn-name;
    pair-policy pair-policy;
  }
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then]

**Release Information** Statement introduced in Junos OS Release 8.5. Support for the **tcp-options** added in Junos OS Release 10.4. Support for the **services-offload** option added in Junos OS Release


Copyright © 2013, Juniper Networks, Inc.

11.4. Support for the **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10.

**Description** Specify the policy action to perform when packets match the defined criteria.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## permit-command

**Syntax** permit-command *protocol-command-list*;

**Hierarchy Level** [edit security utm feature-profile content-filtering profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Apply protocol permit command custom-objects to the content-filtering profile

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## persistent-nat

**Syntax**

```
persistent-nat {
  address-mapping;
  inactivity-timeout seconds;
  max-session-number value;
  permit (any-remote-host | target-host | target-host-port);
}
```

**Hierarchy Level**

[edit security nat source rule-set *ruleset* rule *rule* then source-nat interface]
[edit security nat source rule-set *ruleset* rule *rule* then source-nat pool]

**Release Information**

Statement introduced in Junos OS Release 9.6. Support for address-mapping added in Junos OS Release 10.2.

**Description**

Configure persistent NAT.

**Options**

The remaining statements are explained separately.

**Required Privilege Level**

**security**—To view this statement in the configuration.
**security-control**—To add this statement to the configuration

**Related Documentation**

- Network Address Translation for Security Devices

## ping-death

**Syntax**

```
ping-death;
```

**Hierarchy Level**

[edit security screen ids-option *screen-name* icmp]

**Release Information**

Statement introduced in Release 8.5 of Junos OS.

**Description**

Configure the device to detect and reject oversized and irregular ICMP packets. Although the TCP/IP specification requires a specific packet size, many ping implementations allow larger packet sizes. Larger packets can trigger a range of adverse system reactions, including crashing, freezing, and restarting.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Configuration Statement Hierarchy


Copyright © 2013, Juniper Networks, Inc.

## pki

**Syntax**

```
pki {
  auto-re-enrollment {
    certificate-id certificate-id-name {
      ca-profile-name ca-profile-name ;
      challenge-password password ;
      re-enroll-trigger-time-percentage percentage ;
      re-generate-keypair;
    }
  }
  ca-profile ca-profile-name {
    administrator {
      e-mail-address e-mail-address;
    }
    ca-identity ca-identity;
    enrollment {
        retry number;
        retry-interval seconds;
        url url-name;
    }
    revocation-check {
      crl {
        disable {
          on-download-failure;
        }
        refresh-interval hours;
        url url-name;
      }
      disable;
    }
    routing-instance routing-instance-name;
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Configure an IPsec profile to request digital certificates.

**Options** The remaining statements are explained separately.

Copyright © 2013, Juniper Networks, Inc.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Certificates and Public Key Cryptography for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## policies

**Syntax**

```
policies {
  default-policy (deny-all | permit-all);
  from-zone zone-name to-zone zone-name {
    policy policy-name {
      description description;
      match {
        application {
          [application];
          any;
        }
        destination-address {
          [address];
          any;
          any-ipv4;
          any-ipv6;
        }
        source-address {
          [address];
          any;
          any-ipv4;
          any-ipv6;
        }
        source-identity {
          [role-name];
          any;
          authenticated-user;
          unauthenticated-user;
          unknown-user;
        }
      }
      scheduler-name scheduler-name;
      then {
        count {
          alarm {
            per-minute-threshold number;
            per-second-threshold number;
          }
        }
        deny;
        log {
          session-close;
          session-init;
        }
        permit {
          application-services {
            application-firewall {
              rule-set rule-set-name;
            }
            application-traffic-control {
              rule-set rule-set-name;
            }
            gprs-gtp-profile profile-name;
```

Copyright © 2013, Juniper Networks, Inc.

```
            gprs-sctp-profile profile-name;
            idp;
            redirect-wx | reverse-redirect-wx;
            ssl-proxy {
              profile-name profile-name;
            }
            uac-policy {
              captive-portal captive-portal;
            }
            utm-policy policy-name;
          }
          destination-address {
            drop-translated;
            drop-untranslated;
          }
          firewall-authentication {
            pass-through {
              access-profile profile-name;
              client-match user-or-group-name;
              ssl-termination-profile profile-name;
              web-redirect;
              web-redirect-to-https;
            }
            web-authentication {
              client-match user-or-group-name;
            }
          }
          services-offload;
          tcp-options {
            sequence-check-required;
            syn-check-required;
          }
          tunnel {
            ipsec-group-vpn group-vpn;
            ipsec-vpn vpn-name;
            pair-policy pair-policy;
          }
        }
        reject;
      }
    }
  }
  global {
    policy policy-name {
      description description;
      match {
        application {
          [application];
          any;
        }
        destination-address {
          [address];
          any;
          any-ipv4;
          any-ipv6;
        }
```


Copyright © 2013, Juniper Networks, Inc.

```
    source-address {
      [address];
      any;
      any-ipv4;
      any-ipv6;
    }
    source-identity {
      [role-name];
      any;
      authenticated-user;
      unauthenticated-user;
      unknown-user;
    }
  }
  scheduler-name scheduler-name;
  then {
    count {
      alarm {
        per-minute-threshold number;
        per-second-threshold number;
      }
    }
    deny;
    log {
      session-close;
      session-init;
    }
    permit {
      application-services {
        application-firewall {
          rule-set rule-set-name;
        }
        application-traffic-control {
          rule-set rule-set-name;
        }
        gprs-gtp-profile profile-name;
        gprs-sctp-profile profile-name;
        idp;
        redirect-wx | reverse-redirect-wx;
        ssl-proxy {
          profile-name profile-name;
        }
        uac-policy {
          captive-portal captive-portal;
        }
        utm-policy policy-name;
      }
      destination-address {
        drop-translated;
        drop-untranslated;
      }
      firewall-authentication {
        pass-through {
          access-profile profile-name;
          client-match user-or-group-name;
          ssl-termination-profile profile-name;
```

Copyright © 2013, Juniper Networks, Inc.

```
                web-redirect;
                web-redirect-to-https;
              }
              web-authentication {
                client-match user-or-group-name;
              }
            }
            services-offload;
            tcp-options {
              sequence-check-required;
              syn-check-required;
            }
          }
          reject;
        }
      }
    }
    policy-rematch;
    traceoptions {
      file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
      }
      flag flag;
      no-remote-trace;
    }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Junos OS Release 8.5. Support for the **services-offload** option added in Junos OS Release 11.4. Support for the **source-identitiy** option added in Junos OS Release 12.1. Support for the **description** option added in Junos OS Release 12.1. Support for the **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10.

**Description** Configure network security policies.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Quality of Service
- Security Policies for Security Devices
- Logical Systems for Security Devices
- Security Policy
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## policy (Security Alarms)

**Syntax**

```
policy {
  application {
    duration interval;
    size count;
    threshold value;
  }
  destination-ip {
    duration interval;
    size count;
    threshold value;
  }
  policy match {
    duration interval;
    size count;
    threshold value;
  }
  source-ip {
    duration interval;
    size count;
    threshold value;
  }
}
```

**Hierarchy Level** [edit security alarms potential-violation]

**Release Information** Statement introduced in Junos OS Release 11.2.

**Description** Configure alarms for policy violation, based on source IP, destination IP, application, and policy rule.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## policy (Security IKE)

**Syntax**

```
policy policy-name {
  certificate {
    local-certificate certificate-id;
    peer-certificate-type (pkcs7 | x509-signature);
  }
  description description;
  mode (aggressive | main);
  pre-shared-key (ascii-text key | hexadecimal key);
  proposal-set (basic | compatible | standard);
  proposals [proposal-name];
}
```

**Hierarchy Level**

[edit security group-vpn member ike]
[edit security group-vpn server ike]
[edit security ike]

**Release Information**

Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

**Description**

Configure an IKE policy.

**Options**

***policy-name***—Name of the IKE policy. The policy name can be up to 32 alphanumeric characters long.

The remaining statements are explained separately.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## policy (Security IPsec)

**Syntax**

```
policy policy-name {
    description description;
    perfect-forward-secrecy keys (group1 | group14 | group2 | group5);
    proposal-set (basic | compatible | standard);
    proposals [proposal-name];
}
```

**Hierarchy Level** [edit security ipsec]

**Release Information** Statement modified in Release 8.5 of Junos OS. Support for group 14 is added in Release 11.1 of Junos OS.

**Description** Define an IPsec policy.

**Options** ***policy-name*** —Name of the IPsec policy.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## policy (Security Policies)

**Syntax**

```
policy policy-name {
  description description;
  match {
    application {
      [application];
      any;
    }
    destination-address {
      [address];
      any;
      any-ipv4;
      any-ipv6;
    }
    source-address {
      [address];
      any;
      any-ipv4;
      any-ipv6;
    }
    source-identity {
      [role-name];
      any;
      authenticated-user;
      unauthenticated-user;
      unknown-user;
    }
  }
  scheduler-name scheduler-name;
  then {
    count {
      alarm {
        per-minute-threshold number;
        per-second-threshold number;
      }
    }
    deny;
    log {
      session-close;
      session-init;
    }
    permit {
      application-services {
        application-firewall {
          rule-set rule-set-name;
        }
        application-traffic-control {
          rule-set rule-set-name;
        }
        gprs-gtp-profile profile-name;
        gprs-sctp-profile profile-name;
        idp;
        redirect-wx | reverse-redirect-wx;
```


Copyright © 2013, Juniper Networks, Inc.

```
        ssl-proxy {
            profile-name profile-name;
        }
        uac-policy {
            captive-portal captive-portal;
        }
        utm-policy policy-name;
    }
    destination-address {
        drop-translated;
        drop-untranslated;
    }
    firewall-authentication {
        pass-through {
            access-profile profile-name;
            client-match user-or-group-name;
            web-redirect;
        }
        web-authentication {
            client-match user-or-group-name;
        }
    }
    services-offload;
    tcp-options {
        sequence-check-required;
        syn-check-required;
    }
    tunnel {
        ipsec-group-vpn group-vpn;
        ipsec-vpn vpn-name;
        pair-policy pair-policy;
    }
  }
  reject;
 }
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name*]

**Release Information** Statement introduced in Junos OS Release 8.5. The **services-offload** option added in Junos OS Release 11.4. Statement updated with the **source-identity** option, and the **description** option added in Junos OS Release 12.1.

**Description** Define a security policy.

**Options** ***policy-name***—Name of the security policy.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Copyright © 2013, Juniper Networks, Inc.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- Application Quality of Service
- Security Policies for Security Devices

## policy-lookup-cache

**Syntax** (policy-lookup-cache | no-policy-lookup-cache);

**Hierarchy Level** [edit security idp sensor-configuration global]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Enable cache to accelerate IDP policy lookup.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## policy-match

**Syntax**

```
policy match {
  duration interval;
  size count;
  threshold value;
}
```

**Hierarchy Level** [edit security alarms potential-violation policy]

**Release Information** Statement introduced in Junos OS Release 11.2.

**Description** Configure alarms for a policy rule or a group of rule violations within a specified time period.

**Options**

- **duration *interval***—Indicate the duration of counters.

  **Range:** 1 through 3600 seconds.
  **Default:** 1 second.

- **size *count***—Indicate the number of policies for which policy violation checks can be done concurrently.

  **Range:** 1 through 10240.
  **Default:** 1024.

- **threshold *value***—Indicate the number of policies for which policy violation checks can be done concurrently.

  **Range:** 1 through 4294967295.
  **Default:** 1000.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## policy-rematch

**Syntax** policy-rematch;

**Hierarchy Level** [edit security policies]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Enable the device to add a policy that has just been modified to a deferred action list for reevaluation. For every session associated with the policy, the device reevaluates the policy lookup. If the policy is different from the one associated with the session, the device drops the session. If the policy matches, the session continues.

The policy rematch feature is disabled by default.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## pool (Security Destination NAT)

**Syntax**
```
pool pool-name {
  address ip-address {
    (port port-number | to ip-address);
  }
  description text;
  routing-instance routing-instance-name;
}
```

**Hierarchy Level** [edit security nat destination]

**Release Information** Statement modified in Junos OS Release 9.6. The **description** option added in Junos OS Release 12.1.

**Description** Define a destination NAT pool to identify the pool uniquely.

**Options**
- *pool-name*—Name of the pool.
- description—Description of the pool.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## pool (Security Source NAT)

**Syntax**

```
pool pool-name {
  address ip-address {
    to ip-address;
  }
  description text;
  host-address-base ip-address;
  overflow-pool (interface | pool-name);
  port {
    (no-translation | port-overloading-factor number | range port-low <to port-high>);
  }
  routing-instance routing-instance-name;
}
```

**Hierarchy Level** [edit security nat source]

**Release Information** Statement modified in Junos OS Release 9.6. The **description** option added in Junos OS Release 12.1.

**Description** Define a source NAT pool to identify the pool uniquely.

**Options**

- ***pool-name***—Name of the pool.
- **Description**—Description of the pool.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## pool (Security Source NAT Rule Set)

**Syntax**

```
pool {
  persistent-nat {
    address-mapping;
    inactivity-timeout seconds;
    max-session-number number;
    permit (any-remote-host | target-host | target-host-port);
  }
  pool-name;
}
```

**Hierarchy Level** [edit security nat source rule-set *rule-set-name* rule *rule-name* then source-nat]

**Release Information** Statement introduced in Junos OS Release 9.6.

**Description** Specify to use source NAT pool.

**Options** *pool-name*—Name of the source NAT pool.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

## pool-default-port-range

**Syntax** pool-default-port-range *lower-port-range* to *upper-port-range*;

**Hierarchy Level** [edit security nat source]

**Release Information** Statement introduced in Junos OS Release 11.4.

**Description** Set the default port range for source NAT pools with port translation. If the port range in source NAT pools is not specified, the configured default port range is used.

**Options**
- ***lower-port-range***—Specify the lower limit of the port range.
- ***upper-port-range***—Specify the upper limit of the port range.

**Range:** 1024 through 63,487. To view pool information, use the **show security nat source pool** command.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## pool-utilization-alarm

**Syntax**

```
pool-utilization-alarm {
  clear-threshold value;
  raise-threshold value;
}
```

**Hierarchy Level** [edit security nat source]

**Release Information** Statement modified in Junos OS Release 9.2.

**Description** Define the pool utilization alarm thresholds for a Network Address Translation (NAT) source IP address pool without Port Address Translation (PAT). When pool utilization exceeds the upper (raise) threshold or falls below the lower (clear) threshold, an SNMP trap is triggered.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

## pop3-profile (Security UTM Policy Antivirus)

**Syntax** pop3-profile *profile-name*;

**Hierarchy Level** [edit security utm utm-policy *policy-name* anti-virus]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the antivirus POP3 protocol and attach this policy to a security profile to implement it.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## pop3-profile (Security UTM Policy Content Filtering)

**Syntax** pop3-profile *profile-name*;

**Hierarchy Level** [edit security utm utm-policy *policy-name* content-filtering]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the content-filtering POP3 protocol and attach this policy to a security profile to implement it.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices

## port (Security Antivirus)

**Syntax** port *port-number*;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine pattern-update proxy]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update proxy]
[edit security utm feature-profile anti-virus sophos-engine pattern-update proxy]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Set the port number for the proxy server.

**Options** **Range:** 0 through 65,535

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## port (Security NAT)

**Syntax**

```
port {
    (no-translation | port-overloading-factor number | range port-low <to port-high>);
}
```

**Hierarchy Level** [edit security nat source pool *pool-name*]

**Release Information** Statement introduced in Junos OS Release 9.2.

**Description** Specify the Port Address Translation (PAT) for a source pool.

**Options**

- **no-translation**—If set, no Port Address Translation is required.
- **port-overloading-factor** *number*—Configure the port overloading capacity in source NAT.
- **range** *port-low* **<to** *port-high***>**—Specify the port number range attached to each address in the pool.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

## port (Security Web Filtering Server)

**Syntax** port *number*;

**Hierarchy Level**
[edit security utm feature-profile web-filtering surf-control-integrated server]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name* server]
[edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name* server]

**Release Information** Statement introduced in Release 9.5 of Junos OS.
Statement introduced in Release 11.4 of Junos OS for Enhanced Web Filtering.

**Description** Enter the port number for communicating with the server. (Default ports are 80, 8080, and 8081.)

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## port-overloading (Security NAT Source)

**Syntax**

```
port-overloading {
  off;
}
```

**Hierarchy Level** [edit security nat source interface]

**Release Information** Statement introduced in Junos OS Release 9.6.

**Description** Enable interface NAT with or without port overloading.

**Options**

- **off**—Specify off to disable interface port overloading.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

## port-overloading-factor

**Syntax** port-overloading-factor

**Hierarchy Level** [edit security nat source pool *source-pool-name* port]

**Release Information** Statement introduced in Junos OS Release 11.2.

**Description** Configures the port overloading capacity in source NAT. If the port-overloading-factor is set to *x*, each translated IP address will have *x* number of ports available.



NOTE: The port-overloading-factor statement cannot be configured with port no-translation (source NAT pool without PAT) or port-range configuration statements.

**Options** **Range:** 2 through 32

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## port-randomization

**Syntax**

```
port-randomization {
  disable;
}
```

**Hierarchy Level** [edit security nat source]

**Release Information** Statement introduced in Junos OS Release 9.6.

**Description** Disable random port allocation for pool-based and interface source NAT.

**Options** **disable**—Disables random port allocation for pool-based and interface source NAT. For pool-based source NAT and interface NAT, port numbers are allocated randomly by default. Although randomized port number allocation can provide protection from security threats such as DNS poison attacks, it can also affect performance and memory usage for pool-based source NAT.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## port-scan

**Syntax**

```
port-scan {
  threshold number;
}
```

**Hierarchy Level** [edit security screen ids-option *screen-name* tcp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Prevent port scan attacks. A port scan attack occurs when an attacker sends packets with different port numbers to scan available services. The attack succeeds if a port responds. To prevent this attack, the device internally logs the number of different ports scanned from a single remote source. For example, if a remote host scans 10 ports in 0.005 seconds (equivalent to 5000 microseconds, the default threshold setting), the device flags this behavior as a port scan attack, and rejects further packets from the remote source.

**Options**

**threshold** ***number*** —Number of microseconds during which the device accepts packets from the same remote source with up to 10 different port numbers. If the number of ports during the threshold period reaches 10 or more, the device rejects additional packets from the source.

**Range:** 1000 through 1,000,000 microseconds

**Default:** 5000 microseconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Configuration Statement Hierarchy


Copyright © 2013, Juniper Networks, Inc.

## post-attack

**Syntax** post-attack *number*;

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then notification packet-log]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Specify the number of packets received after an attack that should be captured for further analysis of attacker behavior. If post-attack packets are not significant to your analysis or the configured attack response ends packet transfer, you can set the post-attack option to 0.

**Options** ***number***—Number of post-attack packets to be captured.

**Range:** 0 through 255

**Default:** 5

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## post-attack-timeout

**Syntax** post-attack-timeout *seconds*;

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then notification packet-log]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Specify a time limit for capturing post-attack packets for a session. No packet capture is conducted after the timeout has expired.

**Options** ***seconds***—Maximum number of seconds for post-attack packet capture.

**Range:** 0 to 1800 seconds

**Default:** 5

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## potential-violation

**Syntax**

```
potential-violation {
  authentication failures;
  cryptographic-self-test;
  decryption-failures {
    threshold value;
  }
  encryption-failures {
    threshold value;
  }
  idp;
  ike-phase1-failures {
    threshold value;
  }
  ike-phase2-failures {
    threshold value;
  }
  key-generation-self-test;
  non-cryptographic-self-test;
  policy {
    application {
      duration interval;
      size count;
      threshold value;
    }
    destination-ip {
      duration interval;
      size count;
      threshold value;
    }
    policy match {
      duration interval;
      size count;
      threshold value;
    }
    source-ip {
      duration interval;
      size count;
      threshold value;
    }
  }
  replay-attacks {
    threshold value;
  }
  security-log-percent-full percentage;
}
```

**Hierarchy Level** [edit security alarms]

**Release Information** Statement introduced in Junos OS Release 11.2.

**Description** Configure alarms for potential violation.


Copyright © 2013, Juniper Networks, Inc.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## pptp

**Syntax**

```
pptp {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the Point-to-Point Tunneling Protocol (PPTP) ALG on the device.

**Options**
- **disable**—Disable the PPTP ALG. By default, the PPTP ALG is enabled.
- **traceoptions**—Configure PPTP ALG tracing options.
  - **flag**—Trace operation to perform.
    - **all**—Trace all events.
    - ***extensive***—Display extensive amount of data.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policy Applications for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## pre-attack

**Syntax** pre-attack *number*;

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then notification packet-log]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Specify the number of packets received before an attack that should be captured for further analysis of attacker behavior.

**Options** *number*—Number of pre-attack packets.

**Range:** 1 through 255

**Default:** 1

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## pre-filter-shellcode

**Syntax** pre-filter-shellcode;

**Hierarchy Level** [edit security idp sensor-configuration ips]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Enable to pre-filter the shell code and protects it from buffer overflow attacks. By default this setting is enabled.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## pre-shared-key (Security IKE Policy)

**Syntax** pre-shared-key (ascii-text *key* | hexadecimal *key*);

**Hierarchy Level** [edit security group-vpn member ike policy *policy-name*]
[edit security group-vpn server ike policy *policy-name*]
[edit security ike policy *policy-name*]

**Release Information** Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in OS Release 10.2 of Junos OS.

**Description** Define a preshared key for an IKE policy.



NOTE: The device deletes existing IKE and IPsec SAs when you update the pre-shared-key configuration in the IKE policy.

**Options**
- **ascii-text *key***—ASCII text key.
- **hexadecimal *key***—Hexadecimal key.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPNs for Security Devices

## predefined-attack-groups

**Syntax** predefined-attack-groups [*attack-group-name*];

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match attacks],
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match attacks]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify predefined attack groups that you can use to match the traffic against known attack objects. You can update only the list of attack objects.

**Options** ***attack-name*** —Name of the predefined attack object group.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## predefined-attacks

**Syntax** predefined-attacks [*attack-name*];

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match attacks], [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match attacks]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify predefined attack objects that you can use to match the traffic against known attacks. You can update only the list of attack objects.

**Options** ***attack-name***—Name of the predefined attack objects.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## prefix (Security Static NAT)

**Syntax**

```
prefix {
  address-prefix;
  mapped-port lower-port-range to upper-port-range;
  routing-instance (default | routing-instance-name);
}
```

**Hierarchy Level** [edit security nat static rule-set *rule-set-name* rule *rule-name* then static-nat]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify a static IP address prefix.

**Options**

- ***address-prefix***—Specify address prefix.
- **mapped-port *lower-port-range* to *upper-port-range***—Specify a destination port or port range to allow static NAT to map ports.
- **routing-instance** —Specify routing instance type:
  - ***routing-instance-name***—Use the user-defined static NAT routing instance to perform static NAT.
  - **default**—Use the default routing-instance.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## prefix-name (Security Static NAT)

**Syntax**

```
prefix-name {
  address-prefix-name;
  mapped-port lower-port-range to upper-port-range;
  routing-instance (default | routing-instance-name);
}
```

**Hierarchy Level** [edit security nat static rule-set *rule-set-name* rule *rule-name* then static-nat]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify an address from the address book.

**Options**

- ***address-prefix-name***—Specify address prefix name from address book.
- **mapped-port *lower-port-range* to *upper-port-range***—Specify a destination port or port range to allow static NAT to map ports.
- **routing-instance** —Specify routing instance type:
  - ***routing-instance-name***—Use the user-defined static NAT routing instance to perform static NAT.
  - **default**—Use the default routing-instance.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

## process-ignore-s2c

**Syntax** (process-ignore-s2c | no-process-ignore-s2c);

**Hierarchy Level** [edit security idp sensor-configuration ips]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Set the command to disable the server-to-client inspection.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## process-override

**Syntax** (process-override | no-process-override);

**Hierarchy Level** [edit security idp sensor-configuration ips]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Set the command to forcefully run the IDS inspection module even if there is no policy match.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## process-port

**Syntax** process-port *port-number*;

**Hierarchy Level** [edit security idp sensor-configuration ips]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Set the command to a specific port to forcefully run the IDS inspection module on that TCP/UDP port even if there is no policy match.

**Options** ***port-number***—Port Number.
**Range:** 0 through 65,535

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## products

**Syntax**

```
products {
  values [product-value];
}
```

**Hierarchy Level** [edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify a products filter to add attack objects based on the application that is vulnerable to the attack.

**Options** **values**—Name of the products filter. You can configure multiple filters separated by spaces and enclosed in square brackets.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## profile (Security Antispam SBL)

**Syntax**

```
profile profile-name {
  custom-tag-string [string];
  (sbl-default-server | no-sbl-default-server);
  spam-action (block | tag-header | tag-subject);
}
```

**Hierarchy Level** [edit security utm feature-profile anti-spam sbl]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Create a profile for the antispam sbl feature. This profile includes all subsequent configuration options.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## profile (Security Antivirus Juniper Express Engine)

**Syntax**

```
profile profile-name {
  fallback-options {
    content-size (block | log-and-permit);
    default (block | log-and-permit);
    engine-not-ready (block | log-and-permit);
    out-of-resources (block | (log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  notification-options {
    fallback-block {
      administrator-email email-address;
      allow-email;
      custom-message message;
      custom-message-subject message-subject;
      display-host;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
    fallback-non-block {
      custom-message message;
      custom-message-subject message-subject;
      (notify-mail-recipient | no-notify-mail-recipient);
    }
    virus-detection {
      custom-message message;
      custom-message-subject message-subject;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
  }
  scan-options {
    content-size-limit value;
    (intelligent-prescreening | no-intelligent-prescreening);
    timeout value;
  }
  trickling {
    timeout value;
  }
}
```

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Create a profile for the Juniper express engine. This profile includes all subsequent configuration options.

**Options** The remaining statements are explained separately.

Copyright © 2013, Juniper Networks, Inc.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## profile (Security Antivirus Kaspersky Lab Engine)

**Syntax**

```
profile profile-name {
  fallback-options {
    content-size (block | log-and-permit);
    corrupt-file (block | log-and-permit);
    decompress-layer (block | log-and-permit);
    default (block | log-and-permit);
    engine-not-ready (block | log-and-permit);
    out-of-resources (block | (log-and-permit);
    password-file (block | (log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  notification-options {
    fallback-block {
      administrator-email email-address;
      allow-email;
      custom-message message;
      custom-message-subject message-subject;
      display-host;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
    fallback-non-block {
      custom-message message;
      custom-message-subject message-subject;
      (notify-mail-recipient | no-notify-mail-recipient);
    }
    virus-detection {
      custom-message message;
      custom-message-subject message-subject;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
  }
  scan-options {
    content-size-limit value;
    decompress-layer-limit value;
    (intelligent-prescreening | no-intelligent-prescreening);
    scan-extension filename;
    scan-mode (all | by-extension);
    timeout value;
  }
  trickling {
    timeout value;
  }
}
```

**Hierarchy Level** [edit security utm feature-profile anti-virus kaspersky-lab-engine]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

Copyright © 2013, Juniper Networks, Inc.

**Description** Create a profile for the Kaspersky Lab engine. This profile includes all subsequent configuration options.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## profile (Security Content Filtering)

**Syntax**

```
profile profile-name {
  block-command protocol-command-list;
  block-content-type (activex | exe | http-cookie | java-applet | zip);
  block-extension extension-list;
  block-mime {
    exception list-name;
    list list-name;
  }
  notification-options {
    custom-message message;
    (notify-mail-sender | no-notify-mail-sender);
    type (message | protocol-only);
  }
  permit-command protocol-command-list;
}
```

**Hierarchy Level** [edit security utm feature-profile content-filtering]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Create a profile for the content-filtering feature. This profile includes all subsequent configuration options.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## profile (Security GTP)

**Syntax**

```
profile profile name {
  apn pattern-string {
    imsi-prefix imsi-prefix-digits {
      action {
        drop;
        pass;
        selection (ms|net|vrf);
      }
    }
  }
  drop {
    aa-create-pdp (0 | 1 | 2 | all);
    aa-delete-pdp (0 | 1 | 2 | all);
    bearer-resource (0 | 1 | 2 | all);
    change-notification (0 | 1 | 2 | all);
    config-transfer (0 | 1 | 2 | all);
    context (0 | 1 | 2 | all);
    create-bearer (0 | 1 | 2 | all);
    create-data-forwarding (0 | 1 | 2 | all);
    create pdp (0 | 1 | 2 | all);
    create-session (0 | 1 | 2 | all);
    create-tnl-forwarding (0 | 1 | 2 | all);
    cs-paging (0 | 1 | 2 | all);
    data-record (0 | 1 | 2 | all);
    delete-bearer (0 | 1 | 2 | all);
    delete-command (0 | 1 | 2 | all);
    delete-data-forwarding (0 | 1 | 2 | all);
    delete-pdn (0 | 1 | 2 | all);
    delete-pdp (0 | 1 | 2 | all);
    delete-session (0 | 1 | 2 | all);
    detach (0 | 1 | 2 | all);
    downlink-notification (0 | 1 | 2 | all);
    echo (0 | 1 | 2 | all);
    error-indication (0 | 1 | 2 | all);
    failure-report (0 | 1 | 2 | all);
    fwd-access (0 | 1 | 2 | all);
    fwd-relocation (0 | 1 | 2 | all);
    fwd-srns-context (0 | 1 | 2 | all);
    g-pdu (0 | 1 | 2 | all);
    identification (0 | 1 | 2 | all);
    mbms-sess-start (0 | 1 | 2 | all);
    mbms-sess-stop (0 | 1 | 2 | all);
    mbms-sess-update (0 | 1 | 2 | all);
    modify-bearer (0 | 1 | 2 | all);
    modify-command (0 | 1 | 2 | all);
    node-alive (0 | 1 | 2 | all);
    note-ms-present (0 | 1 | 2 | all);
    pdu-notification (0 | 1 | 2 | all);
    ran-info (0 | 1 | 2 | all);
    redirection (0 | 1 | 2 | all);
    release-access (0 | 1 | 2 | all);
    relocation-cancel (0 | 1 | 2 | all);
```

Copyright © 2013, Juniper Networks, Inc.

```
    resume (0 | 1 | 2 | all);
    send-route (0 | 1 | 2 | all);
    sgsn-context (0 | 1 | 2 | all);
    stop-paging (0 | 1 | 2 | all);
    supported-extension (0 | 1 | 2 | all);
    suspend (0 | 1 | 2 | all);
    trace-session (0 | 1 | 2 | all);
    update-bearer (0 | 1 | 2 | all);
    update-pdn (0 | 1 | 2 | all);
    update-pdp (0 | 1 | 2 | all);
    ver-not-supported (0 | 1 | 2 | all);
  }
  gtp-in-gtp-denied;
  log {
    forwarded (basic | detail);
    prohibited (basic | detail);
    rate-limited {
      (basic | detail);
      frequency-number number;
    }
    state-invalid (basic | detail);
  }
  max-message-length number;
  min-message-length number;
  rate-limit limit;
  remove-ie {
    version v1 {
      number ie-number;
      release (R6 | R7 | R8 | R9);
    }
  }
  restart-path (all | create | echo);
  timeout (value);
  }
}
```

**Hierarchy Level** [edit security gprs gtp]

**Release Information** Statement introduced in Release 10.0 of Junos OS. The **restart-path** option added in Release 11.4 of Junos OS. New GTP message types added in Release 11.4 of Junos OS. Support for GTPv2 added in Release 11.4 of Junos OS.

**Description** Create a profile for the GTP feature. This profile includes all subsequent configuration options.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- General Packet Radio Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## profile (Security SCTP)

**Syntax**

```
profile profile-name {
  association-timeout time-in-minutes;
  drop {
    m3ua-service {
      isup;
      sccp;
      tup;
    }
    payload-protocol {
      all;
      asap;
      bicc;
      ddp-segment;
      ddp-stream;
      dua;
      enrp;
      h248;
      h323;
      iua;
      m2pa;
      m2ua;
      m3ua;
      qipc;
      reserved;
      simco;
      sua;
      tali;
      v5ua;
    }
  }
  handshake-timeout time-in-seconds;
  limit {
    rate {
      address ip-address {
        sccp rate-limit;
        ssp rate-limit;
        sst rate-limit;
      }
      sccp rate-limit;
      ssp rate-limit;
      sst rate-limit;
    }
  }
}
```

**Hierarchy Level** [edit security gprs sctp]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Create a profile of the Stream Control Transmission Protocol (SCTP) feature. This profile includes all subsequent configuration options.

Copyright © 2013, Juniper Networks, Inc.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- General Packet Radio Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## profile (Security Sophos Engine Antivirus)

**Syntax**

```
profile <name> {
  fallback-options {
    content-size (block | log-and-permit | permit);
    default (block | log-and-permit | permit);
    engine-not-ready (block | log-and-permit | permit);
    out-of-resources (block | log-and-permit | permit);
    timeout (block | log-and-permit | permit);
    too-many-requests (block | log-and-permit | permit);
  }
  notification-options {
    fallback-block {
      administrator-email email-address;
      allow-email;
      custom-message message;
      custom-message-subject message-subject;
      display-host;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
    fallback-non-block {
      custom-message message;
      custom-message-subject message-subject;
      (notify-mail-recipient | no-notify-mail-recipient);
    }
    virus-detection {
      custom-message message;
      custom-message-subject message-subject;
      (notify-mail-sender | no-notify-mail-sender);
      type (message | protocol-only);
    }
  }
  scan-options {
    content-size-limit value;
    (no-uri-check | uri-check);
    timeout value;
  }
  trickling {
    timeout value;
  }
}
```

**Hierarchy Level** [edit security utm feature-profile anti-virus sophos-engine]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Create a profile for the Sophos antivirus engine. This profile includes all subsequent configuration options.

**Options** The remaining statements are explained separately.

Copyright © 2013, Juniper Networks, Inc.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

## profile (Security Web Filtering Juniper Enhanced)

**Syntax**

```
profile profile-name {
  category customurl-list name {
    action (block | log-and-permit | permit | quarantine);
  }
  custom-block-message value;
  custom-quarantine-message value;
  default (block | log-and-permit | permit | quarantine);
  fallback-settings {
    default (block | log-and-permit);
    server-connectivity (block | log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  no-safe-search;
  site-reputation-action {
    fairly-safe (block | log-and-permit | permit | quarantine);
    harmful (block | log-and-permit | permit | quarantine);
    moderately-safe (block | log-and-permit | permit | quarantine);
    suspicious (block | log-and-permit | permit | quarantine);
    very-safe (block | log-and-permit | permit | quarantine);
  }
  timeout value;
}
```

**Hierarchy Level**
[edit security utm feature-profile web-filtering juniper-enhanced]

**Release Information**
Statement introduced in Release 11.4 of Junos OS.

**Description**
Create a profile for the juniper-enhanced feature. This profile includes all subsequent configuration options.

**Options**
The remaining statements are explained separately.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- Monitoring Web Filtering Configurations


Copyright © 2013, Juniper Networks, Inc.

## profile (Security Web Filtering Juniper Local)

**Syntax**

```
profile profile-name {
  custom-block-message value;
  default (block | log-and-permit | permit);
  fallback-settings {
    default (block | log-and-permit);
    server-connectivity (block | log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  timeout value;
}
```

**Hierarchy Level** [edit security utm feature-profile web-filtering juniper-local]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Create a profile for the web-filtering juniper–local feature. This profile includes all subsequent configuration options.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- Monitoring Web Filtering Configurations
- Example: Configuring Local Web Filtering

Copyright © 2013, Juniper Networks, Inc.

## profile (Security Web Filtering Surf Control Integrated)

**Syntax**

```
profile profile-name {
  category customurl-list name {
    action (block | log-and-permit | permit);
  }
  custom-block-message value;
  default (block | log-and-permit | permit);
  fallback-settings {
    default (block | log-and-permit);
    server-connectivity (block | log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  timeout value;
}
```

**Hierarchy Level** [edit security utm feature-profile web-filtering surf-control-integrated]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Create a profile for the web-filtering surf-control-integrated feature. This profile includes all subsequent configuration options.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- Monitoring Web Filtering Configurations


Copyright © 2013, Juniper Networks, Inc.

## profile (Security Web Filtering Websense Redirect)

**Syntax**

```
profile profile-name {
  account value;
  custom-block-message value;
  fallback-settings {
    default (block | log-and-permit);
    server-connectivity (block | log-and-permit);
    timeout (block | log-and-permit);
    too-many-requests (block | log-and-permit);
  }
  server {
    host host-name;
    port number;
  }
  sockets value;
  timeout value;
}
```

**Hierarchy Level** [security utm feature-profile web-filtering websense-redirect]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Create a profile for the web-filtering web-sense feature. This profile includes all subsequent configuration options.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- Monitoring Web Filtering Configurations

Copyright © 2013, Juniper Networks, Inc.

## proposal (Security Group VPN Server IKE)

**Syntax**

```
proposal proposal-name {
  authentication-algorithm (md5 | sha-256 | sha1);
  authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
  description description;
  dh-group (group1 | group14 | group2 | group5);
  encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
}
```

**Hierarchy Level** [edit security group-vpn server ike]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Define an IKE proposal for group VPN server.

**Options** *proposal-name*—Name of the IKE proposal. The proposal name can be up to 32 alphanumeric characters long.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Group VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## proposal (Security IKE)

**Syntax**

```
proposal proposal-name {
  authentication-algorithm (md5 | sha-256 | sha1);
  authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
  description description;
  dh-group (group1 | group14 | group2 | group5);
  encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
  lifetime-seconds seconds;
}
```

**Hierarchy Level**

[edit security group-vpn member ike]
[edit security ike]

**Release Information**

Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS. Support for dh-group group 14 and DSA signatures are added in Release 11.1 of Junos OS.

**Description**

Define an IKE proposal.

**Options**

***proposal-name*** —Name of the IKE proposal. The proposal name can be up to 32 alphanumeric characters long.

The remaining statements are explained separately.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## proposal (Security IPsec)

**Syntax**

```
proposal proposal-name {
  authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
  description description;
  encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
  lifetime-kilobytes kilobytes;
  lifetime-seconds seconds;
  protocol (ah | esp);
}
```

**Hierarchy Level** [edit security ipsec]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Define an IPsec proposal.

**Options** *proposal-name*—Name of the IPsec proposal.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## proposal-set (Security IKE)

**Syntax** proposal-set (basic | compatible | standard);

**Hierarchy Level** [edit security group-vpn member ike policy *policy-name*]
[edit security group-vpn server ike policy *policy-name*]
[edit security ike policy *policy-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

**Description** Specify a set of default Internet Key Exchange (IKE) proposals.

**Options**

- **basic**—Basic set of two IKE proposals:
  - Proposal 1—Preshared key, Data Encryption Standard (DES) encryption, and Diffie-Hellman (DH) group 1 and Secure Hash Algorithm 1 (SHA-1) authentication.
  - Proposal 2—Preshared key, DES encryption, and DH group 1 and Message Digest 5 (MD5) authentication.
- **compatible**—Set of four commonly used IKE proposals:
  - Proposal 1—Preshared key, triple DES (3DES) encryption, and Gnutella2 (G2) and SHA-1 authentication.
  - Proposal 2—Preshared key, 3DES encryption, and DH group 2 and MD5 authentication.
  - Proposal 3—Preshared key, DES encryption, and DH group 2 and SHA-1 authentication.
  - Proposal 4—Preshared key, DES encryption, and DH group 2 and MD5 authentication.
- **standard**—Standard set of two IKE proposals:
  - Proposal 1— Preshared key, 3DES encryption, and DH group 2 and SHA-1 authentication.
  - Proposal 2—Preshared key, Advanced Encryption Standard (AES) 128-bit encryption, and DH group 2 and SHA-1 authentication.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## proposal-set (Security IPsec)

**Syntax** proposal-set (basic | compatible | standard);

**Hierarchy Level** [edit security ipsec policy *policy-name*]

**Release Information** Statement modified in Release 10.4 of Junos OS.

**Description** Define a set of default IPsec proposals.

**Options**

- **basic**—nopfs-esp-des-sha and nopfs-esp-des-md5
- **compatible**—nopfs-esp-3des-sha, nopfs-esp-3des-md5, nopfs-esp-des-sha, and nopfs-esp-des-md5
- **standard**—g2-esp-3des-sha and g2-esp-aes128-sha



NOTE: Perfect Forward Secrecy setting in IPsec policy will override the settings in proposal-sets in 10.4 and later releases.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## proposals (Security IKE)

**Syntax** proposals [*proposal-name*];

**Hierarchy Level** [edit security group-vpn member ike policy *policy-name*]
[edit security group-vpn server ike policy *policy-name*]
[edit security ike policy *policy-name*]

**Release Information** Statement modified in Release 8.5 of Junos OS. Support for **group-vpn** hierarchies added in Release 10.2 of Junos OS.

**Description** Specify up to four Phase 1 proposals for an IKE policy. If you include multiple proposals, use the same Diffie-Hellman group in all of the proposals.

**Options** ***proposal-name***—Names of up to four configured Phase 1 proposals.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

## proposals (Security IPsec)

**Syntax** proposals [*proposal-name*];

**Hierarchy Level** [edit security ipsec policy *policy-name*]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Specify one or more proposals for an IPsec policy.

**Options** *proposal-name*—Name of a configured proposal.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## protect

**Syntax**

```
protect {
  deny {
    all {
      timeout value-in-seconds;
    }
    destination-ip address;
    timeout value-in-seconds;
  }
}
```

**Hierarchy Level** [edit security alg sip application-screen]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure options to protect servers against INVITE attacks.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Layer Gateways for Security Devices

## protocol (Security Destination NAT)

**Syntax** protocol [*protocol-name-or-number*];

**Hierarchy Level** [edit security nat destination rule-set *rule-set-name* rule *rule-name* match]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify an IP protocol to match the rule. You can configure multiple protocol names or protocol numbers.

**Options** ***protocol-name-or-number***—Name or number of the specific protocol.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## protocol (Security IDP IP Headers)

**Syntax**

```
protocol {
  match (equal | greater-than | less-than | not-equal);
  value transport-layer-protocol-id;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol ipv4]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the Transport Layer protocol number.

**Options**

- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***transport-layer-protocol-id***—Match the Transport Layer protocol ID.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## protocol (Security IDP Signature Attack)

**Syntax**

```
protocol {
  icmp {
    code {
      match (equal | greater-than | less-than | not-equal);
      value code-value;
    }
    data-length {
      match (equal | greater-than | less-than | not-equal);
      value data-length;
    }
    identification {
      match (equal | greater-than | less-than | not-equal);
      value identification-value;
    }
    sequence-number {
      match (equal | greater-than | less-than | not-equal);
      value sequence-number;
    }
    type {
      match (equal | greater-than | less-than | not-equal);
      value type-value;
    }
  }
  ipv4 {
    destination {
      match (equal | greater-than | less-than | not-equal);
      value ip-address-or-hostname;
    }
    identification {
      match (equal | greater-than | less-than | not-equal);
      value identification-value;
    }
    ip-flags {
      (df | no-df);
      (mf | no-mf);
      (rb | no-rb);
    }
    protocol {
      match (equal | greater-than | less-than | not-equal);
      value transport-layer-protocol-id;
    }
    source {
      match (equal | greater-than | less-than | not-equal);
      value ip-address-or-hostname;
    }
    tos {
      match (equal | greater-than | less-than | not-equal);
      value type-of-service-in-decimal;
    }
    total-length {
      match (equal | greater-than | less-than | not-equal);
      value total-length-of-ip-datagram;
```


Copyright © 2013, Juniper Networks, Inc.

```
    }
    ttl {
      match (equal | greater-than | less-than | not-equal);
      value time-to-live;
    }
  }
  ipv6 {
    destination {
      match (equal | greater-than | less-than | not-equal);
      value ip-address-or-hostname;
    }
    flow-label {
      match (equal | greater-than | less-than | not-equal);
      value flow-label-value;
    }
    hop-limit {
      match (equal | greater-than | less-than | not-equal);
      value hop-limit-value;
    }
    next-header {
      match (equal | greater-than | less-than | not-equal);
      value next-header-value;
    }
    payload-length {
      match (equal | greater-than | less-than | not-equal);
      value payload-length-value;
    }
    source {
      match (equal | greater-than | less-than | not-equal);
      value ip-address-or-hostname;
    }
    traffic-class {
      match (equal | greater-than | less-than | not-equal);
      value traffic-class-value;
    }
  tcp {
    ack-number {
      match (equal | greater-than | less-than | not-equal);
      value acknowledgement-number;
    }
    data-length {
      match (equal | greater-than | less-than | not-equal);
      value tcp-data-length;
    }
    destination-port {
      match (equal | greater-than | less-than | not-equal);
      value destination-port;
    }
    header-length {
      match (equal | greater-than | less-than | not-equal);
      value header-length;
    }
    mss {
      match (equal | greater-than | less-than | not-equal);
      value maximum-segment-size;
    }
```

```
    option {
      match (equal | greater-than | less-than | not-equal);
      value tcp-option;
    }
    sequence-number {
      match (equal | greater-than | less-than | not-equal);
      value sequence-number;
    }
    source-port {
      match (equal | greater-than | less-than | not-equal);
      value source-port;
    }
    tcp-flags {
      (ack | no-ack);
      (fin | no-fin);
      (psh | no-psh);
      (r1 | no-r1);
      (r2 | no-r2);
      (rst | no-rst);
      (syn | no-syn);
      (urg | no-urg);
    }
    urgent-pointer {
      match (equal | greater-than | less-than | not-equal);
      value urgent-pointer;
    }
    window-scale {
      match (equal | greater-than | less-than | not-equal);
      value window-scale-factor;
    }
    window-size {
      match (equal | greater-than | less-than | not-equal);
      value window-size;
    }
  }
  udp {
    data-length {
      match (equal | greater-than | less-than | not-equal);
      value data-length;
    }
    destination-port {
      match (equal | greater-than | less-than | not-equal);
      value destination-port;
    }
    source-port {
      match (equal | greater-than | less-than | not-equal);
      value source-port;
    }
  }
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify a protocol to match the header information for the signature attack.


Copyright © 2013, Juniper Networks, Inc.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## protocol (Security IPsec)

**Syntax** protocol (ah | esp);

**Hierarchy Level** [edit security ipsec proposal *proposal-name* ]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Define the IPsec protocol for a manual or dynamic security association (SA).



NOTE: The device deletes existing IPsec SAs when you update the encryption-algorithm configuration in the IPsec proposal.

**Options**
- **ah**—Authentication Header protocol.
- **esp**—Encapsulating Security Payload (ESP) protocol.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## protocol (Security IPsec Manual SA)

**Syntax** protocol (ah | esp)

**Hierarchy Level** [edit security ipsec vpn *vpn-name* manual]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Define the IPsec protocol for the manual security association. (This statement is not supported on dynamic VPN implementations.)

**Options**
- **ah**—Authentication Header protocol.
- **esp**—ESP protocol (To use the ESP protocol, you must also use the **tunnel** statement at the **[edit security ipsec security-association *sa-name* mode]** hierarchy level.)

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

## protocol (Security Source NAT)

**Syntax** protocol [*protocol-name-or-number*];

**Hierarchy Level** [edit security nat source rule-set *rule-set-name* rule *rule-name* match]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify an IP protocol to match the rule. You can configure multiple protocol names or protocol numbers.

**Options** ***protocol-name-or-number***—Name or number of the specific protocol.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## protocol-binding

**Syntax**

```
protocol-binding {
  application application-name;
  icmp;
  icmpv6;
  ip {
    protocol-number transport-layer-protocol-number;
  }
  ipv6 {
    protocol-number transport-layer-protocol-number;
  }
  nested-application nested-application-name;
  rpc {
    program-number rpc-program-number;
  }
  tcp {
    minimum-port port-number <maximum-port port-number>;
  }
  udp {
    minimum-port port-number <maximum-port port-number>;
  }
}
```

**Hierarchy Level**

[edit security idp custom-attack *attack-name* attack-type chain]
[edit security idp custom-attack *attack-name* attack-type signature]

**Release Information**

Statement introduced in Release 9.3 of Junos OS.

**Description**

Select a protocol that the attack uses to enter your network.

**Options**

The remaining statements are explained separately.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## protocol-command

**Syntax**

```
protocol-command object-name {
  value [value];
}
```

**Hierarchy Level** [edit security utm custom-objects]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Different protocols use different commands to communicate between servers and clients. By blocking or allowing certain commands, traffic can be controlled on the protocol command level.

**Options**

- ***object-name***—Name of the command-list object.
- **value *value***—Value of the command-list object. You can configure multiple values separated by spaces and enclosed in square brackets.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- Understanding UTM Custom Objects


Copyright © 2013, Juniper Networks, Inc.

## protocol-name

**Syntax**

```
protocol-name protocol-name {
  tunable-name  tunable-name {
    tunable-value protocol-value;
  }
}
```

**Hierarchy Level** [edit security idp sensor-configuration detector]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for file format decoding over HTTP using MIME added in Release 11.2 of Junos OS.

**Description** Specify the name of the protocol to be used to configure each of the protocol detector engines.

**Options** ***protocol-name***—Name of the specific protocol.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## protocols (Security Zones Host Inbound Traffic)

**Syntax**

```
protocols protocol-name {
    except;
}
```

**Hierarchy Level** [edit security zones security-zone *zone-name* host-inbound-traffic]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the types of traffic that can reach the device for all interfaces in a zone.

**Options**

- *protocol-name* —Protocol for which traffic is allowed. The following protocols are supported:
  - **all**—Enable traffic from all possible protocols available.
  - **bfd**—Enable incoming Bidirectional Forwarding Detection (BFD) protocol traffic.
  - **bgp**—Enable incoming BGP traffic.
  - **dvmrp**—Enable incoming Distance Vector Multicast Routing Protocol (DVMRP) traffic.
  - **igmp**—Enable incoming Internet Group Management Protocol (IGMP) traffic.
  - **ldp**—Enable incoming Label Distribution Protocol (LDP) traffic (UDP and TCP port 646).
  - **msdp**—Enable incoming Multicast Source Discovery Protocol (MSDP) traffic.
  - **nhrp**—Enable incoming Next Hop Resolution Protocol (NHRP) traffic.
  - **ospf**—Enable incoming OSPF traffic.
  - **ospf3**—Enable incoming OSPF version 3 traffic.
  - **pgm**—Enable incoming Pragmatic General Multicast (PGM) protocol traffic (IP protocol number 113).
  - **pim**—Enable incoming Protocol Independent Multicast (PIM) traffic.
  - **rip**—Enable incoming RIP traffic.
  - **ripng**—Enable incoming RIP next generation traffic.
  - **router-discovery**—Enable incoming router discovery traffic.
  - **rsvp**—Enable incoming Resource Reservation Protocol (RSVP) traffic (IP protocol number 46).
  - **sap**— Enable incoming Session Announcement Protocol (SAP) traffic. SAP always listens on **224.2.127.254:9875**. New addresses and ports can be added dynamically. This information must be propagated to the Packet Forwarding Engine (PFE).
  - **vrrp**—Enable incoming Virtual Router Redundancy Protocol (VRRP) traffic.
- **except**—(Optional) except can only be used if all has been defined.


Copyright © 2013, Juniper Networks, Inc.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Zones and Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## protocols (Security Zones Interfaces)

**Syntax**

```
protocols protocol-name {
    except;
}
```

**Hierarchy Level** [edit security zones security-zone*zone-name* interfaces*interface-name* host-inbound-traffic]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the types of routing protocol traffic that can reach the device on a per-interface basis.

**Options**

- ***protocol-name*** —Protocol for which traffic is allowed. The following protocols are supported:
  - **all**—Enable traffic from all possible protocols available.
  - **bfd**—Enable incoming Bidirectional Forwarding Detection (BFD) Protocol traffic.
  - **bgp**—Enable incoming BGP traffic.
  - **dvmrp**—Enable incoming Distance Vector Multicast Routing Protocol (DVMRP) traffic.
  - **igmp**—Enable incoming Internet Group Management Protocol (IGMP) traffic.
  - **ldp**—Enable incoming Label Distribution Protocol (LDP) traffic (UDP and TCP port 646).
  - **msdp**—Enable incoming Multicast Source Discovery Protocol (MSDP) traffic.
  - **nhrp**—Enable incoming Next Hop Resolution Protocol (NHRP) traffic.
  - **ospf**—Enable incoming OSPF traffic.
  - **ospf3**—Enable incoming OSPF version 3 traffic.
  - **pgm**—Enable incoming Pragmatic General Multicast (PGM) protocol traffic (IP protocol number 113).
  - **pim**—Enable incoming Protocol Independent Multicast (PIM) traffic.
  - **rip**—Enable incoming RIP traffic.
  - **ripng**—Enable incoming RIP next generation traffic.
  - **router-discovery**—Enable incoming router discovery traffic.
  - **rsvp**—Enable incoming Resource Resolution Protocol (RSVP) traffic (IP protocol number 46).
  - **sap**— Enable incoming Session Announcement Protocol (SAP) traffic. SAP always listens on **224.2.127.254:9875**.
  - **vrrp**—Enable incoming Virtual Router Redundancy Protocol (VRRP) traffic.

**except**—(Optional) except can only be used if all has been defined.


Copyright © 2013, Juniper Networks, Inc.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Zones and Interfaces for Security Devices

## proxy (Security Antivirus)

**Syntax**

```
proxy {
  password password-string;
  port port-number;
  server address-or-url;
  username name;
}
```

**Hierarchy Level**
[edit security utm feature-profile anti-virus juniper-express-engine pattern-update]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]
[edit security utm feature-profile anti-virus sophos-engine pattern-update]

**Release Information**
Statement introduced in Release 11.2 of Junos OS.

**Description**
Update the pattern file on the proxy server.

**Options**
The remaining statements are explained separately.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## proxy-arp (Security NAT)

**Syntax**

```
proxy-arp {
  interface interface-name {
    address ip-address {
      to ip-address;
    }
  }
}
```

**Hierarchy Level** [edit security nat]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Configure Address Resolution Protocol (ARP) proxy.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

## proxy-identity

**Syntax**

```
proxy-identity {
  local ip-prefix;
  remote ip-prefix;
  service (all | service-name);
}
```

**Hierarchy Level** [edit security ipsec vpn *vpn-name* ike]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Optionally specify the IPsec proxy ID to use in negotiations. The default behavior is to use the identities taken from the firewall policies.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## proxy-ndp (Security NAT)

**Syntax**

```
proxy-ndp {
  interface interface-name {
    address ip-address {
      to ip-address;
    }
  }
}
```

**Hierarchy Level** [edit security nat]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Configure Neighbor Discovery Protocol (NDP) proxy.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

## quarantine-message (Security UTM)

**Syntax**

```
quarantine-message {
  type {
    custom-redirect-url;
  }
  url url;
}
```

**Hierarchy Level** [edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name*]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10 for Enhanced Web Filtering.

**Description** Configure Juniper enhanced quarantine message settings.

**Options**
- **type**—Specify the following type of the quarantine message:
  - **custom-redirect-url**—Specify Custom redirect URL server.
- **url *url***—Specify an URL of the quarantine message.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## raise-threshold

**Syntax** raise-threshold *raise-threshold*;

**Hierarchy Level** [edit security nat source pool-utilization-alarm]

**Release Information** Statement modified in Junos OS Release 9.2.

**Description** Configure the upper threshold at which an SNMP trap is triggered when pool utilization for a source pool without Port Address Translation (PAT) rises above the threshold. This feature is disabled by default.

**Options** ***raise-threshold*** —Threshold at which an SNMP trap is triggered.
**Range:** 50 through 100

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

## range-address

**Syntax** range-address *lower-limit* to *upper-limit*;

**Hierarchy Level** [edit security address-book address *address-name*]

**Release Information** Statement introduced in Release 12.1 of Junos OS.

**Description** Configure the address range for an address book.

**Options**
- **lower-limit**—Lower limit of an address range.
- **upper-limit**—Upper limit of an address range.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Address Books and Address Sets for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## rate-limit (Security GTP)

**Syntax** rate-limit *value*;

**Hierarchy Level** [edit security gprs gtp profile *profile-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS. Support for GTPv2 added in Release 11.4 of Junos OS.

**Description** Set the limit rate of control traffic to any GSN defined in a GTP profile.

**Options** **Range:** 1 through 80,000 messages per second.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- General Packet Radio Service for Security Devices

## re-assembler

**Syntax**
```
re-assembler {
  (ignore-memory-overflow | no-ignore-memory-overflow);
  (ignore-reassembly-memory-overflow | no-ignore-reassembly-memory-overflow);
  ignore-reassembly-overflow;
  max-flow-mem value;
  max-packet-mem value;
}
```

**Hierarchy Level** [edit security idp sensor-configuration]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Configure TCP reassembler for IDP sensor settings.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## re-enroll-trigger-time-percentage (Security PKI)

**Syntax** re-enroll-trigger-time-percentage *percentage*;

**Hierarchy Level** [edit security pki auto-re-enrollment certificate-id *certificate-id-name*]

**Release Information** Statement modified in Release 9.0 of Junos OS.

**Description** Specify the time before expiration as a percentage.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Certificates and Public Key Cryptography for Security Devices

## re-generate-keypair

**Syntax** <re-generate-keypair>;

**Hierarchy Level** [edit security pki auto-re-enrollment certificate-id]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** (Optional) Automatically generate a new key pair when auto-reenrolling a router certificate. If this statement is not configured, the current key pair is used.

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Documentation**
- Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA
- auto-re-enrollment
- Example: Using SCEP to Automatically Renew a Local Certificate


Copyright © 2013, Juniper Networks, Inc.

## real

**Syntax**

```
real {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the RealAudio and RealVideo ALG on the device.

**Options**

- **disable**—Disable the RealAudio and RealVideo ALG.
- **traceoptions**—Configure Real ALG tracing options.
  - **flag**—Trace operation to perform.
    - **all**—Trace all events.
    - ***extensive***—Display extensive amount of data.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

## recommended

**Syntax** recommended;

**Hierarchy Level** [edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify recommended filter to add predefined attacks recommended by Juniper Networks to the dynamic attack group.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## recommended-action

**Syntax** recommended-action (close | close-client | close-server | drop | drop-packet | ignore | none);

**Hierarchy Level** [edit security idp custom-attack *attack-name*]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** When the security device detects an attack, it performs the specified action.

**Options** The seven actions are as follows, from most to least severe:

- **close**—Reset the client and the server.
- **close-client**—Reset the client.
- **close-server**—Reset the server.
- **drop**—Drop the particular packet and all subsequent packets of the flow.
- **drop-packet**—Drop the particular packet of the flow.
- **ignore**—Do not inspect any further packets.
- **none**—Do not perform any action.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## redirect-wx (Application Services)

**Syntax** redirect-wx;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Define the acceleration zone security policy for WX redirection of packets to the WXC Integrated Service Module (ISM 200) for WAN acceleration. During the redirection process, the direction of the WX packet and its type determine further processing of the packet.

Specify the WX redirection needed for the packets that arrive from the LAN. Use the **reverse-redirect-wx** statement to specify the WX redirection needed for the reverse flow of the packets that arrive from the WAN.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## refresh-timeout

**Syntax** refresh-timeout;

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* then ip-action]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then ip-action]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Refresh the ip-action timeout so it does not expire when future connections match the installed ip-action filter.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- Application-Level Distributed Denial of Service
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## regexp

**Syntax** regexp *regular-expression*;

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify a Perl Compatible Regular Expression (PCRE) expression.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## reject (Security)

**Syntax** reject;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Block the service at the firewall. The device drops the packet and sends a TCP reset (RST) segment to the source host for TCP traffic and an ICMP “destination unreachable, port unreachable” message (type 3, code 3) for UDP traffic. For types of traffic other than TCP and UDP, the device drops the packet without notifying the source host, which is also what occurs when the action is **deny**.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## reject-timeout

**Syntax** reject-timeout *value*;

**Hierarchy Level** [edit security idp sensor-configuration flow]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify the amount of time in milliseconds within which a response must be received.

**Options** *value*—Maximum amount of time in milliseconds.
**Range:** 1 through 65,535 milliseconds
**Default:** 300 milliseconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## remote (Security IPsec)

**Syntax** remote *ip-prefix*;

**Hierarchy Level** [edit security ipsec vpn *vpn-name* ike proxy-identity]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS.

**Description** Specify the remote IPv4 or IPv6 address and subnet mask for the proxy identity.

**Options** *ip-prefix* —IPv4 or IPv6 address and subnet mask.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## remote-exceptions

**Syntax** remote-exceptions *ip-address/mask*;

**Hierarchy Level** [edit security dynamic-vpn clients *configuration-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Use this statement to specify exceptions to the remote protected resources list for the specified dynamic VPN configuration. Traffic to the specified IP address will not go through the dynamic VPN tunnel and therefore will not be protected by the firewall's security policies.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Dynamic VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## remote-identity

**Syntax**

```
remote-identity {
    (distinguished-name <container container-string> <wildcard wildcard-string> | hostname
      hostname | inet ip-address | inet6 ipv6-address | user-at-hostname e-mail-address);
}
```

**Hierarchy Level** [edit security ike gateway *gateway-name*]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Specify the remote IKE identity to exchange with the destination peer to establish communication. If you do not configure a remote-identity, the device uses the IPv4 or IPv6 address corresponding to the remote endpoint by default. (The **distinguished-name** option is not supported on dynamic VPN implementations.)



NOTE: For Network Address Translation Traversal (NAT-T), both remote identity and local identity must be configured.

**Options**

- **distinguished-name**—Specify identity as the distinguished name (DN) from the certificate. If there is more than one certificate on the device, use the **security ike gateway *gateway-name* policy *policy-name* certificate local-certificate *certificate-id***.

  Optional container and wildcard strings may be specified:

  - **container *container-string***—Specify a string for the container.
  - **wildcard *wildcard-string***—Specify a string for the wildcard.

- **hostname *hostname***—Specify identity as a fully qualified domain name (FQDN).
- **inet *ip-address***—Specify identity as an IPv4 address.
- **inet6 *ipv6-address***—Specify identity as an IPv6 address.
- **user-at-hostname *e-mail-address***—Specify identity as an e-mail address.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## remote-protected-resources

**Syntax** remote-protected-resources *ip-address/mask*;

**Hierarchy Level** [edit security dynamic-vpn clients *configuration-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Use this statement to specify which resources to protect using the dynamic VPN feature. Traffic to the protected resource will go through the specified dynamic VPN tunnel and will therefore be protected by the firewall's security policies.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Dynamic VPNs for Security Devices

## remove-ie

**Syntax**
```
remove-ie {
  version v1 {
  number ie-number;
  release (R6 | R7 | R8 | R9);
  }
}
```

**Hierarchy Level** [edit security gprs gtp profile *profile-name*]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Enable the security device to detect and remove 3G-specific attributes from the GTP packet header when the packet passes into a 2G network. This allows you to retain interoperability when roaming between 2G and 3G networks.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- General Packet Radio Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## replay-attacks

**Syntax**

```
replay-attacks {
  threshold value;
}
```

**Hierarchy Level** [edit security alarms potential-violation]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Raise a security alarm when the device detects a replay attack. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

**Default** Replay attacks do not raise security alarms.

**Options**

- **threshold *value***—Number of reply attacks up to which an alarm is not raised. When the configured number is exceeded, an alarm is raised.

  **Range:** Range: 0 through 100,00,00,000.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

## reset (Security IDP)

**Syntax**

```
reset;
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type chain]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Select **reset** if the compound attack should be matched more than once within a single session or transaction.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## reset-on-policy

**Syntax** (reset-on-policy | no-reset-on-policy);

**Hierarchy Level** [edit security idp sensor-configuration flow]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** IDP keeps track of connections in a table. If enabled, the security module resets the flow table each time a security policy loads or unloads. If this setting is disabled, then the security module continues to retain a previous security policy until all flows referencing that security policy go away. Juniper Networks recommends that you keep this setting enabled to preserve memory.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## resource-manager

**Syntax**
```
resource-manager {
  traceoptions {
    flag flag;
  }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced before Release 12.1 of Junos OS.

**Description** Configure resource manager security options.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Flow-Based Processing for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## respond-bad-spi

**Syntax** respond-bad-spi <*max-responses*>;

**Hierarchy Level** [edit security ike]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable response to invalid IPsec Security Parameter Index (SPI) values. If the security associations (SAs) between two peers of an IPsec VPN become unsynchronized, the device resets the state of a peer so that the two peers are synchronized.

**Options** ***max-responses***—Number of times to respond to invalid SPI values per gateway.

**Range:** 1 through 30

**Default:** 5

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## restart-path

**Syntax** restart-path (all | create | echo);

**Hierarchy Level** [edit security gprs gtp profile *profile-name*]

**Release Information** Statement introduced in Release 11.4 of Junos OS. Support for GTPv2 added in Release 11.4 of Junos OS.

**Description** Restart a GTP path. Restarting a GTP path deletes all GTP tunnels between two devices.

**Options**
- **all**—Restart GTP paths by detecting the changed restart number obtained from the Recovery information element (IE) in all GTP messages.
- **create**—Restart GTP paths by detecting the changed restart number obtained from the Recovery IE in create-session messages.
- **echo**—Restart GTP paths by detecting the changed restart number obtained from the Recovery IE in echo messages.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- General Packet Radio Service for Security Devices

## retain-hold-resource

**Syntax** retain-hold-resource;

**Hierarchy Level** [edit security alg sip]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable the device to not free media resources for a Session Initiation Protocol (SIP) Application Layer Gateway (ALG), even when a media stream is placed on hold. By default, media stream resources are released when the media stream is held.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- SIP ALGs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## revocation-check (Security PKI)

**Syntax**

```
revocation-check {
  crl {
    disable {
      on-download-failure;
    }
    refresh-interval hours;
    url url-name;
  }
  disable;
}
```

**Hierarchy Level** [edit security pki ca-profile *ca-profile-name*]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Specify the method the device uses to verify the revocation status of digital certificates.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Certificates and Public Key Cryptography for Security Devices

## route-change-timeout

**Syntax** route-change-timeout *seconds*;

**Hierarchy Level** [edit security flow]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the session timeout value on a route change to a nonexistent route. By default, this feature is disabled. If the timeout is not defined, sessions discovered to have no route are aged out by means of their current session timeout values.

**Options** ***seconds*** —Amount of time before sessions with no route are aged out.

**Range:** 6 through 1800 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Flow-Based Processing for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## routing-instance (Security Destination NAT)

**Syntax** routing-instance *routing-instance-name*;

**Hierarchy Level** [edit security nat destination pool *pool-name*]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify the routing instance on which to perform the route lookup for the address in the pool. It is not a mandatory flag.

A destination NAT pool that does not specify a specific routing instance will default to the routing instance of the ingress zone. You can configure a NAT pool to exist in the default routing instance. As a result, the NAT pool is reachable from zones in the default routing instance and from zones in other routing instances.

**Options** ***routing-instance-name***—Name of the routing instance.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

## routing-instance (Security PKI)

**Syntax** routing-instance *routing-instance-name*

**Hierarchy Level** [edit security pki ca-profile *ca-profile-name*]

**Release Information** Statement modified in Release 9.0 of Junos OS.

**Description** Specify the routing-instance to be used.

**Options**
- ***routing-instance-name***—Name of the routing instance.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Certificates and Public Key Cryptography for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## routing-instance (Security Source NAT)

**Syntax** routing-instance *routing-instance-name*;

**Hierarchy Level** [edit security nat source pool *pool-name*]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify the routing instance to which the pool is bound. It is not a mandatory flag. If the user does not configure the routing instance, by default the pool belongs to routing-instance **inet.0**.

**Options** ***routing-instance-name***—Name of the routing instance.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## routing-engine (SNMP) Global Level

**Syntax**

```
routing-engine
  {
    interval <interval in secs>;
    moderate-threshold <percentage level>;
    high-threshold <percentage level>;
    critical-threshold <percentage level>;
    traceoptions;
  }
```

**Hierarchy Level** [edit snmp health-monitor routing-engine]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Enable the system health management feature to use the specified parameters.

**Options**

- **interval**—Monitoring interval in seconds.

  Default: 300 seconds
- **moderate-threshold**—Percentage of moderate threshold level resource utilization.

  Default: 70 percent.
- **high-threshold** —Percentage of high-threshold level resource utilization.

  Default: 80 percent.
- **critical-threshold** —Percentage of critical threshold level resource utilization.

  Default: 90 percent.
- **history**—Enable or disable the history of logging support.
- **traceoptions**—Enable tracing of system health monitoring daemon.



NOTE: If these configuration parameters are not available, the default parameters are used.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Device and Routing Operations Monitoring


Copyright © 2013, Juniper Networks, Inc.

## routing-engine (SNMP) Resource Level

**Syntax**

```
routing-engine {
  resource <cpu | memory | open-files-count-process | storage | temperature> ;
  {
    interval <interval in secs>;
    moderate-threshold <percentage level>;
    high-threshold <percentage level>;
    critical-threshold <percentage level>;
  }
}
```

**Hierarchy Level** [edit snmp health-monitor routing-engine]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Override the global configuration for a resource.

**Options**

- **interval**—Monitoring interval in seconds.

  Default: 300 seconds

- **moderate-threshold**—Percentage of moderate threshold level resource utilization.

  Default: 70 percent.

- **high-threshold** —Percentage of high-threshold level resource utilization.

  Default: 80 percent.

- **critical-threshold** —Percentage of critical threshold level resource utilization.

  Default: 90 percent.



NOTE: If these configuration parameters are not available, the global configuration is used.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Device and Routing Operations Monitoring

Copyright © 2013, Juniper Networks, Inc.

## rpc

**Syntax**

```
rpc {
  program-number rpc-program-number;
}
```

**Hierarchy Level**

[edit security idp custom-attack *attack-name* attack-type chain protocol-binding]
[edit security idp custom-attack *attack-name* attack-type signature protocol-binding]

**Release Information**

Statement introduced in Release 9.3 of Junos OS.

**Description**

Allow IDP to match the attack for a specified remote procedure call (RPC) program number.

**Options**

**program-number *rpc-program-number***—RPC program number.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## rsh

**Syntax**

```
rsh {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the remote shell (RSH) ALG on the device.

**Options**

- **disable**—Disable the RSH ALG. By default, the RSH ALG is enabled.
- **traceoptions**—Configure RSH ALG tracing options.
  - **flag**—Trace operation to perform.
    - **all**—Trace all events.
    - ***extensive***—Display extensive amount of data.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

## rst-invalidate-session

**Syntax** rst-invalidate-session;

**Hierarchy Level** [edit security flow tcp-session]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable the device to mark a session for immediate termination when it receives a TCP reset (RST) message. By default, this feature is disabled and the device applies the normal session timeout interval. For TCP, normal session timeout is 30 minutes; for HTTP, it is 5 minutes; and for UDP, it is 1 minute.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Flow-Based Processing for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## rst-sequence-check

**Syntax** rst-sequence-check;

**Hierarchy Level** [edit security flow tcp-session]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Verify that the TCP sequence number in a TCP segment with the RST bit enabled matches the previous sequence number for a packet in that session or is the next higher number incrementally. If the sequence number does not match either of these expected numbers, the device drops the packet and sends the host a TCP ACK message with the correct sequence number. By default, this check is disabled.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Flow-Based Processing for Security Devices

## rtsp

**Syntax**
```
rtsp {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the Real-Time Streaming Protocol (RTSP) ALG on the device.

**Options**
- **disable**—Disable the RTSP ALG. By default, the RTSP ALG is enabled.
- **traceoptions**—Configure RTSP ALG tracing options.
  - **flag**—Trace operation to perform.
    - **all**—Trace all events.
    - ***extensive***—Display extensive amount of data.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policy Applications for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## rule (Security DDoS Rulebase)

**Syntax**

```
rule rule-name {
  description text;
  match {
    application (application-name | any | default);
    application-ddos <application-name>;
    destination-address ([address-name] | any | any-ipv4 | any-ipv6);
    destination-except [address-name];
    from-zone (zone-name | any);
    source-address ([address-name] | any | any-ipv4 | any-ipv6);
    source-except [address-name];
    to-zone (zone-name | any);
  }
  then {
    action {
      (close-server | drop-connection | drop-packet | no-action);
    }
    ip-action {
      (ip-block | ip-close | ip-connection-rate-limit connections-per-second | ip-notify);
      log;
      log-create;
      refresh-timeout;
      timeout seconds;
    }
    notification {
      log-attacks {
        alert;
      }
    }
  }
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure application-level DDoS rule match criteria, and the action to be taken on attack clients.

**Options** *rule-name*—Name of the DDoS rulebase rule.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## rule (Security Destination NAT)

**Syntax**

```
rule rule-name {
  description text;
  match {
    (destination-address <ip-address> | destination-address-name <address-name>);
    destination-port port-number;
    protocol [protocol-name-or-number];
    source-address [ip-address];
    source-address-name [address-name];
  }
  then {
    destination-nat (off | pool pool-name);
  }
}
```

**Hierarchy Level** [edit security nat destination rule-set *rule-set-name*]

**Release Information** Statement introduced in Junos OS Release 9.2. The **description** option added in Junos OS Release 12.1.

**Description** Define a destination NAT rule.

**Options**

- ***rule-name***—Name of the destination NAT rule.
- **description**—Description of the destination NAT rule.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## rule (Security Exempt Rulebase)

**Syntax**

```
rule rule-name {
  description text;
  match {
    attacks {
      custom-attack-groups [attack-group-name];
      custom-attacks [attack-name];
      dynamic-attack-groups [attack-group-name];
      predefined-attack-groups [attack-group-name];
      predefined-attacks [attack-name];
    }
    destination-address ([address-name] | any | any-ipv4 | any-ipv6);
    destination-except [address-name];
    from-zone (zone-name | any );
    source-address ([address-name] | any | any-ipv4 | any-ipv6);
    source-except [address-name];
    to-zone (zone-name | any);
  }
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-exempt]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify exempt rule to create, modify, delete, and reorder the rules in a rulebase.

**Options** ***rule-name***—Name of the exempt rulebase rule.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## rule (Security IPS Rulebase)

**Syntax**

```
rule rule-name {
  description text;
  match {
    application (application-name | any | default);
    attacks {
      custom-attack-groups [attack-group-name];
      custom-attacks [attack-name];
      dynamic-attack-groups [attack-group-name];
      predefined-attack-groups [attack-group-name];
      predefined-attacks [attack-name];
    }
    destination-address ([address-name] | any | any-ipv4 | any-ipv6);
    destination-except [address-name];
    from-zone (zone-name | any );
    source-address ([address-name] | any | any-ipv4 | any-ipv6);
    source-except [address-name];
    to-zone (zone-name | any);
  }
  terminal;
  then {
    action {
      class-of-service {
        dscp-code-point number;
        forwarding-class forwarding-class;
      }
      (close-client | close-client-and-server | close-server |drop-connection | drop-packet
        | ignore-connection | mark-diffserv value | no-action | recommended);
    }
    ip-action {
      (ip-block | ip-close | ip-notify);
      log;
      log-create;
      refresh-timeout;
      target (destination-address | service | source-address | source-zone |
        source-zone-address | zone-service);
      timeout seconds;
    }
    notification {
      log-attacks {
        alert;
      }
      packet-log {
        post-attack number;
        post-attack-timeout seconds;
        pre-attack number;
      }
    }
    severity (critical | info | major | minor | warning);
  }
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ips]


Copyright © 2013, Juniper Networks, Inc.

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify IPS rule to create, modify, delete, and reorder the rules in a rulebase.

**Options** ***rule-name***—Name of the IPS rulebase rule.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## rule (Security Source NAT)

**Syntax**

```
rule rule-name {
  description text;
  match {
    (destination-address <ip-address> | destination-address-name <address-name>);
    destination-port port-number;
    protocol [protocol-name-or-number];
    source-address [ip-address];
    source-address-name [address-name];
  }
  then {
    source-nat {
      interface {
        persistent-nat {
          address-mapping;
          inactivity-timeout seconds;
          max-session-number value;
          permit (any-remote-host | target-host | target-host-port);
        }
      }
      off;
      pool {
        persistent-nat {
          address-mapping;
          inactivity-timeout seconds;
          max-session-number number;
          permit (any-remote-host | target-host | target-host-port);
        }
        pool-name;
      }
    }
  }
}
```

**Hierarchy Level** [edit security nat source rule-set *rule-set-name*]

**Release Information** Statement modified in Junos OS Release 9.6. The **description** option added in Junos OS Release 12.1.

**Description** Define a source NAT rule.

**Options**

- ***rule-name***—Name of the source NAT rule.
- **description**—Description of the source NAT rule.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## rule (Security Static NAT)

**Syntax**

```
rule rule-name {
  description text;
  match {
    (destination-address ip-address | destination-address-name address-name);
    destination-port lower-port-range to upper-port-range;
  }
  then {
    static-nat {
      inet {
        routing-instance (default | routing-instance-name);
      }
      prefix {
        address-prefix;
        mapped-port lower-port-range to upper-port-range;
        routing-instance (default | routing-instance-name);
      }
      prefix-name {
        address-prefix-name;
        mapped-port lower-port-range to upper-port-range;
        routing-instance (default | routing-instance-name);
      }
    }
  }
}
```

**Hierarchy Level** [edit security nat static rule-set *rule-set-name*]

**Release Information** Statement introduced in Junos OS Release 9.3. The **description** option added in Junos OS Release 12.1.

**Description** Define a static NAT rule.

**Options**

- ***rule-name***—Name of the static NAT rule.
- **Description**—Description of the static NAT rule.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## rule-set (Security Destination NAT)

**Syntax**

```
rule-set rule-set-name {
  description text;
  from {
    interface [interface-name];
    routing-instance [routing-instance-name];
    zone [zone-name];
  }
  rule rule-name {
    description text;
    match {
      (destination-address <ip-address> | destination-address-name <address-name>);
      destination-port port-number;
      protocol [protocol-name-or-number];
      source-address [ip-address];
      source-address-name [address-name];
    }
    then {
      destination-nat (off | pool pool-name);
    }
  }
}
```

**Hierarchy Level** [edit security nat destination]

**Release Information** Statement modified in Junos OS Release 9.6. The **description** option added in Junos OS Release 12.1.

**Description** Configure a set of rules for destination NAT.

**Options**

- ***rule-set-name***—Name of the rule set.
- **description**—Description of the rule set.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## rule-set (Security Source NAT)

**Syntax**

```
rule-set rule-set-name {
  description text;
  from {
    interface [interface-name];
    routing-instance [routing-instance-name];
    zone [zone-name];
  }
  rule rule-name {
    description text;
    match {
      (destination-address <ip-address> | destination-address-name <address-name>);
      destination-port port-number;
      protocol [protocol-name-or-number];
      source-address [ip-address];
      source-address-name [address-name];
    }
    then {
      source-nat {
        interface {
          persistent-nat {
            address-mapping;
            inactivity-timeout seconds;
            max-session-number value;
            permit (any-remote-host | target-host | target-host-port);
          }
        }
        off;
        pool {
          persistent-nat {
            address-mapping;
            inactivity-timeout seconds;
            max-session-number number;
            permit (any-remote-host | target-host | target-host-port);
          }
          pool-name;
        }
      }
    }
  }
  to {
    interface [interface-name];
    routing-instance [routing-instance-name];
    zone [zone-name];
  }
}
```

**Hierarchy Level** [edit security nat source]

**Release Information** Statement modified in Junos OS Release 9.6. The **description** option added in Junos OS Release 12.1.

**Description** Configure a set of rules for source NAT.

Copyright © 2013, Juniper Networks, Inc.

**Options**

- ***rule-set-name***—Name of the rule set.
- **description**—Description of the rule set.

The remaining statements are explained separately.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## rule-set (Security Static NAT)

**Syntax**

```
rule-set rule-set-name {
  description text;
  from {
    interface [interface-name];
    routing-instance [routing-instance-name];
    zone [zone-name];
  }
  rule rule-name {
    description text;
    match {
      (destination-address ip-address | destination-address-name address-name);
      destination-port lower-port-range to upper-port-range;
    }
    then {
      static-nat {
        inet {
          routing-instance (default | routing-instance-name);
        }
        prefix {
          address-prefix;
          mapped-port lower-port-range to upper-port-range;
          routing-instance (default | routing-instance-name);
        }
        prefix-name {
          address-prefix-name;
          mapped-port lower-port-range to upper-port-range;
          routing-instance (default | routing-instance-name);
        }
      }
    }
  }
}
```

**Hierarchy Level** [edit security nat static]

**Release Information** Statement modified in Junos OS Release 9.6. The **description** option added in Junos OS Release 12.1.

**Description** Configure a set of rules for static NAT.

**Options** ***rule-set-name*** —Name of the rule set.

**Description**—Description of the rule set.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## rule-sets (Security Application Firewall)

**Syntax**

```
rule-sets rule-set-name {
  default-rule {
    (deny | permit | reject);
  }
  rule rule-name {
    match {
      dynamic-application [system-application];
      dynamic-application-groups [system-application-group];
      ssl-encryption (any | yes | no);
    }
    then {
      (deny | permit | reject);
    }
  }
}
```

**Hierarchy Level** [edit security application-firewall]

**Release Information** Statement introduced in Junos OS Release 11.1. Statement updated in Junos OS Release 12.1X44-D10 to include the **ssl-encryption** and **reject** options.

**Description** Configure the set of rules for the application firewall.

**Options** *rule-set-name*—Name of the rule set.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Firewall


Copyright © 2013, Juniper Networks, Inc.

## rulebase-ddos

**Syntax**

```
rulebase-ddos {
  rule rule-name {
    description text;
    match {
      application (application-name | any | default);
      application-ddos <application-name>;
      destination-address ([address-name] | any | any-ipv4 | any-ipv6);
      destination-except [address-name];
      from-zone (zone-name | any);
      source-address ([address-name] | any | any-ipv4 | any-ipv6);
      source-except [address-name];
      to-zone (zone-name | any);
    }
    then {
      action {
        (close-server | drop-connection | drop-packet | no-action);
      }
      ip-action {
        (ip-block | ip-close | ip-connection-rate-limit connections-per-second | ip-notify);
        log;
        log-create;
        refresh-timeout;
        timeout seconds;
      }
      notification {
        log-attacks {
          alert;
        }
      }
    }
  }
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure the rulebase parameters for application-level DDoS attacks.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## rulebase-exempt

**Syntax**

```
rulebase-exempt {
  rule rule-name {
    description text;
    match {
      attacks {
        custom-attack-groups [attack-group-name];
        custom-attacks [attack-name];
        dynamic-attack-groups [attack-group-name];
        predefined-attack-groups [attack-group-name];
        predefined-attacks [attack-name];
      }
      destination-address ([address-name] | any | any-ipv4 | any-ipv6);
      destination-except [address-name];
      from-zone (zone-name | any );
      source-address ([address-name] | any | any-ipv4 | any-ipv6);
      source-except [address-name];
      to-zone (zone-name | any);
    }
  }
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name*]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Configure the exempt rulebase to skip detection of a set of attacks in certain traffic.



NOTE: You must configure the IPS rulebase before configuring the exempt rulebase.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## rulebase-ips

**Syntax**

```
rulebase-ips {
  rule rule-name {
    description text;
    match {
      application (application-name | any | default);
      attacks {
        custom-attack-groups [attack-group-name];
        custom-attacks [attack-name];
        dynamic-attack-groups [attack-group-name];
        predefined-attack-groups [attack-group-name];
        predefined-attacks [attack-name];
      }
      destination-address ([address-name] | any | any-ipv4 | any-ipv6);
      destination-except [address-name];
      from-zone (zone-name | any );
      source-address ([address-name] | any | any-ipv4 | any-ipv6);
      source-except [address-name];
      to-zone (zone-name | any);
    }
    terminal;
    then {
      action {
        class-of-service {
          dscp-code-point number;
          forwarding-class forwarding-class;
        }
        (close-client | close-client-and-server | close-server |drop-connection | drop-packet
          | ignore-connection | mark-diffserv value | no-action | recommended);
      }
      ip-action {
        (ip-block | ip-close | ip-notify);
        log;
        log-create;
        refresh-timeout;
        target (destination-address | service | source-address | source-zone |
          source-zone-address | zone-service);
        timeout seconds;
      }
      notification {
        log-attacks {
          alert;
        }
        packet-log {
          post-attack number;
          post-attack-timeout seconds;
          pre-attack number;
        }
      }
      severity (critical | info | major | minor | warning);
    }
  }
}
```

Copyright © 2013, Juniper Networks, Inc.

**Hierarchy Level** [edit security idp idp-policy *policy-name*]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Configure the IPS rulebase to detect attacks based on stateful signature and protocol anomalies.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices
- IDP Class of Service Action for Security Devices

## sbl

**Syntax**

```
sbl {
  profile profile-name {
    custom-tag-string [string];
    (sbl-default-server | no-sbl-default-server);
    spam-action (block | tag-header | tag-subject);
  }
}
```

**Hierarchy Level** [edit security utm feature-profile anti-spam]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure UTM server-based antispam features.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## sbl-default-server

**Syntax** sbl-default-server;

**Hierarchy Level** [edit security utm feature-profile anti-spam sbl profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Enable the default SBL server lookup. You should enable this feature if you are using server-based spam filtering. (The SBL server is predefined on the device. It ships with the name and address of the SBL server.)

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

## scan-extension

**Syntax** scan-extension *filename*;

**Hierarchy Level** [edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* scan-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** For antivirus file extension scanning, configure the scan extension setting by specifying the name of the defined file extension list.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## scan-mode

**Syntax** scan-mode (all | by-extension);

**Hierarchy Level** [edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* scan-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** You can scan all content or scan content with specific file extensions. You can use a file extension list to define a set of file extensions that are used in file extension scan mode. The antivirus module can then only scan files with extensions on the scan-extension list.

**Options**
- **all**—Scan all files.
- **by-extension**—Scan only files with extensions specified in a file extension list custom object.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## scan-options (Security Antivirus Juniper Express Engine)

**Syntax**
```
scan-options {
  content-size-limit value;
  (intelligent-prescreening | no-intelligent-prescreening);
  timeout value;
}
```

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure the antivirus feature to scan specific types of traffic based on various scanning configuration parameters.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## scan-options (Security Antivirus Kaspersky Lab Engine)

**Syntax**

```
scan-options {
  content-size-limit value;
  decompress-layer-limit value;
  (intelligent-prescreening | no-intelligent-prescreening);
  scan-extension filename;
  scan-mode (all | by-extension);
  timeout value;
}
```

**Hierarchy Level** [edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure the antivirus feature to scan specific types of traffic based on various scanning configuration parameters.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## scan-options (Security Antivirus Sophos Engine)

**Syntax**

```
scan-options {
  content-size-limit value;
  (no-uri-check | uri-check);
  timeout value;
}
```

**Hierarchy Level** [edit security utm feature-profile anti-virus sophos-engine profile *profile-name*]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Configure the antivirus feature to scan specific types of traffic based on various scanning configuration parameters.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## sccp

**Syntax**

```
sccp {
  application-screen {
    call-flood {
      threshold rate;
    }
    unknown-message {
      permit-nat-applied;
      permit-routed;
    }
  }
  disable;
  dscp-rewrite {
    code-point string;
  }
  inactive-media-timeout value-in-seconds;
  traceoptions {
    flag flag <extensive>;
  }
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the Skinny Client Control Protocol (SCCP) ALG on the device.

**Options** **disable**—Disable the SCCP ALG. By default, the SCCP ALG is enabled.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- SCCP ALGs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## scheduler-name

**Syntax** scheduler-name *scheduler-name*;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name*]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the schedule (as defined by the **scheduler** ***scheduler-name*** statement) for which the policy is in effect.

**Options** ***scheduler-name*** —Name of the scheduler.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## scope (Security IDP Chain Attack)

**Syntax** scope (session | transaction);

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type chain]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify whether the match should occur over a single session or can be made across multiple transactions within a session.

**Options**
- **session**—Allow multiple matches for the object within the same session.
- **transaction**—Match the object across multiple transactions that occur within the same session.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## scope (Security IDP Custom Attack)

**Syntax** scope (destination | peer | source);

**Hierarchy Level** [edit security idp custom-attack *attack-name* time-binding]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify whether the counting of the attack is from the same source IP address, the same destination IP address, or a peer.

**Options**

- **destination**—IDP detects attacks to a given destination IP address for the specified number of times, regardless of the source IP address.
- **peer**—IDP detects attacks between source and destination IP addresses of the sessions for the specified number of times.
- **source**—IDP detects attacks from a given source IP address for the specified number of times, regardless of the destination IP address.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## screen (Security)

**Syntax**

```
screen {
    ids-option screen-name {
        alarm-without-drop;
        description text;
        icmp {
            flood {
                threshold number;
            }
            fragment;
            ip-sweep {
                threshold number;
            }
            large;
            ping-death;
        }
        ip {
            bad-option;
            block-frag;
            loose-source-route-option;
            record-route-option;
            security-option;
            source-route-option;
            spoofing;
            stream-option;
            strict-source-route-option;
            tear-drop;
            timestamp-option;
            unknown-protocol;
        }
        limit-session {
            destination-ip-based number;
            source-ip-based number;
        }
        tcp {
            fin-no-ack;
            land;
            port-scan {
                threshold number;
            }
            syn-ack-ack-proxy {
                threshold number;
            }
            syn-fin;
            syn-flood {
                alarm-threshold number;
                attack-threshold number;
                destination-threshold number;
                source-threshold number;
                timeout seconds;
                white-list name {
                    destination-address destination-address;
                    source-address source-address;
```

Copyright © 2013, Juniper Networks, Inc.

```
            }
          }
          syn-frag;
          tcp-no-flag;
          tcp-sweep {
            threshold threshold number;
          }
          winnuke;
        }
        udp {
          flood {
            threshold number;
          }
          udp-sweep {
            threshold threshold number;
          }
        }
      }
    }
    traceoptions {
      file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
      }
      flag flag;
      no-remote-trace;
    }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Release 8.5 of Junos OS. The **description** option added in Release 12.1 of Junos OS.

**Description** Configure security screen options.

**Options** *screen-name*—Name of the screen configured at the **security screen ids-options** level.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Logical Systems for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## screen (Security Zones)

**Syntax** screen *screen-name*;

**Hierarchy Level** [edit security zones functional-zone management],
[edit security zones security-zone *zone-name*]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify a security screen for a security zone.

**Options** ***screen-name*** —Name of the screen.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Zones and Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## sctp

**Syntax**

```
sctp {
  log {
    configuration;
    decoding-error;
    dropped-packet;
    exceeding-rate-limit;
  }
  profile profile-name {
    association-timeout time-in-minutes;
    drop {
      m3ua-service {
        isup;
        sccp;
        tup;
      }
      payload-protocol {
        all;
        asap;
        bicc;
        ddp-segment;
        ddp-stream;
        dua;
        enrp;
        h248;
        h323;
        iua;
        m2pa;
        m2ua;
        m3ua;
        qipc;
        reserved;
        simco;
        sua;
        tali;
        v5ua;
      }
    }
    handshake-timeout time-in-seconds;
    limit {
      rate {
        address ip-address {
          sccp rate-limit;
          ssp rate-limit;
          sst rate-limit;
        }
        sccp rate-limit;
        ssp rate-limit;
        sst rate-limit;
      }
    }
  }
  traceoptions {
```


Copyright © 2013, Juniper Networks, Inc.

```
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
```

**Hierarchy Level** [edit security gprs]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Use the Stream Control Transmission Protocol (SCTP) commands to configure SCTP objects, configure SCTP logs, set trace options, and set address rate limit.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- General Packet Radio Service for Security Devices

## security-log-percent-full

**Syntax** security-log-percent-full *percentage*;

**Hierarchy Level** [edit security alarms potential-violation]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Raise a security alarm when security log exceeds a specified percent of total capacity.

**Options** *percentage*—Percentage of security log capacity at which a security alarm is raised.
**Range:** 0 through 100 percent

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- System Log Messages
- Security Logs

Copyright © 2013, Juniper Networks, Inc.

## security-package

**Syntax**

```
security-package {
  automatic {
    download-timeout minutes;
    enable;
    interval hours;
    start-time start-time;
  }
  install {
    ignore-version-check;
  }
  source-address address;
  url url-name;
}
```

**Hierarchy Level** [edit security idp]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Configure the device to automatically download the updated signature database from the specified URL.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices
- IDP Signature Database for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## security-zone

**Syntax**

```
security-zone zone-name {
  address-book {
    address address-name {
      ip-prefix {
        description text;
      }
      description text;
      dns-name domain-name {
        ipv4-only;
        ipv6-only;
      }
      range-address lower-limit to upper-limit;
      wildcard-address ipv4-address/wildcard-mask;
    }
    address-set address-set-name {
      address address-name;
      address-set address-set-name;
      description text;
    }
  }
  application-tracking;
  description text;
  host-inbound-traffic {
    protocols protocol-name {
      except;
    }
    system-services service-name {
      except;
    }
  }
  interfaces interface-name {
    host-inbound-traffic {
      protocols protocol-name {
        except;
      }
      system-services service-name {
        except;
      }
    }
  }
  screen screen-name;
  tcp-rst;
}
```

**Hierarchy Level** [edit security zones]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for wildcard addresses added in Release 11.1 of Junos OS. The **description** option added in Release 12.1 of Junos OS.

**Description** Define a security zone, which allows you to divide the network into different segments and apply different security options to each segment.

Copyright © 2013, Juniper Networks, Inc.

**Options**

***zone-name*** —Name of the security zone.

The remaining statements are explained separately.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- Application Tracking


Copyright © 2013, Juniper Networks, Inc.

## sensor-configuration

**Syntax**

```
sensor-configuration {
  application-ddos {
    statistics {
      interval minutes;
    }
  }
  application-identification {
    max-packet-memory value;
    max-tcp-session-packet-memory value;
    max-udp-session-packet-memory value;
  }
  detector {
    protocol-name protocol-name {
      tunable-name  tunable-name {
        tunable-value protocol-value;
      }
    }
  }
  flow {
    (allow-icmp-without-flow | no-allow-icmp-without-flow);
    fifo-max-size value;
    hash-table-size value;
    (log-errors | no-log-errors);
    max-timers-poll-ticks value;
    reject-timeout value;
    (reset-on-policy | no-reset-on-policy);
    udp-anticipated-timeout value;
  }
  global {
    (enable-all-qmodules | no-enable-all-qmodules);
    (enable-packet-pool | no-enable-packet-pool);
    gtp (decapsulation | no-decapsulation);
    memory-limit-percent value;
    (policy-lookup-cache | no-policy-lookup-cache);
  }
  high-availability {
    no-policy-cold-synchronization;
  }
  ips {
    content-decompression-max-memory-kb value;
    content-decompression-max-ratio value;
    (detect-shellcode | no-detect-shellcode);
    fifo-max-size value;
    (ignore-regular-expression | no-ignore-regular-expression);
    log-supercede-min minimum-value;
    pre-filter-shellcode;
    (process-ignore-s2c | no-process-ignore-s2c);
    (process-override | no-process-override);
    process-port port-number;
  }
  log {
    cache-size size;
```

Copyright © 2013, Juniper Networks, Inc.

```
    suppression {
      disable;
      (include-destination-address | no-include-destination-address);
      max-logs-operate value;
      max-time-report value;
      start-log value;
    }
  }
  packet-log {
    host ip-address <port number>;
    max-sessions percentage;
    source-address ip-address;
    total-memory percentage;
  }
  re-assembler {
    (ignore-memory-overflow | no-ignore-memory-overflow);
    (ignore-reassembly-memory-overflow | no-ignore-reassembly-memory-overflow);
    ignore-reassembly-overflow;
    max-flow-mem value;
    max-packet-mem value;
  }
  ssl-inspection {
    cache-prune-chunk-size number;
    key-protection;
    maximum-cache-size number;
    session-id-cache-timeout seconds;
    sessions number;
  }
}
```

**Hierarchy Level** [edit security idp]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Configure various IDP parameters to match the properties of transiting network traffic.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## sequence-check-required

**Syntax** sequence-check-required;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit tcp-options]

**Release Information** Statement introduced in Junos OS Release 10.4.

**Description** Enable sequence check per policy. The sequence-check-required value overrides the global value no-sequence-check.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## sequence-number (Security IDP ICMP Headers)

**Syntax**
```
sequence-number {
    match (equal | greater-than | less-than | not-equal);
    value sequence-number;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol icmp]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the sequence number of the packet. This number identifies the location of the request/reply in relation to the entire sequence.

**Options**
- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***sequence-number***—Match a decimal value.

  **Range:** 0 through 65,535

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## sequence-number (Security IDP TCP Headers)

**Syntax**

```
sequence-number {
  match (equal | greater-than | less-than | not-equal);
  value sequence-number;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the sequence number of the packet. This number identifies the location of the data in relation to the entire data sequence.

**Options**

- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***sequence-number***—Match a decimal value.

  **Range:** 0 through 4,294,967,295

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## server (Security Antivirus)

**Syntax** server *address-or-url*;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine pattern-update proxy]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update proxy]
[edit security utm feature-profile anti-virus sophos-engine pattern-update proxy]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Set the IP address or URL for the proxy server.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- Unified Threat Management


Copyright © 2013, Juniper Networks, Inc.

## server (Security Group VPN)

**Syntax**

```
server {
  group name {
    activation-time-delay seconds;
    anti-replay-time-window seconds;
    description description;
    group-id number;
    ike-gateway gateway-name;
    ipsec-sa name {
      match-policy policy-name {
        destination ip-address/netmask;
        destination-port number;
        protocol number;
        source ip-address/netmask;
        source-port number;
      }
      proposal proposal-name;
    }
    no-anti-replay;
    server-address ip-address;
    server-member-communication {
      certificate certificate-id;
      communication-type (multicast | unicast);
      encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
      heartbeat seconds;
      lifetime-seconds seconds;
      multicast-group address;
      multicast-outgoing-interface interface;
      number-of-retransmission number;
      retransmission-period seconds;
      sig-hash-algorithm (md5 | sha1);
    }
  }
  ike {
    gateway gateway-name {
      address ip-address-or-hostname;
      dynamic {
        (distinguished-name <container container-string> <wildcard wildcard-string> |
          hostname domain-name | inet ip-address | user-at-hostname e-mail-address);
      }
      ike-policy policy-name;
      local-identity {
        (distinguished-name | hostname hostname | inet ip-address | user-at-hostname
          e-mail-address);
      }
    }
    policy policy-name {
      certificate {
        local-certificate certificate-id;
        peer-certificate-type [pkcs7 | x509-signature);
      }
      description description;
      mode (aggressive | main);
```

Copyright © 2013, Juniper Networks, Inc.

```
        pre-shared-key (ascii-text key | hexadecimal key);
        proposal-set (basic | compatible | standard);
        proposals [proposal-name];
      }
      proposal proposal-name {
        authentication-algorithm (md5 | sha-256 | sha1);
        authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
        description description;
        dh-group (group1 | group14 | group2 | group5);
        encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
      }
    }
    ipsec {
      proposal proposal-name {
        authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
        description description;
        encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
        lifetime-seconds seconds;
      }
    }
    traceoptions {
      file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
      }
      flag flag;
      no-remote-trace;
    }
}
```

**Hierarchy Level** [edit security group-vpn]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure group VPN server. You configure the following on the group server:

- Phase 1 IKE SA for group members
- Phase 2 IPsec proposal
- Group identifier, group members, server-member communications, and group policies to be downloaded to members
- Group VPN trace options

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## server (Security Web Filtering)

**Syntax**

```
server {
    host host-name;
    port number;
}
```

**Hierarchy Level**

[edit security utm feature-profile web-filtering surf-control-integrated]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name*]
[edit security utm feature-profile web-filtering juniper-enhanced]

**Release Information**

Statement introduced in Release 9.5 of Junos OS.
Statement introduced in Release 11.4 of Junos OS for Enhanced Web Filtering.

**Description**

Set server parameters by entering the server name or IP address.

**Options**

The remaining statements are explained separately.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## server-connectivity

**Syntax** server-connectivity (block | log-and-permit);

**Hierarchy Level**
[edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name* fallback-settings]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name* fallback-settings]
[edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name* fallback-settings]

**Release Information** Statement introduced in Release 9.5 of Junos OS.
Statement introduced in Release 11.4 of Junos OS for Enhanced Web Filtering.

**Description** Fallback settings tell the system how to handle errors. This is the action that occurs when a request fails for this reason.

**Options**
- block—Log the error and deny the traffic
- log-and-permit—Log the error and permit the traffic

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## server-member-communication

**Syntax**

```
server-member-communication {
  certificate certificate-id;
  communication-type (multicast | unicast);
  encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
  heartbeat seconds;
  lifetime-seconds seconds;
  multicast-group address;
  multicast-outgoing-interface interface;
  number-of-retransmission number;
  retransmission-period seconds;
  sig-hash-algorithm (md5 | sha1);
}
```

**Hierarchy Level** [edit security group-vpn server group *name*]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Enable and configure server to member communication. When these options are configured, group members receive new keys before current keys expire. These options also enable members to receive heartbeat messages from the server; members can detect server reboots when heartbeats are missed.

**Options**

- **certificate** ***certificate-id***—Specify the certificate identification. Only RSA keys are supported.
- **communication-type**—Configure **unicast** (the default) or **multicast**. If **multicast** is specified, you need to specify an IPv4 multicast address for the **multicast-group** option.
- **encryption-algorithm**—Encryption used for communications between the group server and group member. Specify **3des-cbc**, **aes-128-cbc**, **aes-192-cbc**, **aes-256-cbc**, or **des-cbc**.
- **heartbeat** ***seconds***— Interval, in seconds, at which the group server sends heartbeats to the group member. Specify a value from 60 to 3600. The default is 300 seconds.
- **lifetime-seconds** ***seconds***—Lifetime, in seconds, of the key encryption key (KEK). Specify a value from 180 to 86,400. The default is 3600 seconds.
- **multicast-group** ***address***—If **communication-type** is **multicast**, specify the multicast address for the group.
- **multicast-outgoing-interface** ***interface***—If **communication-type** is multicast, specify the name of the interface on which multicast packets are sent.
- **number-of-retransmission** ***number***—For unicast communications, the number of times the group server retransmits messages to a group member when there is no reply. For multicast communications, the number of copies of a message the group server sends to group members. Specify a value from 0 to 60. The default is 2.
- **retransmission-period** ***seconds***—The time period between a transmission and the first retransmission when there is no reply from the group member. Specify a value from 2 to 60. The default is 4 seconds.

Copyright © 2013, Juniper Networks, Inc.

- **sig-hash-algorithm**—Authentication algorithm used to authenticate the group member to the group server. Specify **md5** or **sha1**.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPNs for Security Devices

## service (Security IDP Anomaly Attack)

**Syntax** service *service-name*;

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type anomaly]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Service is the protocol whose anomaly is defined in the attack. IP, TCP, UDP, and ICMP are also valid as services. (Protocol names must be entered in lower case.)

**Options** ***service-name***—Name of the protocol in lower case.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## service (Security IDP DDoS)

**Syntax** service *service-name*;

**Hierarchy Level** [edit security idp application-ddos *application-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Defines the Application Layer service to be monitored for application-level DDoS attacks, such as DNS or HTTP.

**Options** ***service-name***—Name of the application layer protocol in lower case.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application-Level Distributed Denial of Service


Copyright © 2013, Juniper Networks, Inc.

## service (Security IDP Dynamic Attack Group)

**Syntax**

```
service {
  values [service-value];
}
```

**Hierarchy Level** [edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify a service filter to add attack objects based on the attack service, such as FTP, HTTP, NetBios, and so on.

**Options** **values**—Name of the service filter. You can configure multiple filters separated by spaces and enclosed in square brackets.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## service (Security IPsec)

**Syntax** service (all | *service-name*);

**Hierarchy Level** [edit security ipsec vpn *vpn-name* ike proxy-identity]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the service (port and protocol combination) to protect.

**Options** ***service-name*** —Name of the service, as defined with **system-services** (**Interface Host-Inbound Traffic**) and **system-services** (**Zone Host-Inbound Traffic**).

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## services-offload (Security)

**Syntax** services-offload;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit]

**Release Information** Statement introduced in Junos OS Release 11.4.

**Description** Enable services offloading within a security policy.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## session-affinity

**Syntax** session-affinity ipsec

**Hierarchy Level** [edit security flow load-distribution]

**Release Information** Statement introduced in Junos OS Release 11.4R5.

**Description** Enable VPN session affinity.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IPsec VPNs for Security Devices

## session-close

**Syntax** session-close;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then log]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Enable traffic to which the policy applies to be logged at the end of a session.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## session-distribution-mode

**Syntax**
```
session-distribution-mode {
  hash-based;
}
```

**Hierarchy Level** [edit security forwarding-process application-services]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Enable the **session-distribution-mode** option to change the mechanism that a central point uses to distribute sessions to SPUs.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Processing Overview for Security Devices

## session-id-cache-timeout

**Syntax** session-id-cache-timeout *seconds*;

**Hierarchy Level** [edit security idp sensor-configuration ssl inspection]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Sets the timeout value for an IDP session ID cache (range: 1 through 7200 seconds).

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

Copyright © 2013, Juniper Networks, Inc.

## session-init

**Syntax** session-init;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then log]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Enable traffic to which the policy applies to be logged at the beginning of a session.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## session-update-interval

**Syntax** session-update-interval *session-update-interval*;

**Hierarchy Level** [edit security application-tracking]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the interval between session update messages for long-lived sessions being monitored by AppTrack. Byte count, packet count, and start and end times are updated and logged when the amount of time between session start or the previous update and the current time exceeds the interval.

**Options** ***session-update-interval***—Minutes between updates.
**Default:** 5

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Tracking


Copyright © 2013, Juniper Networks, Inc.

## sessions

**Syntax** sessions *number*;

**Hierarchy Level** [edit security idp sensor-configuration ssl-inspection]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Maximum number of SSL sessions for inspection. This limit is per Services Processing Unit (SPU).

**Options** ***number***—Number of SSL session to inspect.

**Range:** 1 through 100000

**Default:** 10000

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## sessions-per-client

**Syntax**

```
sessions-per-client {
   limit value;
   over-limit (block | log-and-permit);
}
```

**Hierarchy Level** [edit security utm utm-policy *policy-name* traffic-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM Basics for Security Devices
- Unified Threat Management

Copyright © 2013, Juniper Networks, Inc.

## severity (Security IDP Custom Attack)

**Syntax** severity (critical | info | major | minor | warning);

**Hierarchy Level** [edit security idp custom-attack *attack-name*]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Select the severity that matches the lethality of the attack object on your network.

**Options** You can set the severity level to the following levels:

- **critical**—Contains attack objects matching exploits that attempt to evade detection, cause a network device to crash, or gain system-level privileges.
- **info**—Contains attack objects matching normal, harmless traffic containing URLs, DNS lookup failures, SNMP public community strings, and Peer-to-Peer (P2P) parameters. You can use informational attack objects to obtain information about your network.
- **major**—Contains attack objects matching exploits that attempt to disrupt a service, gain user-level access to a network device, or activate a Trojan horse previously loaded on a device.
- **minor**—Contains attack objects matching exploits that detect reconnaissance efforts attempting to access vital information through directory traversal or information leaks.
- **warning**—Contains attack objects matching exploits that attempt to obtain noncritical information or scan a network with a scanning tool.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## severity (Security IDP Dynamic Attack Group)

**Syntax**

```
severity {
  values [critical info major minor warning];
}
```

**Hierarchy Level** [edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify a severity filter to add attack objects based on the attack severity.

**Options** **values**—Name of the severity filter. You can select from the following severity:

- **critical**—The attack is a critical one.
- **info**—Provide information of attack when it matches.
- **major**—The attack is a major one.
- **minor**—The attack is a minor one.
- **warning**—Issue a warning when attack matches.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## severity (Security IDP IPS Rulebase)

**Syntax** severity (critical | info | major | minor | warning);

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Set the rule severity levels in logging to support better organization and presentation of log records on the log server. You can use the default severity settings of the selected attack object, or choose a specific severity for your rule. The severity you configure in the rules overrides the inherited attack severity.

**Options** You can set the severity level to the following levels:

- **critical**—2
- **info**—3
- **major**—4
- **minor**—5
- **warning**—7

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## severity (Security Log)

**Syntax** severity (alert | critical | debug | emergency | error | info | notice | warning)

**Hierarchy Level** [edit security log stream *stream-name*]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Set severity threshold for security logs.

**Options**

- **alert**— Conditions that require immediate attention.
- **critical**—Critical conditions.
- **debug**—Information normally used in debugging.
- **emergency**—Conditions that cause security functions to stop.
- **error**—General error conditions.
- **info**—Information about normal security operations.
- **notice**—Nonerror conditions that are of interest.
- **warning**—General warning conditions.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- System Log Messages
- Security Logs

Copyright © 2013, Juniper Networks, Inc.

## shellcode

**Syntax** shellcode (all | intel | no-shellcode | sparc);

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type anomaly]
[edit security idp custom-attack *attack-name* attack-type signature]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Shellcode signifies that the attack is a shellcode attack and is capable of creating its own shell.

**Options**

- **all**—All shellcode checks will be performed if this attack matches.
- **intel**—Basic shellcode checks and Intel-specific shellcode checks will be performed.
- **no-shellcode**—No shellcode checks will be performed.
- **sparc**—Basic shellcode checks and Sparc-specific shellcode checks will be performed.

**Default:** Basic shellcode checks will be performed when this field is not configured.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## signature (Security IDP)

**Syntax**

```
signature {
    context context-name;
    direction (any | client-to-server | server-to-client);
    negate;
    pattern signature-pattern;
    protocol {
        icmp {
            code {
                match (equal | greater-than | less-than | not-equal);
                value code-value;
            }
            data-length {
                match (equal | greater-than | less-than | not-equal);
                value data-length;
            }
            identification {
                match (equal | greater-than | less-than | not-equal);
                value identification-value;
            }
            sequence-number {
                match (equal | greater-than | less-than | not-equal);
                value sequence-number;
            }
            type {
                match (equal | greater-than | less-than | not-equal);
                value type-value;
            }
        }
        ipv4 {
            destination {
                match (equal | greater-than | less-than | not-equal);
                value ip-address-or-hostname;
            }
            identification {
                match (equal | greater-than | less-than | not-equal);
                value identification-value;
            }
            ip-flags {
                (df | no-df);
                (mf | no-mf);
                (rb | no-rb);
            }
            protocol {
                match (equal | greater-than | less-than | not-equal);
                value transport-layer-protocol-id;
            }
            source {
                match (equal | greater-than | less-than | not-equal);
                value ip-address-or-hostname;
            }
            tos {
                match (equal | greater-than | less-than | not-equal);
```

Copyright © 2013, Juniper Networks, Inc.

```
        value type-of-service-in-decimal;
    }
    total-length {
        match (equal | greater-than | less-than | not-equal);
        value total-length-of-ip-datagram;
    }
    ttl {
        match (equal | greater-than | less-than | not-equal);
        value time-to-live;
    }
}
ipv6 {
    destination {
        match (equal | greater-than | less-than | not-equal);
        value ip-address-or-hostname;
    }
    flow-label {
        match (equal | greater-than | less-than | not-equal);
        value flow-label-value;
    }
    hop-limit {
        match (equal | greater-than | less-than | not-equal);
        value hop-limit-value;
    }
    next-header {
        match (equal | greater-than | less-than | not-equal);
        value next-header-value;
    }
    payload-length {
        match (equal | greater-than | less-than | not-equal);
        value payload-length-value;
    }
    source {
        match (equal | greater-than | less-than | not-equal);
        value ip-address-or-hostname;
    }
    traffic-class {
        match (equal | greater-than | less-than | not-equal);
        value traffic-class-value;
    }
tcp {
    ack-number {
        match (equal | greater-than | less-than | not-equal);
        value acknowledgement-number;
    }
    data-length {
        match (equal | greater-than | less-than | not-equal);
        value tcp-data-length;
    }
    destination-port {
        match (equal | greater-than | less-than | not-equal);
        value destination-port;
    }
    header-length {
        match (equal | greater-than | less-than | not-equal);
        value header-length;
```


Copyright © 2013, Juniper Networks, Inc.

```
        }
        mss {
            match (equal | greater-than | less-than | not-equal);
            value maximum-segment-size;
        }
        option {
            match (equal | greater-than | less-than | not-equal);
            value tcp-option;
        }
        sequence-number {
            match (equal | greater-than | less-than | not-equal);
            value sequence-number;
        }
        source-port {
            match (equal | greater-than | less-than | not-equal);
            value source-port;
        }
        tcp-flags {
            (ack | no-ack);
            (fin | no-fin);
            (psh | no-psh);
            (r1 | no-r1);
            (r2 | no-r2);
            (rst | no-rst);
            (syn | no-syn);
            (urg | no-urg);
        }
        urgent-pointer {
            match (equal | greater-than | less-than | not-equal);
            value urgent-pointer;
        }
        window-scale {
            match (equal | greater-than | less-than | not-equal);
            value window-scale-factor;
        }
        window-size {
            match (equal | greater-than | less-than | not-equal);
            value window-size;
        }
    }
    udp {
        data-length {
            match (equal | greater-than | less-than | not-equal);
            value data-length;
        }
        destination-port {
            match (equal | greater-than | less-than | not-equal);
            value destination-port;
        }
        source-port {
            match (equal | greater-than | less-than | not-equal);
            value source-port;
        }
    }
}
protocol-binding {
```

```
    application application-name;
    icmp;
    icmpv6;
    ip {
      protocol-number transport-layer-protocol-number;
    }
    ipv6 {
      protocol-number transport-layer-protocol-number;
    }
    nested-application nested-application-name;
    rpc {
      program-number rpc-program-number;
    }
    tcp {
      minimum-port port-number <maximum-port port-number>;
    }
    udp {
      minimum-port port-number <maximum-port port-number>;
    }
  }
  regexp regular-expression;
  shellcode (all | intel | no-shellcode | sparc);
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** IDP uses stateful signatures to detect attacks. Stateful signatures are more specific than regular signatures. With stateful signatures, IDP can look for the specific protocol or service used to perpetrate the attack.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## sip (Security)

**Syntax**

```
sip {
  application-screen {
    protect {
      deny {
        all {
          timeout value-in-seconds;
        }
        destination-ip address;
        timeout value-in-seconds;
      }
    }
    unknown-message {
      permit-nat-applied;
      permit-routed;
    }
  }
  c-timeout value-in-minutes;
  disable;
  dscp-rewrite {
    code-point string;
  }
  inactive-media-timeout value-in-seconds;
  maximum-call-duration value-in-minutes;
  retain-hold-resource;
  t1-interval value-in-milliseconds;
  t4-interval value-in-seconds;
  traceoptions {
    flag flag <detail | extensive | terse>;
  }
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Specify the Session Initiation Protocol (SIP) ALG on the device.

**Options** **disable**—Disable the SIP ALG. Use CLI command **set security alg *alg-name* disable** to disable the SIP ALG.

The remaining statements are explained separately.



NOTE: By default, the SIP ALG is disabled for SRX1400, SRX3400, SRX3600, SRX5600 and SRX5800 devices. Use CLI command **delete security alg *alg-name* disable** to enable the SIP ALG.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Copyright © 2013, Juniper Networks, Inc.

**Related Documentation**
- SIP ALGs for Security Devices

## site-reputation-action

**Syntax**

```
site-reputation-action {
  harmful (block | log-and-permit | permit | quarantine);
  fairly-safe (block | log-and-permit | permit | quarantine);
  moderately-safe (block | log-and-permit | permit | quarantine);
  suspicious (block | log-and-permit | permit | quarantine);
  very-safe (block | log-and-permit | permit | quarantine);
}
```

**Hierarchy Level** [edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name* category *category-name*]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Specify the action to be taken depending on the site reputation returned for all types of URLs whether it is categorized or uncategorized.

**Options**

**fairly-safe** —Permit, log-and-permit, block or quarantine a request if a site-reputation of 70 through 79 is returned.

**harmful**—Permit, log-and-permit, block or quarantine a request if a site-reputation of zero through 59 is returned.

**moderately-safe**—Permit, log-and-permit, block or quarantine a request if a site-reputation of 80 through 89 is returned.

**suspicious**—Permit, log-and-permit, block or quarantine a request if a site-reputation of 60 through 69 is returned.

**very-safe**—Permit, log-and-permit, block or quarantine a request if a site-reputation of 90 through 100 is returned.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## size (Security Web Filtering Cache)

**Syntax** size *value*;

**Hierarchy Level** [edit security utm feature-profile web-filtering surf-control-integrated cache]
[edit security utm feature-profile web-filtering juniper-enhanced cache]

**Release Information** Statement introduced in Release 9.5 of Junos OS.
Statement introduced in Release 11.4 of Junos OS for Enhanced Web Filtering.

**Description** Set the cache size parameters for web filtering.

**Options** **Range:** 0 through 4096 kilobytes.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

## smtp-profile (Security UTM Policy Antispam)

**Syntax** smtp-profile *profile-name*;

**Hierarchy Level** [edit security utm utm-policy *policy-name* anti-spam]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the antispam SMTP protocol and attach this policy to a security profile to implement it.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices
- Unified Threat Management

Copyright © 2013, Juniper Networks, Inc.

## smtp-profile (Security UTM Policy Antivirus)

**Syntax** smtp-profile *profile-name*;

**Hierarchy Level** [edit security utm utm-policy *policy-name* anti-virus]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the antivirus SMTP protocol and attach this policy to a security profile to implement it.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## smtp-profile (Security UTM Policy Content Filtering)

**Syntax** smtp-profile *profile-name*;

**Hierarchy Level** [edit security utm utm-policy *policy-name* content-filtering]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the content-filtering SMTP protocol and attach this policy to a security profile to implement it.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## sockets

**Syntax** sockets *value*;

**Hierarchy Level** [edit security utm feature-profile web-filtering websense-redirect profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Enter the number of sockets used for communicating between the client and server. The default is 1.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## softwires

**Syntax**

```
softwires {
  softwire-name name {
    softwire-concentrator ipv6-address;
    softwire-type IPv4-in-IPv6;
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag (all | configuration | flow);
    no-remote-trace;
  }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced before Release 12.1 of Junos OS.

**Description** Configure softwires for IPv6 dual-stack lite (DS-Lite). DS-Lite allows migration to an IPv6 access network without changing end-user software. IPv4 users can continue to access IPv4 internet content using their current hardware, while IPv6 users are able to access IPv6 content.

**Options**

- **softwire-name *name***—Name of the softwire configuration.
  - **softwire-concentrator *ipv6-address***—IPv6 address of the concentrator.
  - **softwire-type**—Must be IPv4-in-IPv6.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Logical Systems for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## sophos-engine

**Syntax**

```
sophos-engine {
  pattern-update {
    email-notify {
      admin-email email-address;
      custom-message message;
      custom-message-subject message-subject;
    }
    interval value;
    no-autoupdate;
    proxy {
      password password-string;
      port port-number;
      server address-or-url;
      username name;
    }
    url url;
  }
  profile <name> {
    fallback-options {
      content-size (block | log-and-permit | permit);
      default (block | log-and-permit | permit);
      engine-not-ready (block | log-and-permit | permit);
      out-of-resources (block | log-and-permit | permit);
      timeout (block | log-and-permit | permit);
      too-many-requests (block | log-and-permit | permit);
    }
    notification-options {
      fallback-block {
        administrator-email email-address;
        allow-email;
        custom-message message;
        custom-message-subject message-subject;
        display-host;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
      fallback-non-block {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-recipient | no-notify-mail-recipient);
      }
      virus-detection {
        custom-message message;
        custom-message-subject message-subject;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
    }
    scan-options {
      content-size-limit value;
      (no-uri-check | uri-check);
      timeout value;
```

Copyright © 2013, Juniper Networks, Inc.

```
    }
    trickling {
      timeout value;
    }
  }
  sxl-retry value;
  sxl-timeout seconds;
}
```

**Hierarchy Level** [edit security utm feature-profile anti-virus]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Configure the UTM Sophos antivirus feature.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

## source (Security IDP IP Headers)

**Syntax**

```
source {
  match (equal | greater-than | less-than | not-equal);
  value ip-address-or-hostname;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol ipv4]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the IP address of the attacking device.

**Options**
- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***ip-address-or-hostname***—Match an ip-address or a host name.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## source (Security Source NAT)

**Syntax**

```
source {
    address-persistent;
    interface {
        port-overloading {
            off;
        }
    }
    pool pool-name {
        address ip-address {
            to ip-address;
        }
        description text;
        host-address-base ip-address;
        overflow-pool (interface | pool-name);
        port {
            (no-translation | port-overloading-factor number | range port-low <to port-high>);
        }
        routing-instance routing-instance-name;
    }
    pool-default-port-range lower-port-range to upper-port-range;
    pool-utilization-alarm {
        clear-threshold value;
        raise-threshold value;
    }
    port-randomization {
        disable;
    }
    rule-set rule-set-name {
        description text;
        from {
            interface [interface-name];
            routing-instance [routing-instance-name];
            zone [zone-name];
        }
        rule rule-name {
            description text;
            match {
                (destination-address <ip-address> | destination-address-name <address-name>);
                destination-port port-number;
                protocol [protocol-name-or-number];
                source-address [ip-address];
                source-address-name [address-name];
            }
            then {
                source-nat {
                    interface {
                        persistent-nat {
                            address-mapping;
                            inactivity-timeout seconds;
                            max-session-number value;
                            permit (any-remote-host | target-host | target-host-port);
                        }
```

Copyright © 2013, Juniper Networks, Inc.

```
                }
                off;
                pool {
                  persistent-nat {
                    address-mapping;
                    inactivity-timeout seconds;
                    max-session-number number;
                    permit (any-remote-host | target-host | target-host-port);
                  }
                  pool-name;
                }
              }
            }
          }
          to {
            interface [interface-name];
            routing-instance [routing-instance-name];
            zone [zone-name];
          }
        }
      }
```

**Hierarchy Level** [edit security nat]

**Release Information** Statement modified in Junos OS Release 9.6. The **description** option added in Junos OS Release 12.1.

**Description** Configure source NAT, which allows you to configure the following:

- Translate source IP address or addresses to the egress interface's IP address.
- Translate a range of source IP addresses to another range of IP addresses. This mapping is dynamic and without PAT.
- Translate a range of source IP addresses to another range of IP addresses. This mapping is dynamic and with PAT.
- Translate a range of source IP addresses to another range of IP addresses. This mapping is one-to-one, static, and without PAT.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## source-address (Security Destination NAT)

**Syntax** source-address [*ip-address*];

**Hierarchy Level** [edit security nat destination rule-set *rule-set-name* rule *rule-name* match]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify source address to match the rule. You can configure multiple addresses or subnets.

**Options** ***ip-address*** —Source address or a subnet.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

## source-address (Security IDP)

**Syntax** source-address *address*;

**Hierarchy Level** [edit security idp security-package]

**Description** Sets the source address to be used for sending download requests.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Signature Database for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## source-address (Security IDP Policy)

**Syntax** source-address ([*address-name*] | any | any-ipv4 | any-ipv6);

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* match]
[edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Junos 10.0.

**Description** Specify a source IP address or IP address set object to be used as the match source address object. The default value is any.

**Options**
- ***address-name***—IP address or IP address set object.
- ***any***—Specify any IPv4 or IPv6 address.
- ***any-ipv4***—Specify any IPv4 address.
- ***any-ipv6***—Specify any IPv6 address.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- Application-Level Distributed Denial of Service
- IDP Application Identification for Security Devices

## source-address (Security IDP Sensor Configuration)

**Syntax** source-address *ip-address*;

**Hierarchy Level** [edit security idp sensor-configuration packet-log]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the source IP address for the carrier UDP packet.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## source-address (Security Policies)

**Syntax**

```
source-address {
    [address];
    any;
    any-ipv4;
    any-ipv6;
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]

**Release Information** Statement introduced in Junos OS Release 8.5. Support for IPv6 addresses added in Junos OS Release 10.2. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Junos OS Release 10.4. Support for wildcard addresses added in Junos OS Release 11.1.

**Description** Define the matching criteria. You can specify one or more IP addresses, address sets, or wildcard addresses. You can specify wildcards **any**, **any-ipv4**, or **any-ipv6**.

**Options**

***address***—IP addresses, address sets, or wildcard addresses (represented as A.B.C.D/wildcard-mask). You can configure multiple addresses or address prefixes separated by spaces and enclosed in square brackets.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## source-address (Security Source NAT)

**Syntax** source-address [*ip-address*];

**Hierarchy Level** [edit security nat source rule-set *rule-set-name* rule *rule-name* match]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify source address to match the rule. You can configure multiple addresses or subnets.

**Options** ***ip-address***—Source address or a subnet.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

## source-address-name (Security Destination NAT)

**Syntax** source-address-name [*address-name*];

**Hierarchy Level** [edit security nat destination rule-set *rule-set-name* rule *rule-name* match]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify a source address name to match the rule. You can configure multiple address names.

**Options** ***address-name***—Source address name.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## source-address-name (Security Source NAT)

**Syntax** source-address-name [*address-name*];

**Hierarchy Level** [edit security nat source rule-set *rule-set-name* rule *rule-name* match]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify a source address name to match the rule. You can configure multiple address names.

**Options** ***address-name***—Source address name.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices

## source-except

**Syntax** source-except [*address-name*];

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* match]
[edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Release 10.0 of Junos OS.

**Description** Specify a source IP address or IP address set object to specify all source address objects except the specified address objects. The default value is any.

**Options** ***address-name***—IP address or IP address set object.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- Application-Level Distributed Denial of Service
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## source-identity

**Syntax**

```
source-identity {
  [user-or-role-name];
  any;
  authenticated-user;
  unauthenticated-user;
  unknown-user;
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]

**Release Information** Statement introduced in Junos OS Release 12.1. Statement updated in Junos OS Release 12.1X44-D10.

**Description** Identifies users and roles to be used as match criteria for a policy. If a value other than **any** is specified as match criteria for a policy within a zone pair, the traffic is matched to table entries to retrieve associated user and roles before policy lookup occurs. Users and roles are retrieved from the local authentication table or from a UIT pushed to the SRX Series device from an access control service when a user is authenticated.

The following entries specify the source identities that match a policy.

*user-or-role-name*—A list of specific users and roles.

any—All users and roles.

authenticated-user—Any user or role specified in an entry in the local authentication table or in the UIT.

unauthenticated-user—Any user or role that is not specified in an entry in the local authentication table or in the UIT.

unknown-user—Any user or role that cannot be determined because the local authentication table or UIT is not accessible, such as a system outage.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Understanding User Role Firewalls
- Understanding the User Identification Table
- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## source-interface (Security)

**Syntax** source-interface *interface-name* ;

**Hierarchy Level** [edit security ipsec vpn *vpn-name* vpn-monitor]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the source interface for ICMP requests (VPN monitoring “hellos” ). If no source interface is specified, the device automatically uses the local tunnel endpoint interface. (This statement is not supported on dynamic VPN implementations.)

**Options** *interface-name* —Name of the interface for the ICMP requests.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## source-ip (Security Alarms)

**Syntax**

```
source-ip {
  duration interval;
  size count;
  threshold value;
}
```

**Hierarchy Level** [edit security alarms potential-violation policy]

**Release Information** Statement introduced in Junos OS Release 11.2.

**Description** Configure alarms for a number of policy violations by a source network identifier within a specified time period.

**Options**

- **duration** ***interval***—Indicate the duration of counters.

  **Range:** 1 through 3600 seconds.
  **Default:** 1 second.

- **size** ***count***—Indicate the number of source IP addresses for which policy violation checks can be done concurrently.

  **Range:** 1 through 10240.
  **Default:** 1024.

- **threshold** ***value***—Indicate the maximum number of source IP address matches required to raise an alarm.

  **Range:** 1 through 4294967295.
  **Default:** 1000.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## source-ip-based

**Syntax** source-ip-based *number*;

**Hierarchy Level** [edit security screen ids-option *screen-name* limit-session ]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Limit the number of concurrent sessions the device can initiate from a single source IP address.

**Options** ***number*** —Maximum number of concurrent sessions that can be initiated from a source IP address.

**Range:** 1 through 1000000

**Default:** 128



NOTE: For SRX Series devices the applicable range is 1 through 8000000.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Configuration Statement Hierarchy

Copyright © 2013, Juniper Networks, Inc.

## source-nat

**Syntax**

```
source-nat {
  interface {
    persistent-nat {
      address-mapping;
      inactivity-timeout seconds;
      max-session-number value;
      permit (any-remote-host | target-host | target-host-port);
    }
  }
  off;
  pool {
    persistent-nat {
      address-mapping;
      inactivity-timeout seconds;
      max-session-number number;
      permit (any-remote-host | target-host | target-host-port);
    }
    pool-name;
  }
}
```

**Hierarchy Level** [edit security nat source rule-set *rule-set-name* rule *rule-name* then]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify the action of the source NAT rule.

**Options**

- **off**—Do not perform the source NAT operation.

The remaining statements are explained separately.

**Required Privilege Level** security — To view this statement in the configuration.
security-control— To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## source-port (Security IDP)

**Syntax**

```
source-port {
  match (equal | greater-than | less-than | not-equal);
  value source-port;
}
```

**Hierarchy Level**

[edit security idp custom-attack *attack-name* attack-type signature protocol udp]
[edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

**Release Information**

Statement introduced in Release 9.3 of Junos OS.

**Description**

Specify the port number on the attacking device.

**Options**

- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***source-port***—Port number on the attacking device.

  **Range:** 0 through 65,535

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## source-threshold

**Syntax** source-threshold *number*;

**Hierarchy Level** [edit security screen ids-option *screen-name* tcp syn-flood]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Specify the number of SYN segments that the device can receive per second from a single source IP address (regardless of the destination IP address and port number) before the device begins dropping connection requests from that source.

**Options** ***number*** —Number of SYN segments to be received per second before the device starts dropping connection requests.

**Range:** 4 through 500,000 per second

**Default:** 1024 per second



NOTE: For SRX Series devices the applicable range is 4 through 1,000,000 per second.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Configuration Statement Hierarchy

## spam-action

**Syntax** spam-action (block | tag-header | tag-subject);

**Hierarchy Level** [edit security utm feature-profile anti-spam sbl profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure the action to be taken by the device when spam is detected.

**Options**

- **block**— Block e-mail.
- **tag-header**—Tag header of e-mail.
- **tag-subject**—Tag subject of e-mail.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**


Copyright © 2013, Juniper Networks, Inc.

## spi (Security IPsec)

**Syntax** spi *spi-value*;

**Hierarchy Level** [edit security ipsec vpn *vpn-name* manual]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Configure a security parameter index (SPI) for a security association (SA). (This statement is not supported on dynamic VPN implementations.)

**Options** ***spi-value*** —An arbitrary value that uniquely identifies which security association (SA) to use at the receiving host (the destination address in the packet).

**Range:** 256 through 16639

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## sql

**Syntax**

```
sql {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the Oracle SQL ALG on the device.

**Options**

- **disable**—Disable the SQL ALG. By default, the SQL ALG is enabled.
- **traceoptions**—Configure SQL ALG tracing options.
  - **flag**—Trace operation to perform.
    - **all**—Trace all events.
    - ***extensive***—Display extensive amount of data.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Layer Gateways for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ssh-known-hosts

**Syntax**

```
ssh-known-hosts {
  fetch-from-server server-name;
  host hostname {
    dsa-key dsa-key;
    ecdsa-sha2-nistp256-key ecdsa-sha2-nistp256-key;
    ecdsa-sha2-nistp384-key ecdsa-sha2-nistp384-key;
    ecdsa-sha2-nistp521-key ecdsa-sha2-nistp521-key;
    rsa-key rsa-key;
    rsa1-key rsa1-key;
  }
  load-key-file key-file;
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Configure SSH support for known hosts and for administering SSH host key updates.

**Options**

- **fetch-from-server** ***server-name***—Retrieve SSH public host key information from a specified server.
- **load-key-file** ***key-file***—Import SSH host-key information from the specified **/var/tmp/ssh-known-hosts** file.

The remaining statements are explained separately

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Device Configuration

Copyright © 2013, Juniper Networks, Inc.

## ssl-encryption

**Syntax** ssl-encryption (any | no | yes);

**Hierarchy Level** [edit security application-firewall rule-sets *rule-set-name* rule *rule-name* match]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Distinguishes between encrypted and unencrypted SSL traffic as match criteria for the rule. In application firewall usage, this option lets you specify different actions for encrypted and unencrypted SSL traffic.

**Options**
- **any**—Matches both encrypted and unencrypted SSL traffic.
- **no**—Matches unencrypted SSL traffic only.
- **yes**—Matches encrypted SSL traffic only.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

## ssl-inspection

**Syntax**
```
ssl-inspection {
  cache-prune-chunk-size number;
  key-protection;
  maximum-cache-size number;
  session-id-cache-timeout seconds;
  sessions number;
}
```

**Hierarchy Level** [edit security idp sensor-configuration]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Inspect HTTP traffic encrypted in SSL protocol. SSL inspection is disabled by default. It is enabled if you configure ssl-inspection.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ssl-proxy (Application Services)

**Syntax**
```
ssl-proxy {
  profile-name profile-name
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]

**Release Information** Statement introduced in Junos OS Release 12.1.

**Description** Enable SSL proxy and identify the name of the SSL proxy profile to be used.

**Options** ***profile-name***—SSL proxy profile.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## ssl-termination-profile

**Syntax** ssl-termination-profile *profile-name*;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit firewall-authentication pass-through]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the SSL termination profile used for SSL offloading.

**Options** ***profile-name***—Specify the name of the SSL termination profile used to the SSL offload.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Copyright © 2013, Juniper Networks, Inc.

## start-log

**Syntax** start-log *value*;

**Hierarchy Level** [edit security idp sensor-configuration log suppression]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify how many instances of a specific event must occur before log suppression begins.

**Options** ***value***—Log suppression begins after how many occurrences.
**Range:** 1 through 128
**Default:** 1

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## start-time (Security IDP)

**Syntax** start-time *start-time*;

**Hierarchy Level** [edit security idp security-package automatic]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify the time that the device automatically starts downloading the updated signature database from the specified URL.

**Options** ***start-time***—Time in MM-DD.hh:mm format.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## static (Security NAT)

**Syntax**

```
static {
  rule-set rule-set-name {
    description text;
    from {
      interface [interface-name];
      routing-instance [routing-instance-name];
      zone [zone-name];
    }
    rule rule-name {
      description text;
      match {
        (destination-address ip-address | destination-address-name address-name);
        destination-port lower-port-range to upper-port-range;
      }
      then {
        static-nat {
          inet {
            routing-instance (default | routing-instance-name);
          }
          prefix {
            address-prefix;
              mapped-port lower-port-range to upper-port-range;
            routing-instance (default | routing-instance-name);
          }
          prefix-name {
            address-prefix-name;
            mapped-port lower-port-range to upper-port-range;
            routing-instance (default | routing-instance-name);
          }
        }
      }
    }
  }
}
```

**Hierarchy Level** [edit security nat]

**Release Information** Statement introduced in Junos OS Release 9.3. The **description** option added in Junos OS Release 12.1.

**Description** Configure static NAT.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## static-nat

**Syntax**

```
static-nat {
  inet {
    routing-instance (default | routing-instance-name);
  }
  prefix {
    address-prefix;
    routing-instance (default | routing-instance-name);
  }
  prefix-name {
    address-prefix-name;
    routing-instance (default | routing-instance-name);
  }
}
```

**Hierarchy Level** [edit security nat static rule-set *rule-set-name* rule *rule-name* then]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify the translated address of the static NAT rule.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## statistics (Security IDP)

**Syntax**

```
statistics {
  interval minutes;
}
```

**Hierarchy Level** [edit security idp sensor-configuration application-ddos]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** The statistics command will enable application-level DDoS statistic collection at the defined internal. Statistic report files are stored on the routing engine (RE) data storage device in /var/log/addos in comma separated value (CSV) format. The data storage device must have at least 2GB of free space before logging will occur.

**Options**

interval *minutes*—Set the interval in minutes that will define when application statistic will be collected.

**Range:** 1 through 60 minutes (1 minute increments)

**Default:** 1 minute

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## stream (Security Log)

**Syntax**

```
stream stream-name {
  category (all | content-security)
  format (binary | sd-syslog | syslog | welf)
  host {
    <ipaddr> ip-address;
    port port-number;
  }
  severity (alert | critical | debug | emergency | error | info | notice | warning);
}
```

**Hierarchy Level** [edit security log]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Set stream settings for a security log. You can set a maximum of three streams.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Tracking

## strict-syn-check

**Syntax** strict-syn-check;

**Hierarchy Level** [edit security flow tcp-session]

**Release Information** Statement introduced in Release 9.4 of Junos OS.

**Description** Enable the strict three-way handshake check for the TCP session. It enhances security by dropping data packets before the three-way handshake is done. By default, strict-syn-check is disabled.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Reconnaissance Deterrence for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## sunrpc

**Syntax**

```
sunrpc {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Specify the Sun Microsystems remote procedure call (RPC) ALG on the device.

**Options**

- **disable**—Disable the Sun RPC ALG. By default, the Sun RPC ALG is enabled.
- **traceoptions**—Configure Sun RPC ALG tracing options.
  - **flag**—Trace operation to perform.
    - **all**—Trace all events.
    - ***extensive***—Display extensive amount of data.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Copyright © 2013, Juniper Networks, Inc.

## suppression

**Syntax**

```
suppression {
  disable;
  (include-destination-address | no-include-destination-address);
  max-logs-operate value;
  max-time-report value;
  start-log value;
}
```

**Hierarchy Level** [edit security idp sensor-configuration log]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Log suppression reduces the number of logs by displaying a single record for multiple occurrences of the same event. Log suppression can negatively impact sensor performance if the reporting interval is set too high. By default this feature is enabled.

**Options** **disable**—Disable log suppression.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## surf-control-integrated

**Syntax**

```
surf-control-integrated {
  cache {
    size value;
    timeout value;
  }
  profile profile-name {
      category customurl-list name {
        action (block | log-and-permit | permit);
      }
    custom-block-message value;
    default (block | log-and-permit | permit);
    fallback-settings {
      default (block | log-and-permit);
      server-connectivity (block | log-and-permit);
      timeout (block | log-and-permit);
      too-many-requests (block | log-and-permit);
      }
      timeout value;
    }
  }
  server {
    host host-name;
    port number;
  }
}
```

**Hierarchy Level** [set security utm feature-profile web-filtering]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure the UTM web-filtering integrated feature.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## sxl-retry

**Syntax** sxl-retry *value;*

**Hierarchy Level** [edit security utm feature-profile anti-virus sophos-engine]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Configure the number of retry attempts to the remote Sophos Extensible List (SXL) server when a request timeout occurs.

**Options** ***value*** —Number of retries.
**Range:** 0 through 5
**Default:** 1

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

## sxl-timeout

**Syntax** sxl-timeout *seconds;*

**Hierarchy Level** [edit security utm feature-profile anti-virus sophos-engine]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Configure the timeout value for responses to a Sophos checksum or URI query.

**Options** ***seconds*** —Number of seconds before timeout occurs.
**Range:** 1 through 5 seconds
**Default:** 2 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## syn-ack-ack-proxy

**Syntax**
```
syn-ack-ack-proxy; {
  threshold number,
}
```

**Hierarchy Level** [edit security screen ids-option *screen-name* tcp]

**Release Information** Statement introduced in Release 8.5 of Junos OS; support for IPv6 addresses added in Release 10.4 of Junos OS.

**Description** Prevent the SYN-ACK-ACK attack, which occurs when the attacker establishes multiple telnet sessions without allowing each session to terminate. This behavior consumes all open slots, generating a denial-of-service (DoS) condition.

**Options** threshold ***number*** — Number of connections from any single IP address.

**Range:** 1 through 250000

**Default:** 512

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Configuration Statement Hierarchy

## syn-check-required

**Syntax** syn-check-required;

**Hierarchy Level** [edit security policies from-zone ***zone-name*** to-zone ***zone-name*** policy ***policy-name*** then permit tcp-options]

**Release Information** Statement introduced in Junos OS Release 10.4.

**Description** Enable sync check per policy. The syn-check-required value overrides the global value no-syn-check.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## syn-fin

**Syntax** syn-fin;

**Hierarchy Level** [edit security screen ids-option *screen-name* tcp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable detection of an illegal combination of flags that attackers can use to consume sessions on the target device, thus resulting in a denial-of-service (DoS) condition.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Configuration Statement Hierarchy

## syn-flood

**Syntax**
```
syn-flood {
  alarm-threshold number;
  attack-threshold number;
  destination-threshold number;
  source-threshold number;
  timeout seconds;
  white-list name {
    destination-address destination-address;
    source-address source-address;
  }
}
```

**Hierarchy Level** [edit security screen ids-option *screen-name* tcp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure detection and prevention of SYN flood attacks. Such attacks occur when the connecting host continuously sends TCP SYN requests without replying to the corresponding ACK responses.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Configuration Statement Hierarchy


Copyright © 2013, Juniper Networks, Inc.

## syn-flood-protection-mode

**Syntax** syn-flood-protection-mode (syn-cookie | syn-proxy);

**Hierarchy Level** [edit security flow]

**Release Information** Statement introduced in Release 8.5 of Junos OS; support for IPv6 addresses added in Release 10.4 of Junos OS.

**Description** Enable SYN cookie or SYN proxy defenses against SYN attacks. SYN flood protection mode is enabled globally on the device and is activated when the configured **syn-flood attack-threshold value** is exceeded.

**Options**
- **syn-cookie**—Uses a cryptographic hash to generate a unique Initial Sequence Number (ISN). This is enabled by default.
- **syn-proxy**—Uses a proxy to handle the SYN attack.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Flow-Based Processing for Security Devices

## syn-frag

**Syntax** syn-frag;

**Hierarchy Level** [edit security screen ids-option *screen-name* tcp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable detection of a SYN fragment attack and drops any packet fragments used for the attack. A SYN fragment attack floods the target host with SYN packet fragments. The host caches these fragments, waiting for the remaining fragments to arrive so it can reassemble them. The flood of connections that cannot be completed eventually fills the host's memory buffer. No further connections are possible, and damage to the host's operating system can occur.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Configuration Statement Hierarchy

Copyright © 2013, Juniper Networks, Inc.

## system-services (Security Zones Host Inbound Traffic)

**Syntax**

```
system-services service-name {
    except;
}
```

**Hierarchy Level** [edit security zones security-zone *zone-name* host-inbound-traffic]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the types of traffic that can reach the device for all interfaces in a zone.

**Options**

- *service-name* —Service for which traffic is allowed. The following services are supported:
  - **all**—Enable all possible system services available on the Routing Engine (RE).
  - **any-service**—Enable services on entire port range.
  - **bootp**—Enable traffic destined to BOOTP and DHCP relay agents.
  - **dhcp**—Enable incoming DHCP requests.
  - **dns**—Enable incoming DNS services.
  - **finger**—Enable incoming finger traffic.
  - **ftp**—Enable incoming FTP traffic.
  - **http**—Enable incoming J-Web or clear-text Web authentication traffic.
  - **https**—Enable incoming J-Web or Web authentication traffic over Secure Sockets Layer (SSL).
  - **ident-reset**—Enable the access that has been blocked by an unacknowledged identification request.
  - **ike**—Enable Internet Key Exchange traffic.
  - **netconf SSH**—Enable incoming NetScreen Security Manager (NSM) traffic over SSH.
  - **ntp**—Enable incoming Network Time Protocol (NTP) traffic.
  - **ping**—Allow the device to respond to ICMP echo requests.
  - **r2cp**—Enable incoming Radio Router Control Protocol traffic.
  - **reverse-ssh**—Reverse SSH traffic.
  - **reverse-telnet**—Reverse Telnet traffic.
  - **rlogin**—Enable incoming **rlogin** (remote login) traffic.
  - **rpm**—Enable incoming Real-time performance monitoring (RPM) traffic.
  - **rsh**—Enable incoming Remote Shell (**rsh**) traffic.
  - **sip**—Enable incoming Session Initiation Protocol traffic.
  - **snmp**—Enable incoming SNMP traffic (UDP port 161).


Copyright © 2013, Juniper Networks, Inc.

- **snmp-trap**—Enable incoming SNMP traps (UDP port 162).
- **ssh**—Enable incoming SSH traffic.
- **telnet**—Enable incoming Telnet traffic.
- **tftp**—Enable TFTP services.
- **traceroute**—Enable incoming traceroute traffic (UDP port 33434).
- **xnm-clear-text**—Enable incoming Junos XML protocol traffic for all specified interfaces.
- **xnm-ssl**— Enable incoming Junos XML protocol-over-SSL traffic for all specified interfaces.

- **except**—(Optional) except can only be used if all has been defined.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Zones and Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## system-services (Security Zones Interfaces)

**Syntax**

```
system-services service-name {
  except;
}
```

**Hierarchy Level** [edit security zones security-zone *zone-name* interfaces *interface-name* host-inbound-traffic]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the types of traffic that can reach the device on a particular interface.

**Options**

- *service-name* —Service for which traffic is allowed. The following services are supported:
  - **all**—Enable all possible system services available on the Routing Engine (RE).
  - **any-service**—Enable services on entire port range.
  - **bootp**—Enable traffic destined to BOOTP and DHCP relay agents.
  - **dhcp**—Enable incoming DHCP requests.
  - **dns**—Enable incoming DNS services.
  - **finger**—Enable incoming finger traffic.
  - **ftp**—Enable incoming FTP traffic.
  - **http**—Enable incoming J-Web or clear-text Web authentication traffic.
  - **https**—Enable incoming J-Web or Web authentication traffic over Secure Sockets Layer (SSL).
  - **ident-reset**—Enable the access that has been blocked by an unacknowledged identification request.
  - **ike**—Enable Internet Key Exchange traffic.
  - **netconf SSH**—Enable incoming NetScreen Security Manager (NSM) traffic over SSH.
  - **ntp**—Enable incoming Network Time Protocol (NTP) traffic.
  - **ping**—Allow the device to respond to ICMP echo requests.
  - **r2cp**—Enable incoming Radio Router Control Protocol traffic.
  - **reverse-ssh**—Reverse SSH traffic.
  - **reverse-telnet**—Reverse Telnet traffic.
  - **rlogin**—Enable incoming **rlogin** (remote login) traffic.
  - **rpm**—Enable incoming real-time performance monitoring (RPM) traffic.
  - **rsh**—Enable incoming Remote Shell (**rsh**) traffic.
  - **snmp**—Enable incoming SNMP traffic (UDP port 161).
  - **snmp-trap**—Enable incoming SNMP traps (UDP port 162).


Copyright © 2013, Juniper Networks, Inc.

- **ssh**—Enable incoming SSH traffic.
- **telnet**—Enable incoming Telnet traffic.
- **tftp**—Enable TFTP services.
- **traceroute**—Enable incoming traceroute traffic (UDP port 33434).
- **xnm-clear-text**—Enable incoming Junos XML protocol traffic for all specified interfaces.
- **xnm-ssl**— Enable incoming Junos XML protocol-over-SSL traffic for all specified interfaces.

- **except**—(Optional) except can only be used if all has been defined.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- Security Zones and Interfaces for Security Devices

## t1-interval

**Syntax**
t1-interval *value-in-milliseconds*;

**Hierarchy Level**
[edit security alg sip]

**Release Information**
Statement introduced in Release 8.5 of Junos OS.

**Description**
Specify the maximum round-trip time (RTT) (in milliseconds) allowed for Session Initiation Protocol (SIP) transactions.

**Options**
*value-in-milliseconds*—Maximum round-trip time (RTT) allowed measured in milliseconds.
**Range:** 500 through 5000 milliseconds
**Default:** 500 milliseconds

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- SIP ALGs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## t4-interval

**Syntax** t4-interval *value-in-seconds*;

**Hierarchy Level** [edit security alg sip]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the maximum length of time (in seconds) that the network can take to clear messages between client and server Session Initiation Protocol (SIP) transactions.

**Options** ***value-in-seconds***—Maximum number of seconds that the network can take to clear messages between client and server transactions.

**Range:** 5 through 10 seconds

**Default:** 5 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- SIP ALGs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## talk

**Syntax**

```
talk {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the TALK program ALG on the device.

**Options**

- **disable**—Disable the TALK program ALG. By default, the TALK program ALG is enabled.
- **traceoptions**—Configure TALK program ALG tracing options.
  - **flag**—Trace operation to perform.
    - **all**—Trace all events.
    - ***extensive***—Display extensive amount of data.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Layer Gateways for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## target (Security IDP)

**Syntax** target (destination-address | service | source-address | source-zone | source-zone-address | zone-service);

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then ip-action]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify the blocking options that you want to set to block the future connections. Blocking options can be based on the following matches of the attack traffic:

**Options**

- **destination-address**—Matches traffic based on the destination address of the attack traffic.
- **service**—For TCP and UDP, matches traffic based on the source address, source port, destination address, and destination port of the attack traffic. This is the default.

  For ICMP flows, the destination port is 0. Any ICMP flow matching source port, source address, and destination address is blocked.
- **source-address**—Matches traffic based on the source address of the attack traffic.
- **source-zone**—Matches traffic based on the source zone of the attack traffic.
- **source-zone-address**—Matches traffic based on the source zone and source address of the attack traffic.
- **zone-service**—Matches traffic based on the source zone, destination address, destination port, and protocol of the attack traffic.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## tcp (Security IDP Protocol Binding)

**Syntax**

```
tcp {
  minimum-port port-number <maximum-port port-number>;
}
```

**Hierarchy Level**

[edit security idp custom-attack *attack-name* attack-type chain protocol-binding]
[edit security idp custom-attack *attack-name* attack-type signature protocol-binding]

**Release Information**

Statement introduced in Release 9.3 of Junos OS.

**Description**

Allow IDP to match the attack for specified TCP port(s).

**Options**

**minimum-port** ***port-number***—Minimum port in the port range.

**Range:** 0 through 65,535

**maximum-port** ***port-number***—Maximum port in the port range.

**Range:** 0 through 65,535

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## tcp (Security IDP Signature Attack)

**Syntax**

```
tcp {
    ack-number {
        match (equal | greater-than | less-than | not-equal);
        value acknowledgement-number;
    }
    data-length {
        match (equal | greater-than | less-than | not-equal);
        value tcp-data-length;
    }
    destination-port {
        match (equal | greater-than | less-than | not-equal);
        value destination-port;
    }
    header-length {
        match (equal | greater-than | less-than | not-equal);
        value header-length;
    }
    mss {
        match (equal | greater-than | less-than | not-equal);
        value maximum-segment-size;
    }
    option {
        match (equal | greater-than | less-than | not-equal);
        value tcp-option;
    }
    sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number;
    }
    source-port {
        match (equal | greater-than | less-than | not-equal);
        value source-port;
    }
    tcp-flags {
        (ack | no-ack);
        (fin | no-fin);
        (psh | no-psh);
        (r1 | no-r1);
        (r2 | no-r2);
        (rst | no-rst);
        (syn | no-syn);
        (urg | no-urg);
    }
    urgent-pointer {
        match (equal | greater-than | less-than | not-equal);
        value urgent-pointer;
    }
    window-scale {
        match (equal | greater-than | less-than | not-equal);
        value window-scale-factor;
    }
    window-size {
```


Copyright © 2013, Juniper Networks, Inc.

```
    match (equal | greater-than | less-than | not-equal);
    value window-size;
  }
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Allow IDP to match the TCP header information for the signature attack.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## tcp (Security Screen)

**Syntax**

```
tcp {
  fin-no-ack;
  land;
  port-scan {
    threshold number;
  }
  syn-ack-ack-proxy {
    threshold number;
  }
  syn-fin;
  syn-flood {
    alarm-threshold number;
    attack-threshold number;
    destination-threshold number;
    source-threshold number;
    timeout seconds;
    white-list name {
      destination-address destination-address;
      source-address source-address;
    }
  }
  syn-frag;
  tcp-no-flag;
  tcp-sweep {
    threshold threshold number;
  }
  winnuke;
}
```

**Hierarchy Level** [edit security screen ids-option *screen-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure TCP-layer intrusion detection service (IDS) options.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Configuration Statement Hierarchy


Copyright © 2013, Juniper Networks, Inc.

## tcp-flags

**Syntax**

```
tcp-flags {
  (ack | no-ack);
  (fin | no-fin);
  (psh | no-psh);
  (r1 | no-r1);
  (r2 | no-r2);
  (rst | no-rst);
  (syn | no-syn);
  (urg | no-urg);
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify that IDP looks for a pattern match whether or not the TCP flag is set.

**Options**

- **ack** | **no-ack**—When set, the acknowledgment flag acknowledges receipt of a packet.
- **fin** | **no-fin**—When set, the final flag indicates that the packet transfer is complete and the connection can be closed.
- **psh** | **no-psh**—When set, the push flag indicates that the receiver should push all data in the current sequence to the destination application (identified by the port number) without waiting for the remaining packets in the sequence.
- **r1** | **no-r1**—When set, indicates that the R1 retransmission threshold has been reached.
- **r2** | **no-r2**—When set, indicates that the R2 retransmission threshold has been reached.
- **rst** | **no-rst**—When set, the reset flag resets the TCP connection, discarding all packets in an existing sequence.
- **syn** | **no-syn**—When set, indicates that the sending device is asking for a three-way handshake to initialize communications.
- **urg** | **no-urg**—When set, the urgent flag indicates that the packet data is urgent.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## tcp-initial-timeout

**Syntax** tcp-initial-timeout *seconds*;

**Hierarchy Level** [edit security flow tcp-session]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Define the length of time (in seconds) that the device keeps an initial TCP session in the session table before dropping it, or until the device receives a FIN (no more data) or RST (reset) packet.

**Options** ***seconds***—Number of seconds that the device keeps an initial TCP session in the session table before dropping it.

**Range:** 4 through 300 seconds

**Default:** 20 seconds



NOTE: The minimum value you can configure for TCP session initialization is 4 seconds. The default value is 20 seconds; if required you can set the TCP session initialization value to less than 20 seconds.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Flow-Based Processing for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## tcp-mss (Security Flow)

**Syntax**

```
tcp-mss {
  all-tcp mss value;
  gre-in {
    mss value;
  }
  gre-out {
    mss value;
  }
  ipsec-vpn {
    mss value;
  }
}
```

**Hierarchy Level** [edit security flow]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure TCP maximum segment size (TCP MSS) for the following packet types:

- All TCP packets for network traffic.
- GRE packets entering the IPsec VPN tunnel.
- GRE packets exiting the IPsec VPN tunnel.
- TCP packets entering the IPsec VPN tunnel.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Flow-Based Processing for Security Devices

## tcp-no-flag

**Syntax** tcp-no-flag;

**Hierarchy Level** [edit security screen ids-option *screen-name* tcp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable the device to drop illegal TCP packets with a missing or malformed flag field.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Configuration Statement Hierarchy

Copyright © 2013, Juniper Networks, Inc.

## tcp-options (Security Policies)

**Syntax**

```
tcp-options {
  sequence-check-required;
  syn-check-required;
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit]

**Release Information** Statement introduced in Junos OS Release 10.4.

**Description** Specify the tcp options for each policy. You can configure sync and sequence checks for each policy based on your requirements. To configure per-policy TCP options, you must turn off the respective global options. Otherwise, the commit check will fail.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

## tcp-rst

**Syntax**

```
tcp-rst;
```

**Hierarchy Level** [edit security zones security-zone *zone-name*]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Enable the device to send a TCP segment with the RST (reset) flag set to 1 (one) in response to a TCP segment with any flag other than SYN set and that does not belong to an existing session.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Zones and Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## tcp-session

**Syntax**

```
tcp-session {
  no-sequence-check;
  no-syn-check;
  no-syn-check-in-tunnel;
  rst-invalidate-session;
  rst-sequence-check;
  strict-syn-check;
  tcp-initial-timeout seconds;
  time-wait-state {
    (session-ageout | session-timeout seconds);
  }
}
```

**Hierarchy Level** [edit security flow]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure TCP session attributes:

- TCP sequence number checking.
- TCP SYN bit checking.
- Reset (RST) checking.
- Initial TCP session timeout—The minimum value you can configure for TCP session initialization is 4 seconds. The default value is 20 seconds; if required you can set the TCP session initialization value to less than 20 seconds.
- Strict TCP SYN checking.
- TCP session timeout for time-wait state.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Flow-Based Processing for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## tcp-sweep

**Syntax**

```
tcp-sweep {
  threshold number;
}
```

**Hierarchy Level** [edit security screen ids-option *screen-name* tcp]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the device to detect and prevent TCP sweep attack. In a TCP sweep attack, an attacker sends TCP SYN packets to the target device as part of the TCP handshake. If the device responds to those packets, the attacker gets an indication that a port in the target device is open, which makes the port vulnerable to attack. If a remote host sends TCP packets to 10 addresses in 0.005 seconds (5000 microseconds), then the device flags this as a TCP sweep attack.

If the **alarm-without-drop** option is not set, the device rejects the eleventh and all further TCP packets from that host for the remainder of the specified threshold period.

**Options**

**threshold *number***—Maximum number of microseconds during which up to 10 TCP SYN packets from the same host are allowed into the device. More than 10 requests from a host during this period triggers TCP Sweep attack response on the router during the remainder of the second.

**Range:** 1000 through 1,000,000 microseconds

**Default:** 5000 microseconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Configuration Statement Hierarchy

## terminal

**Syntax**

```
terminal;
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name*]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Set or unset a terminal rule flag. The device stops matching rules for a session when a terminal rule is matched.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## test (Security IDP)

**Syntax** test *test-condition*;

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type anomaly]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify protocol anomaly condition to be checked.

**Options** ***test-condition***—Name of the anomaly test condition.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## tftp (Security ALG)

**Syntax**

```
tftp {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Configure the Trivial File Transfer Protocol (TFTP) ALG on the device.

**Options**

- **disable**—Disable the TFTP ALG. By default, the TFTP ALG is enabled.

  NOTE: By default, the TFTP ALG is disabled for SRX Series devices.

- **traceoptions**—Configure TFTP ALG tracing options.
  - **flag**—Trace operation to perform.
    - **all**—Trace all events.
    - ***extensive***—Display extensive amount of data.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Layer Gateways for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## then (Security Application Firewall)

**Syntax**

```
then {
   (deny | permit | reject);
}
```

**Hierarchy Level** [edit security application-firewall rule-set *rule-set-name* rule *rule-name*]

**Release Information** Statement introduced in Junos OS Release 11.1. Statement updated in Junos OS Release 12.1X44-D10 with the **reject** option.

**Description** Specify the action to be performed when traffic matches the associated match criteria.

Note that an application firewall is applied after a session has already been created by the security firewall. When traffic is rejected or denied by an application firewall, therefore, logs contain a session open message, a session reject or deny message, and a session close message.

**Options**

- **deny**—Block the traffic at the firewall. The device drops the packet. No message is returned to the sender.
- **permit**—Permit traffic at the firewall.
- **reject**—Block the traffic at the firewall. For TCP traffic, the device drops the packet and returns a TCP reset (RST) message to the source host. For UDP and other protocol traffic, the device drops the packet and returns an ICMP "destination unreachable, port unreachable" message to both the client and the server.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Firewall

Copyright © 2013, Juniper Networks, Inc.

## then (Security Destination NAT)

**Syntax**

```
then {
  destination-nat (off | pool pool-name);
}
```

**Hierarchy Level** [edit security nat destination rule-set *rule-set-name* rule *rule-name*]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify the action to be performed when traffic matches the destination NAT rule criteria.

**Options** The remaining statement is explained separately.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## then (Security IDP Policy)

**Syntax**

```
then {
  action {
    class-of-service {
      dscp-code-point number;
      forwarding-class forwarding-class;
    }
    (close-client | close-client-and-server | close-server |drop-connection | drop-packet |
      ignore-connection | mark-diffserv value | no-action | recommended);
  }
  ip-action {
    (ip-block | ip-close | ip-notify);
    log;
    log-create;
    refresh-timeout;
    target (destination-address | service | source-address | source-zone | source-zone-address
      | zone-service);
    timeout seconds;
  }
  notification {
    log-attacks {
      alert;
    }
    packet-log {
      post-attack number;
      post-attack-timeout seconds;
      pre-attack number;
    }
  }
  severity (critical | info | major | minor | warning);
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name*]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify the action to be performed when traffic matches the defined criteria.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices
- IDP Class of Service Action for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## then (Security Policies)

**Syntax**

```
then {
  count {
    alarm {
      per-minute-threshold number;
      per-second-threshold number;
    }
  }
  deny;
  log {
    session-close;
    session-init;
  }
  permit {
    application-services {
      application-firewall {
        rule-set rule-set-name;
      }
      application-traffic-control {
        rule-set rule-set-name;
      }
      gprs-gtp-profile profile-name;
      gprs-sctp-profile profile-name;
      idp;
      redirect-wx | reverse-redirect-wx;
      ssl-proxy {
        profile-name profile-name;
      }
      uac-policy {
        captive-portal captive-portal;
      }
      utm-policy policy-name;
    }
    destination-address {
      drop-translated;
      drop-untranslated;
    }
    firewall-authentication {
      pass-through {
        access-profile profile-name;
        client-match user-or-group-name;
        ssl-termination-profile profile-name;
        web-redirect;
        web-redirect-to-https;
      }
      web-authentication {
        client-match user-or-group-name;
      }
    }
    services-offload;
    tcp-options {
      sequence-check-required;
      syn-check-required;
```


Copyright © 2013, Juniper Networks, Inc.

```
    }
    tunnel {
      ipsec-group-vpn group-vpn;
      ipsec-vpn vpn-name;
      pair-policy pair-policy;
    }
  }
  reject;
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name*]

**Release Information** Statement introduced in Junos OS Release 8.5. Support for the **services-offload** option added in Junos OS Release 11.4. Support for the **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10.

**Description** Specify the policy action to be performed when packets match the defined criteria.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## then (Security Rulebase DDos)

**Syntax**

```
then {
  action {
    (close-server | drop-connection | drop-packet | no-action);
  }
  ip-action {
    (ip-block | ip-close | ip-connection-rate-limit connections-per-second | ip-notify);
    log;
    log-create;
    refresh-timeout;
    timeout seconds;
  }
  notification {
    log-attacks {
      alert;
    }
  }
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Specify the session action to be performed when traffic matches the defined criteria.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## then (Security Source NAT)

**Syntax**

```
then {
  source-nat {
    interface {
      persistent-nat {
        address-mapping;
        inactivity-timeout seconds;
        max-session-number value;
        permit (any-remote-host | target-host | target-host-port);
      }
    }
    off;
    pool {
      persistent-nat {
        address-mapping;
        inactivity-timeout seconds;
        max-session-number number;
        permit (any-remote-host | target-host | target-host-port);
      }
      pool-name;
    }
  }
}
```

**Hierarchy Level** [edit security nat source rule-set *rule-set-name* rule *rule-name*]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify the action to be performed when traffic matches the source NAT rule criteria.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## then (Security Static NAT)

**Syntax**

```
then {
  static-nat {
    inet {
      routing-instance (default | routing-instance-name);
    }
    prefix {
      address-prefix;
      mapped-port lower-port-range to upper-port-range;
      routing-instance (default | routing-instance-name);
    }
    prefix-name {
      address-prefix-name;
      mapped-port lower-port-range to upper-port-range;
      routing-instance (default | routing-instance-name);
    }
  }
}
```

**Hierarchy Level** [edit security nat static rule-set *rule-set-name* rule *rule-name*]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Specify the action to be performed when traffic matches the static NAT rule criteria.

**Options** The remaining statement is explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## threshold (Security IKE Gateway)

**Syntax** threshold *number*;

**Hierarchy Level** [edit security ike gateway *gateway-name* dead-peer-detection]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the maximum number of unsuccessful dead peer detection (DPD) requests to be sent before the peer is considered unavailable. (This statement is not supported on dynamic VPN implementations.)

**Options** ***number*** —Maximum number of unsuccessful DPD requests to be sent.

**Range:** 1 through 5

*Output:* 5



NOTE: The threshold number for the IKEv2 protocol is predefined as 5.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## time-binding

**Syntax**

```
time-binding {
  count count-value;
  scope (destination | peer | source);
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name*]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Allow IDP to detect a sequence of the same attacks over a period of time.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## time-binding-count

**Syntax** time-binding-count *number*;

**Hierarchy Level** [edit security idp application-ddos *application-name* context *context-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** (Optional) Configure the number of context or context value hits from each client over the time binding period to determine if it should be considered a bot client.

**Options** *number*—Time-binding count for the source address.
**Range:** 2 to 50,000

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application-Level Distributed Denial of Service


Copyright © 2013, Juniper Networks, Inc.

## time-binding-period statement

**Syntax** time-binding-period *seconds*;

**Hierarchy Level** [edit security idp application-ddos *application-name* context *context-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** (Optional) Configure the time-binding period to determine if a client should be classified as a bot client or not. This setting is used in conjunction with time-binding count to detect an attack if a client request for the same context value exceeds time-binding-count times in time-binding-period seconds.

Contexts values are monitored until overall requests for a given application-level distributed denial-of-service (DDoS) application no longer exceeds hit-rate-threshold limit for each configured context. If overall context requests exceeds hit-rate-threshold limit, context value monitoring is disabled and system applies time-binding with PEER scope (source-ip, destination-ip, destination-port, destination-protocol, destination-zone), if configured.

**Options** *number*—Time-binding period (seconds).

**Range:** 1 to 3600 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service

Copyright © 2013, Juniper Networks, Inc.

## time-wait-state

**Syntax**

```
time-wait-state {
    (session-ageout | session-timeout seconds);
}
```

**Hierarchy Level** [edit security flow tcp-session]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Defines the length of time (in seconds) that the device keeps the defined TCP session in the session table. The default is 150 seconds.

**Options**

- **session-ageout**—Set a TCP session to age out, using the service based timeout value.
- **session-timeout *seconds***—Set the session timeout value allowed before the device ages out a session from its session table.

  Range: 2 through 600 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Flow-Based Processing for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## timeout (Security Antivirus Fallback Options)

**Syntax** timeout (block | log-and-permit);

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* fallback-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Updated in

**Description** Scanning a complex file could consume resources and time. If the time it is taking to scan exceeds the timeout setting in the antivirus profile, the processing is aborted and the content is either passed or blocked without completing the virus checking. The decision is made based on the timeout fallback option. The default action is block.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- Unified Threat Management
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## timeout (Security Antivirus Fallback Options Sophos Engine)

**Syntax** default (block | log-and-permit | permit);

**Hierarchy Level** [edit security utm feature-profile anti-virus sophos-engine profile *profile-name* fallback-options]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Scanning a complex file could consume resources and time. If the time it is taking to scan exceeds the timeout setting in the antivirus profile, the processing is aborted and the content is either passed or blocked without completing the virus checking. The decision is made based on the timeout fallback option.

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## timeout (Security Antivirus Scan Options)

**Syntax** timeout *value*;

**Hierarchy Level**
[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* scan-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* scan-options]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* scan-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** The scanning timeout value includes the time frame from when the scan request is generated to when the scan result is returned by the scan engine. The time range can be 1 to 1800 seconds. By default, it is 180 seconds.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- Unified Threat Management
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## timeout (Security IDP Policy)

**Syntax** timeout *seconds*;

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* then ip-action]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then ip-action]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Release 10.0 of Junos OS.

**Description** Specify the number of seconds that you want the IP action to remain in effect after a traffic match.

**Options** ***seconds***—Number of seconds the IP action should remain effective.
**Range:** 0 through 64,800 seconds
**Default:** 0 second

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- Application-Level Distributed Denial of Service
- IDP Application Identification for Security Devices

## timeout (Security GTP)

**Syntax** timeout *value*;

**Hierarchy Level** [edit security gprs gtp profile *profile-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS. Support for GTPv2 added in Release 11.4 of Junos OS.

**Description** Set the tunnel timeout value in hours. The default is 36 hours.

If a device detects no activity in a tunnel for a specified period, it removes the tunnel from the state table.

**Options** **Range:** 1 through 1,000 hours.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- General Packet Radio Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## timeout (Security Screen)

**Syntax** timeout *seconds*;

**Hierarchy Level** [edit security screen ids-option *screen-name* tcp syn-flood]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the maximum length of time before a half-completed connection is dropped from the queue. You can decrease the timeout value until you see any connections dropped during normal traffic conditions.

**Options** ***seconds*** —Time interval before a half-completed connection is dropped from the queue.
**Range:** 1 through 50 seconds
**Default:** 20 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Configuration Statement Hierarchy

## timeout (Security Web Filtering)

**Syntax** timeout *value*;

**Hierarchy Level** [edit security utm feature-profile web-filtering websense-redirect profile *profile-name*]
[edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.
Statement introduced in Release 11.4 of Junos OS for Enhanced Web Filtering.

**Description** Enter a timeout limit for requests. Once this limit is reached, fail mode settings are applied. The default here is 15 seconds.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## timeout (Security Web Filtering Cache)

**Syntax** timeout *value*;

**Hierarchy Level** [edit security utm feature-profile web-filtering surf-control-integrated cache]
[edit security utm feature-profile web-filtering juniper-enhanced cache]

**Release Information** Statement introduced in Release 9.5 of Junos OS.
Statement introduced in Release 11.4 of Junos OS for Enhanced Web Filtering.

**Description** Set the cache timeout parameters for surf-control-integrated web filtering (24 hours is the default and the maximum allowed life span of cached items).

**Options** **Range:** 1 through 1800 minutes.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices

## timeout (Security Web Filtering Fallback Settings)

**Syntax** timeout (block | log-and-permit);

**Hierarchy Level** [edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name* fallback-settings]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name* fallback-settings]
[edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name* fallback-settings]

**Release Information** Statement introduced in Release 9.5 of Junos OS.
Statement introduced in Release 11.4 of Junos OS for Enhanced Web Filtering.

**Description** Fallback settings tell the system how to handle errors.

**Options**
- log-and-permit—Log the error and permit the traffic
- block—Log the error and deny the traffic

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## to (Security Source NAT)

**Syntax**

```
to {
  interface [interface-name];
  routing-instance [routing-instance-name];
  zone [zone-name];
}
```

**Hierarchy Level** [edit security nat source rule-set *rule-set-name*]

**Release Information** Statement introduced in Junos OS Release 9.2.

**Description** Specify the destination of the packet among the routing instance, interface, or zone.

**Options**

- **interface [*interface-name*]**—Name of the interface.
- **routing-instance [*routing-instance-name*]**—Name of the routing instance.
- **zone [*zone-name*]**—Name of the zone.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

## to-zone (Security IDP Policy)

**Syntax** to-zone (*zone-name* | any);

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name* match]
[edit security idp idp-policy *policy-name* rulebase-exempt rule *rule-name* match]
[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for rulebase-ddos introduced in Release 10.0 of Junos OS.

**Description** Specify a destination zone to be associated with the security policy. The default value is any.

**Options** *zone-name*—Name of the destination zone object.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- Application-Level Distributed Denial of Service
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## to-zone (Security Policies)

**Syntax**

```
to-zone zone-name {
  policy policy-name {
    description description;
    match {
      application {
        [application];
        any;
      }
      destination-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
      }
      source-address {
        [address];
        any;
        any-ipv4;
        any-ipv6;
      }
      source-identity {
        [role-name];
        any;
        authenticated-user;
        unauthenticated-user;
        unknown-user;
      }
    }
    scheduler-name scheduler-name;
    then {
      count {
        alarm {
          per-minute-threshold number;
          per-second-threshold number;
        }
      }
      deny;
      log {
        session-close;
        session-init;
      }
      permit {
        application-services {
          application-firewall {
            rule-set rule-set-name;
          }
          application-traffic-control {
            rule-set rule-set-name;
          }
          gprs-gtp-profile profile-name;
          gprs-sctp-profile profile-name;
          idp;
```


Copyright © 2013, Juniper Networks, Inc.

```
            redirect-wx | reverse-redirect-wx;
            ssl-proxy {
              profile-name profile-name;
            }
            uac-policy {
              captive-portal captive-portal;
            }
            utm-policy policy-name;
          }
          destination-address {
            drop-translated;
            drop-untranslated;
          }
          firewall-authentication {
            pass-through {
              access-profile profile-name;
              client-match user-or-group-name;
              ssl-termination-profile profile-name;
              web-redirect;
              web-redirect-to-https;
            }
            web-authentication {
              client-match user-or-group-name;
            }
          }
          services-offload;
          tcp-options {
            sequence-check-required;
            syn-check-required;
          }
          tunnel {
            ipsec-group-vpn group-vpn;
            ipsec-vpn vpn-name;
            pair-policy pair-policy;
          }
        }
        reject;
      }
    }
  }
```

**Hierarchy Level** [edit security policies from-zone *zone-name*]

**Release Information** Statement introduced in Junos OS Release 8.5. Support for the **services-offload** and **junos-host** options added in Junos OS Release 11.4. Support for the **source-identity** option added in Junos OS Release 12.1. Support for the **ssl-termination-profile** and **web-redirect-to-https** options added in Junos OS Release 12.1X44-D10.

**Description** Specify a destination zone to be associated with the security policy.

**Options**

- **zone-name**—Name of the destination zone object.
- **junos-host**—Default security zone for self-traffic of the device.

The remaining statements are explained separately.

Copyright © 2013, Juniper Networks, Inc.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices
- Security Policy
- UTM for Security Devices

## too-many-requests (Security Antivirus Fallback Options)

**Syntax**
too-many-requests (block | log-and-permit);

**Hierarchy Level**
[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* fallback-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* fallback-options]

**Release Information**
Statement introduced in Release 9.5 of Junos OS.

**Description**
If the total number of messages received concurrently exceeds 4000, the content is either passed or blocked depending on the too-many-request fallback option. The default action is block. (The allowed request limit is not configurable.)

**Options**
- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- Unified Threat Management
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## too-many-requests (Security Antivirus Fallback Options Sophos Engine)

**Syntax** default (block | log-and-permit | permit);

**Hierarchy Level** [edit security utm feature-profile anti-virus sophos-engine profile *profile-name* fallback-options]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** If the total number of messages received concurrently exceeds the device limits, the content is either passed or blocked depending on the too-many-request fallback option. (The allowed request limit is not configurable.)

**Options**

- **block**—Log the error and deny the traffic
- **log-and-permit**—Log the error and permit the traffic
- **permit**—Permit the traffic

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## too-many-requests (Security Web Filtering Fallback Settings)

**Syntax** too-many-requests (block | log-and-permit);

**Hierarchy Level**
[edit security utm feature-profile web-filtering surf-control-integrated profile *profile-name* fallback-settings]
[edit security utm feature-profile web-filtering websense-redirect profile *profile-name* fallback-settings]
[edit security utm feature-profile web-filtering juniper-enhanced profile *profile-name* fallback-settings]

**Release Information**
Statement introduced in Release 9.5 of Junos OS.
Statement introduced in Release 11.4 of Junos OS for Enhanced Web Filtering.

**Description** If the total number of messages received concurrently exceeds the device limits, the content is either passed or blocked depending on the too-many-request fallback option. The default action is BLOCK. (The allowed request limit is not configurable.)

**Options**
- block—Log the error and deny the traffic
- log-and-permit—Log the error and permit the traffic

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## tos

**Syntax**

```
tos {
  match (equal | greater-than | less-than | not-equal);
  value type-of-service-in-decimal;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol ipv4]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the type of service.

**Options**

- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***type-of-service-in-decimal***—The following service types are available:
  - 0000—Default
  - 0001—Minimize Cost
  - 0002—Maximize Reliability
  - 0003—Maximize Throughput
  - 0004—Minimize Delay
  - 0005—Maximize Security

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## total-length

**Syntax**

```
total-length {
  match (equal | greater-than | less-than | not-equal);
  value total-length-of-ip-datagram;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol ipv4]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the number of bytes in the packet, including all header fields and the data payload.

**Options**

- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***total-length-of-ip-datagram***—Length of the IP datagram.

  **Range:** 0 through 65,535

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## total-memory

**Syntax** total-memory *percentage*;

**Hierarchy Level** [edit security idp sensor-configuration packet-log]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the maximum amount of memory to be allocated to packet capture for the device. This value is expressed as a percentage of the memory available on the device. The total memory for a device will differ depending on its operating mode.

**Options**

- ***percentage***—Amount of packet capture memory expressed as a percentage of total memory for the device mode.

  **Range:** 1 to 100 percent

  **Default:** 10

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security)

**Syntax**

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
  rate-limit messages-per-second;
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Configure security tracing options.

**Options**

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

    Syntax: ***x* K** to specify KB, ***x* m** to specify MB, or ***x* g** to specify GB

    Range: 10 KB through 1 GB

Copyright © 2013, Juniper Networks, Inc.

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace all security events
  - **compilation**—Trace security compilation events
  - **configuration**—Trace security configuration events
  - **routing-socket**—Trace routing socket events
- **no-remote-trace**—Set remote tracing as disabled.
- **rate-limit *messages-per-second***—Limit the incoming rate of trace messages.

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- Flow-Based Processing for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security ALG)

**Syntax**

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  level (brief | detail | extensive | verbose);
  no-remote-trace;
}
```

**Hierarchy Level** [edit security alg]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure ALG tracing options.

**Options**

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

    Syntax: ***x* K** to specify KB, ***x* m** to specify MB, or ***x* g** to specify GB

    Range: 10 KB through 1 GB

Copyright © 2013, Juniper Networks, Inc.

Default: 128 KB

- **world-readable** | **no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **level**—Set the level of debugging the output option.
  - **brief**—Match brief messages
  - **detail**—Match detail messages.
  - **extensive**—Match extensive messages.
  - **verbose**—Match verbose messages.
- **no-remote-trace**—Set remote tracing as disabled.

**Required Privilege Level** trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**
- Application Layer Gateways for Security Devices

## traceoptions (Security Antispam)

**Syntax** traceoptions flag *flag*;

**Hierarchy Level** [edit security utm feature-profile anti-spam]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Define tracing operations for UTM antispam features.

**Options**
- *flag*:
  - **all**—Enable all antispam trace flags.
  - **manager** —Trace antispam manager information.
  - **sbl**—Trace SBL server information.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security Antivirus)

**Syntax** traceoptions flag *flag*;

**Hierarchy Level** [edit security utm feature-profile anti-virus]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Define tracing operations for UTM antivirus features.

**Options**

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Enable trace all antivirus trace options.
  - **basic**—Trace antivirus module generic basic information.
  - **detail**—Trace antivirus module generic detail information.
  - **engine**—Trace scan engine information.
  - **event**—Trace communication events between routing engine side processes.
  - **ipc**—Trace communication events with Packet Forwarding Engine.
  - **manager**—Trace antivirus manager process activities.
  - **pattern**—Trace detail information of pattern loading.
  - **sendmail**—Trace mail notifying process activities.
  - **statistics**—Trace statistics information.
  - **updater**—Trace pattern updater process activities.
  - **worker**—Trace antivirus worker process activities.

**Required Privilege Level** trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security Application Firewall)

**Syntax**

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

**Hierarchy Level** [edit security application-firewall]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Configure trace options for the application firewall.

**Options**

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

    Syntax: ***x* K** to specify KB, ***x* m** to specify MB, or ***x* g** to specify GB

    Range: 10 KB through 1 GB


Copyright © 2013, Juniper Networks, Inc.

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace with all flags enabled
  - **compilation**—Trace rule set compilation events
  - **configuration**—Trace configuration events
  - **ipc**—Trace process inter communication events
  - **lookup**—Trace rule set lookup events
- **no-remote-trace**—Set remote tracing as disabled.

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- Application Firewall

## traceoptions (Security Application Proxy)

**Syntax**

```
traceoptions {
  flag flag;
}
```

**Hierarchy Level** [edit security utm application-proxy]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure tracing options for application proxy.

**Options**

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **abort**—Trace aborted sessions for application proxy.
  - **all**—Trace with all flags enabled.
  - **anti-virus**—Trace anti-virus information.
  - **application-objects**—Trace application-proxy objects information.
  - **basic**—Trace application-proxy related basic information.
  - **buffer**— Trace application-proxy data buffer information.
  - **connection-rating**—Trace connection rating information.
  - **detail**—Trace application-proxy related detailed information.
  - **express-anti-virus**—Trace anti-virus express engine information.
  - **ftp-control**—Trace FTP control connection information.
  - **ftp-data**—Trace FTP data connection information.
  - **http**—Trace HTTP protocol information.
  - **imap**—Trace IMAP protocol information.
  - **memory**—Trace memory usage.
  - **mime**—Trace MIME parser information.
  - **parser**— Trace protocol parser information.
  - **pfe**—Trace communication with PFE.
  - **pop3**—Trace POP3 protocol information.
  - **queue**—Trace queue information.
  - **regex-engine**—Trace Pattern Match Engine (PME) information.
  - **smtp**—Trace SMTP protocol information.
  - **sophos-anti-virus**—Trace anti-virus sophos engine information.
  - **tcp**—Trace TCP level information.


Copyright © 2013, Juniper Networks, Inc.

- **timer**—Trace timer processing.
- **utm-realtime**—Trace application-proxy realtime-thread information

**Required Privilege Level**
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

## traceoptions (Security Content Filtering)

**Syntax**
traceoptions flag *flag*;

**Hierarchy Level**
[edit security utm feature-profile content-filtering]

**Release Information**
Statement introduced in Release 9.5 of Junos OS.

**Description**
Define tracing options for content filtering features.

**Options**
- *flag*:
  - **all**—Enable all content filtering trace flags.
  - **basic** —Trace content filtering basic information.
  - **detail**—Trace content filtering detailed information.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security Datapath Debug)

**Syntax**

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  no-remote-trace;
}
```

**Hierarchy Level** [edit security datapath-debug]

**Release Information** Command introduced in Release 9.6 of Junos OS.

**Description** Sets the trace options for datapath-debug.

**Options**

- **file**—Configure the trace file options.
  - **filename**—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed to trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named trace-file reaches this size, it is renamed trace-file.0. When the trace-file again reaches its maximum size, trace-file.0 is renamed trace-file.1 and trace-file is renamed trace-file.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and a filename.

    Syntax: x K to specify KB, x m to specify MB, or x g to specify GB

    Range: 10 KB through 1 GB

    Default: 128 KB


Copyright © 2013, Juniper Networks, Inc.

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option

- **no-remote-trace**—Set remote tracing as disabled.

**Required Privilege Level**
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

## traceoptions (Security Dynamic VPN)

**Syntax**

```
traceoptions {
  file filename;
  flag {
    all <detail | extensive | terse>;
  }
}
```

**Hierarchy Level**
[edit security dynamic-vpn]

**Release Information**
Statement introduced in Junos OS Release 12.1X44-D10.

**Description**
Configure dynamic VPN tracing options.

**Options**

- **file**—Configure the trace file options.

  **file *filename***—Name of the file to receive the output of the tracing operation.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Enable all tracing operations
    - **detail**—Display moderate amount of data in trace.
    - **extensive**—Display extensive amount of data in trace.
    - **terse**—Display minimum amount of data in trace.

**Required Privilege Level**
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- Dynamic VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security Firewall Authentication)

**Syntax**

```
traceoptions {
  flag {
    all <detail | extensive | terse>;
    authentication <detail | extensive | terse>;
    proxy <detail | extensive | terse>;
  }
}
```

**Hierarchy Level** [edit security firewall-authentication]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Define data-plane firewall authentication tracing options.

**Options**

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Enable all tracing operations
  - **authentication**—Trace data-plane firewall authentication events
  - **proxy**—Trace data-plane firewall authentication proxy events
- **detail**—Display moderate amount of data in trace.
- **extensive**—Display extensive amount of data in trace.
- **terse**—Display minimum amount of data in trace.

**Required Privilege Level**
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security Flow)

**Syntax**

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
  packet-filter filter-name {
    destination-port port-identifier;
    destination-prefix address;
    interface interface-name;
    protocol protocol-identifier;
    source-port port-identifier;
    source-prefix address;
  }
  rate-limit messages-per-second;
}
```

**Hierarchy Level** [edit security flow]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure flow tracing options.

**Options**

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme

Copyright © 2013, Juniper Networks, Inc.

continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

Syntax: ***x*** **K** to specify KB, ***x*** **m** to specify MB, or ***x*** **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace with all flags enabled
  - **basic-datapath**—Trace basic packet flow activity
  - **packet-drops**—Trace packet drop activity
- **no-remote-trace**—Set remote tracing as disabled.
- **packet-filter *filter-name***—Packet filter to enable during the tracing operation. Configure the filtering options.
  - **destination-port *port-identifier***—Match TCP/UDP destination port
  - **destination-prefix *address***—Destination IP address prefix
  - **interface *interface-name***—Logical interface
  - **protocol *protocol-identifier***—Match IP protocol type
  - **source-port *port-identifier***—Match TCP/UDP source port
  - **source-prefix *address***—Source IP address prefix
- **rate-limit *messages-per-second***—Limit the incoming rate of trace messages.

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- MPLS for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security Group VPN)

**Syntax**

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

**Hierarchy Level** [edit security group-vpn server]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure group VPN trace options.

**Options**

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

    Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB

    Range: 10 KB through 1 GB

    Default: 128 KB

Copyright © 2013, Juniper Networks, Inc.

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace all activity
  - **certificates**—Trace certificate-related activity
  - **database**—Trace SA-related database activity
  - **general**—Trace general activity
  - **high-availability**—Trace high-availability operations
  - **ike**—Trace IKE protocol activity
  - **next-hop-tunnels**—Trace next-hop tunnel operations
  - **parse**—Trace configuration processing
  - **policy-manager**—Trace IKE callback activity
  - **routing-socket**—Trace routing socket activity
  - **thread**—Trace thread processing
  - **timer**—Trace timer activity
- **no-remote-trace**—Disable remote tracing.

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security GTP)

**Syntax**

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

**Hierarchy Level** [edit security gprs gtp]

**Release Information** Statement introduced in Release 10.0 of Junos OS. Support for GTPv2 added in Release 11.4 of Junos OS.

**Description** Enable the device to identify and log the contents of GTP-U or GTP-C messages based on IMSI prefixes or Mobile Station-Integrated Services Data Network (MS-ISDN) identification.

**Options**

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

Copyright © 2013, Juniper Networks, Inc.

Syntax: ***x*** **K** to specify KB, ***x*** **m** to specify MB, or ***x*** **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable** | **no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace everything.
  - **chassis-cluster**—Trace chassis cluster events.
  - **configuration**—Trace configuration events.
  - **flow**—Trace flow events.
  - **parser**—Trace parser events.
- **no-remote-trace**—Set remote tracing as disabled.

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- General Packet Radio Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security H323 ALG)

**Syntax**

```
traceoptions {
  flag flag <detail | extensive | terse>;
}
```

**Hierarchy Level** [edit security alg h323]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure H.323 tracing options.

**Options**

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace with all flags enabled.
  - **chassis-cluster**—Trace chassis cluster information.
  - **h225-asn1**—Trace H.225 ASN.1 processing activity.
  - **h245**—Trace H.245 processing activity.
  - **h245-asn1**—Trace H.245 ASN.1 processing activity.
  - **q931**—Trace Q.931 processing activity.
  - **ras**—Trace remote access server (RAS) processing activity.
  - **ras-asn1**—Trace RAS ASN.1 processing activity.
- **detail**—Display moderate amount of data in trace.
- **extensive**—Display extensive amount of data in trace.
- **terse**—Display minimum amount of data in trace.

**Required Privilege Level** trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- H.323 ALGs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security IDP)

**Syntax**

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag all;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
```

**Hierarchy Level** [edit security idp]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Configure IDP tracing options.

**Options**

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

    Syntax: ***x*** **K** to specify KB, ***x*** **m** to specify MB, or ***x*** **g** to specify GB

    Range: 10 KB through 1 GB


Copyright © 2013, Juniper Networks, Inc.

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform.
  - **all**—Trace with all flags enabled
- **level**—Set the level of debugging the output option.
  - **all**—Match all levels
  - **error**—Match error conditions
  - **info**—Match informational messages
  - **notice**—Match conditions that should be handled specially
  - **verbose**—Match verbose messages
  - **warning**—Match warning messages
- **no-remote-trace**—Set remote tracing as disabled.

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices
- IDP Signature Database for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security IKE)

**Syntax**

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
  rate-limit messages-per-second;
}
```

**Hierarchy Level** [edit security ike]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure IKE tracing options.

**Options**

- file—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.
  - **files** ***number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0,** then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match** ***regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size** ***maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and filename.

    Syntax: ***x*** **k** to specify KB, ***x*** **m** to specify MB, or ***x*** **g** to specify GB

    Range: 10 KB through 1 GB


Copyright © 2013, Juniper Networks, Inc.

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace all iked process modules activity
  - **certificates**—Trace certificate-related activity
  - **config**—Trace configuration download processing
  - **database**—Trace VPN-related database activity
  - **general**—Trace general activity
  - **high-availability**—Trace high-availability operations
  - **ike**—Trace IKE protocol activity
  - **next-hop-tunnels**—Trace next-hop tunnels operations
  - **parse**—Trace VPN parsing activity
  - **policy-manager**—Trace iked callback activity
  - **routing-socket**—Trace routing socket activity
  - **thread**—Trace thread processing
  - **timer**—Trace timer activity
- **no-remote-trace**—Set remote tracing as disabled.
- **rate-limit *messages-per-second***—Configure the incoming rate of trace messages.

  Range: 0 through 4,294,967,295

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security IPsec)

**Syntax**

```
traceoptions {
  flag flag;
}
```

**Hierarchy Level** [edit security ipsec]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure IPsec tracing options.

**Options**

- **flag**—To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace with all flags enabled
  - **next-hop-tunnel-binding**—Trace next-hop tunnel binding events
  - **packet-drops**—Trace packet drop activity
  - **packet-processing**—Trace data packet processing events
  - **security-associations**—Trace security association (SA) management events

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security Log)

**Syntax**

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

**Hierarchy Level** [edit security log]

**Release Information** Statement modified in Release 9.2 of Junos OS.

**Description** Configure security log tracing options.

**Options**

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

    Syntax: ***x* K** to specify KB, ***x* m** to specify MB, or ***x* g** to specify GB

    Range: 10 KB through 1 GB

Copyright © 2013, Juniper Networks, Inc.

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace with all flags enabled
  - **configuration**—Trace configuration events
  - **hpl**— Trace HPL logging
  - **report**— Trace HPL logging
  - **source**—Communicate with security log forwarder
- **no-remote-trace**—Set remote tracing as disabled.

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- System Log Messages
- Security Logs


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security MGCP ALG)

**Syntax**

```
traceoptions {
  flag flag <extensive>;
}
```

**Hierarchy Level** [edit security alg mgcp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure Media Gateway Control Protocol (MGCP) tracing options.

**Options**

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace with all flags enabled.
  - **call**—Trace call processing activity.
  - **chassis-cluster**—Trace chassis cluster information.
  - **decode**—Trace decoder operations activity.
  - **error**—Trace processing errors activity.
  - **nat**—Trace Network Address Translation (NAT) processing activity.
  - **packet**—Trace MGCP protocol packet processing activity.
  - **rm**—Trace MGCP Resource Management (Resmgr) functions activity.

**Required Privilege Level** trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- MGCP ALGs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security NAT)

**Syntax**

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

**Hierarchy Level** [edit security nat]

**Release Information** Statement modified in Junos OS Release 9.6.

**Description** Configure NAT tracing options.

**Options**

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

    Syntax: ***x* K** to specify KB, ***x* m** to specify MB, or ***x* g** to specify GB

    Range: 10 KB through 1 GB


Copyright © 2013, Juniper Networks, Inc.

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace with all flags enabled
  - **destination-nat-pfe**—Trace destination NAT events on PFE-ukernel side
  - **destination-nat-re**—Trace destination NAT events on Routing Engine (RE) side
  - **destination-nat-rt**—Trace destination NAT events on Packet Forwarding Engine real-time (PFE-RT) side
  - **source-nat-pfe**—Trace source NAT events on PFE-ukernel side
  - **source-nat-re**—Trace source NAT events on RE side
  - **source-nat-rt**—Trace source NAT events on PFE-RT side
  - **static-nat-pfe**—Trace static NAT events on PFE-ukernel side
  - **static-nat-re**—Trace static NAT events on RE side
  - **static-nat-rt**—Trace static NAT events on PFE-RT side
- **no-remote-trace**—Set remote tracing as disabled.

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- Network Address Translation for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security PKI)

**Syntax**

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

**Hierarchy Level** [edit security pki]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Configure public key infrastructure (PKI) tracing options.

**Options**

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

    Syntax: ***x* K** to specify KB, ***x* m** to specify MB, or ***x* g** to specify GB

    Range: 10 KB through 1 GB


Copyright © 2013, Juniper Networks, Inc.

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace with all flags enabled
  - **certificate-verification**—Trace PKI certificate verification events
  - **online-crl-check**—Trace PKI online certificate revocation list (CRL) events
- **no-remote-trace**—Set remote tracing as disabled.

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- Certificates and Public Key Cryptography for Security Devices

## traceoptions (Security Policies)

**Syntax**

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

**Hierarchy Level** [edit security policies]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Configure policy tracing options.

**Options**

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

    Syntax: ***x* K** to specify KB, ***x* m** to specify MB, or ***x* g** to specify GB

    Range: 10 KB through 1 GB


Copyright © 2013, Juniper Networks, Inc.

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace with all flags enabled
  - **configuration**—Trace configuration events
  - **compilation**—Trace policy compilation events
  - **ipc**—Trace process inter communication events
  - **lookup**—Trace policy lookup events
  - **routing-socket**—Trace routing socket events
  - **rules**—Trace policy rules-related events
- **no-remote-trace**—Set remote tracing as disabled.

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security SCCP ALG)

**Syntax**

```
traceoptions {
  flag flag <extensive>;
}
```

**Hierarchy Level** [edit security alg sccp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure Skinny Client Control Protocol (SCCP) tracing options.

**Options**

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace with all flags enabled.
  - **call**—Trace call processing activity.
  - **chassis-cluster**—Trace chassis cluster information.
  - **cli**—Trace CLI configuration activity and command changes.
  - **decode**—Trace decoder operations activity.
  - **error**—Trace processing errors activity.
  - **init**—Enable tracing for SCCP initialization errors
  - **nat**—Enable tracing for SCCP NAT processing
  - **rm**——Trace SCCP Resource Management (Resmgr) functions activity.

**Required Privilege Level** trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- SCCP ALGs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security Screen)

**Syntax**

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

**Hierarchy Level** [edit security screen]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure screen tracing options.

To specify more than one tracing option, include multiple **flag** statements.

**Options**

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

    Syntax: ***x* K** to specify KB, ***x* m** to specify MB, or ***x* g** to specify GB

Copyright © 2013, Juniper Networks, Inc.

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable** | **no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace all screen events
  - **configuration**—Trace screen configuration events
  - **flow**—Trace flow events
- **no-remote-trace**—Set remote tracing as disabled.

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- Security Configuration Statement Hierarchy


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security SCTP)

**Syntax**

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

**Hierarchy Level** [edit security gprs sctp]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Set the trace options for Stream Control Transmission Protocol (SCTP).

**Options**

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

    Syntax: ***x* K** to specify KB, ***x* m** to specify MB, or ***x* g** to specify GB

    Range: 10 KB through 1 GB

Copyright © 2013, Juniper Networks, Inc.

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace everything.
  - **chassis-cluster**—Trace chassis cluster events.
  - **configuration**—Trace configuration events.
  - **flow**—Trace flow events.
  - **parser**—Trace parser events.
- **no-remote-trace**—Set remote tracing as disabled.

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- General Packet Radio Service for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security SIP ALG)

**Syntax**

```
traceoptions {
  flag flag <detail | extensive | terse>;
}
```

**Hierarchy Level** [edit security alg sip]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure Session Initiation Protocol (SIP) tracing options.

**Options**

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace with all flags enabled.
  - **call**—Trace call processing activity.
  - **chassis-cluster**—Trace chassis cluster information.
  - **nat**—Trace SIP Network Address Translation (NAT) processing activity.
  - **parser**—Trace SIP parser operations.
  - **rm**—Trace SIP Resource Management (Resmgr) functions activity.
- detail—Display moderate amount of data in trace.
- extensive—Display extensive amount of data in trace.
- terse—Display minimum amount of data in trace.

**Required Privilege Level**
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- SIP ALGs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security User Identification)

**Syntax**

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

**Hierarchy Level** [edit security user-identification]

**Release Information** Statement introduced in Release 12.1 of Junos OS.

**Description** Configure flow tracing options.

**Options**

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

    Syntax: ***x* K** to specify KB, ***x* m** to specify MB, or ***x* g** to specify GB

    Range: 10 KB through 1 GB


Copyright © 2013, Juniper Networks, Inc.

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform.
  - **all**—Trace with all flags enabled
  - **no-remote-trace**—Set remote tracing as disabled.

**Required Privilege Level**
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

## traceoptions (Security UTM)

**Syntax**
traceoptions flag *flag*;

**Hierarchy Level**
[edit security utm]

**Release Information**
Statement introduced in Release 9.5 of Junos OS.

**Description**
Define tracing operations for UTM features.

**Options**
- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Enable trace for all UTM trace options.
  - **cli**—Trace CLI configuration activity and command changes.
  - **daemon**—Trace daemon information.
  - **ipc**—Trace communication events with Packet Forwarding Engine (PFE).
  - **pfe**—Trace PFE information.

**Required Privilege Level**
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM Basics for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Security Web Filtering)

**Syntax** traceoptions flag *flag*;

**Hierarchy Level** [edit security utm feature-profile web-filtering]

**Release Information** Command introduced in Release 10.1 of Junos OS.
Command introduced in Release 11.4 of Junos OS for Enhanced Web Filtering.

**Description** Define tracing operations for individual Web filtering modules. To specify more than one tracing operation, include multiple flag statements.

**Options**

- *flag*:
  - **all**—Enable all Web filtering trace flags.
  - **basic** —Trace basic information on the Web filtering module.
  - **cache**—Enable Web filtering flags for the Web filtering cache maintained on the Web filtering module.
  - **enhanced**—Enable Web filtering flags for processing through Enhanced Web Filtering.
  - **heartbeat**—Trace connectivity information with Web filter server.
  - **ipc**—Trace Web filtering IPC messages.
  - **packet**—Trace packet information from session management.
  - **profile**—Trace profile configuration information.
  - **requests**—Trace requests sent to Web filter server.
  - **response**—Trace response received from Web filter server.
  - **session manager**—Trace session management information.
  - **socket**—Trace the communication socket with Web filter server.
  - **timer**—Trace aging information for requests sent to server.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## traffic-options

**Syntax**

```
traffic-options {
  sessions-per-client {
    limit value;
    over-limit (block | log-and-permit);
  }
}
```

**Hierarchy Level** [edit security utm utm-policy *policy-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** In an attempt to consume all available resources and hinder the ability of the device, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose a session throttle.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices
- Unified Threat Management

## transaction-timeout

**Syntax** transaction-timeout *value-in-seconds*;

**Hierarchy Level** [edit security alg mgcp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Timeout value for Media Gateway Control Protocol (MGCP) transactions. If the timeout value exceeds transaction will be removed by MGCP transactions ager out processing.

**Options** ***value-in-seconds***—Timeout value.
**Range:** 3 through 50 seconds
**Default:** 30 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- MGCP ALGs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## trickling

**Syntax**

```
trickling {
  timeout value;
}
```

**Hierarchy Level**

[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name*]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name*]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name*]

**Release Information**

Statement introduced in Release 9.5 of Junos OS. Statement updated in Release 11.1 of Junos OS for Sophos support.

**Description**

HTTP trickling is a mechanism used to prevent the HTTP client or server from timing-out during a file transfer or during antivirus scanning. HTTP Trickling is time-based and there is only one parameter to configure for this feature, which is the timeout Interval. By default, trickling is disabled.



WARNING: When you enable the trickling option, keep in mind that trickling might send part of a file to the client during its antivirus scan. It is therefore possible that some of the content could be received by the client before the file has been fully scanned.

**Options**

*value*—Timeout interval in seconds.

**Range:** 0 through 600 seconds

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ttl (Security IDP)

**Syntax**

```
ttl {
  match (equal | greater-than | less-than | not-equal);
  value time-to-live;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol ipv4]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the time-to-live (TTL) value of the packet. This value represents the number of routers the packet can pass through. Each router that processes the packet decrements the TTL by 1; when the TTL reaches 0, the packet is discarded.

**Options**

**match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

**value** ***time-to-live***—The time-to-live value.

**Range:** 0 through 255

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## tunable-name

**Syntax**

```
tunable-name tunable-name {
  tunable-value protocol-value;
}
```

**Hierarchy Level** [edit security idp sensor-configuration detector protocol-name *protocol-name*]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for file format decoding over HTTP using MIME added in Release 11.2 of Junos OS.

**Description** Specify the name of the tunable parameter to enable or disable the protocol detector for each of the service. By default, the protocol decoders for all services are enabled.

**Options** *tunable-name*—Name of the specific tunable parameter.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## tunable-value

**Syntax** tunable-value *protocol-value*;

**Hierarchy Level** [edit security idp sensor-configuration detector protocol-name *protocol-name* tunable-name *tunable-name*]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for file format decoding over HTTP using MIME added in Release 11.2 of Junos OS.

**Description** Specify the value of the tunable parameter to enable or disable the protocol detector for each of the service.

**Options** *tunable-value*—Integer representing a selected option for the switch specified in **tunable-name**. The range of values depends on the options defined for the specified switch.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## tunnel (Security Policies)

**Syntax**

```
tunnel {
  ipsec-group-vpn group-vpn;
  ipsec-vpn vpn-name;
  pair-policy pair-policy;
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit]

**Release Information** Statement introduced in Junos OS Release 8.5. The **ipsec-group-vpn** option added in Junos OS Release 10.2.

**Description** Encapsulate outgoing IP packets and decapsulate incoming IP packets.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

## type (Security Antivirus Feature Profile)

**Syntax** type (juniper-express-engine | kaspersky-lab-engine | sophos-engine);

**Hierarchy Level** [edit security utm feature-profile anti-virus]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Statement updated for Sophos in Release 11.1 of Junos OS.

**Description** Set the antivirus engine that will be used on the device. You can only have one engine type running and you must restart the device if you change engines.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- Unified Threat Management
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## type (Security Content Filtering Notification Options)

**Syntax** type (message | protocol-only);

**Hierarchy Level** [edit security utm feature-profile content-filtering profile *profile-name* notification-options]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** When content is blocked, the client generally still receives a successful response code but with modified content (file replacement) containing a warning message. But with protocol-only notifications, a protocol-specific error code may be returned to the client.

**Options**
- **message**—Send a generic notification.
- **protocol-only**—Send a protocol-specific notification.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices

## type (Security Fallback Block)

**Syntax** type (message | protocol-only);

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options fallback-block]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options fallback-block]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** You can configure notifications for both fallback blocking and fallback nonblocking actions. With protocol-only notifications, a protocol-specific error code may be returned to the client.

**Options**
- message—Send a generic notification.
- protocol-only—Send a protocol-specific notification.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## type (Security IDP Dynamic Attack Group)

**Syntax**

```
type {
  values [anomaly signature];
}
```

**Hierarchy Level** [edit security idp dynamic-attack-group *dynamic-attack-group-name* filters]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify an attack type filter to add attack objects based on the type of attack object (signature or protocol anomaly).

**Options** **values**—Name of the attack type filter.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## type (Security IDP ICMP Headers)

**Syntax**

```
type {
  match (equal | greater-than | less-than | not-equal);
  value type-value;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol icmp]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the primary code that identifies the function of the request/reply.

**Options** **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.

**value** ***type-value***—Match a decimal value.

**Range:** 0 through 255

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## type (Security Virus Detection)

**Syntax** type (message | protocol-only);

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options virus-detection]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options virus-detection]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options virus-detection]

**Release Information** Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** When content is blocked because a virus is found or a scan error occurs, the client generally still receives a successful response code but with modified content (file replacement) containing a warning message. But with protocol-only notifications, a protocol-specific error code may be returned to the client.

**Options**
- message—Send a generic notification.
- protocol-only—Send a protocol-specific notification.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM Express Antivirus Protection for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## type (Security Web Filtering)

**Syntax** type (juniper-enhanced | juniper-local | surf-control-integrated | websense-redirect);

**Hierarchy Level** [edit security utm feature-profile web-filtering]

**Release Information** Command introduced in Release 9.5 of Junos OS.
Command introduced in Release 11.4 of Junos OS for Enhanced Web Filtering.

**Description** Define the type of Web filtering solution or URL filtering solution used by the device.

**Options**
- **juniper-enhanced**—Enable Enhanced Web Filtering on the device.
- **juniper-local** —Enable Juniper Networks local URL filtering on the device.
- **surf-control-integrated**—Enable integrated Web filtering on the device.
- **websense-redirect**—Redirect the URL to the Websense server.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

## uac-policy (Application Services)

**Syntax**
```
uac-policy {
  captive-portal captive-portal;
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]

**Release Information** Statement modified in Junos OS Release 9.4.

**Description** Enable Unified Access Control (UAC) for the security policy. This statement is required when you are configuring the SRX Series device to act as a Junos OS Enforcer in a UAC deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series UAC Appliance .

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## udp (Security IDP Protocol Binding)

**Syntax**

```
udp {
  minimum-port port-number <maximum-port port-number>;
}
```

**Hierarchy Level**

[edit security idp custom-attack *attack-name* attack-type chain protocol-binding]
[edit security idp custom-attack *attack-name* attack-type signature protocol-binding]

**Release Information**

Statement introduced in Release 9.3 of Junos OS.

**Description**

Allow IDP to match the attack for specified UDP port(s).

**Options**

- **minimum-port** ***port-number***—Minimum port in the port range.

  **Range:** 0 through 65,535

- **maximum-port** ***port-number***—Maximum port in the port range.

  **Range:** 0 through 65,535

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## udp (Security IDP Signature Attack)

**Syntax**

```
udp {
  data-length {
    match (equal | greater-than | less-than | not-equal);
    value data-length;
  }
  destination-port {
    match (equal | greater-than | less-than | not-equal);
    value destination-port;
  }
  source-port {
    match (equal | greater-than | less-than | not-equal);
    value source-port;
  }
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Allow IDP to match the UDP header information for the signature attack.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## udp (Security Screen)

**Syntax**

```
udp {
  flood {
    threshold number;
  }
  udp-sweep {
    threshold threshold number;
  }
}
```

**Hierarchy Level** [edit security screen ids-option *screen-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the number of packets allowed per second to the same destination IP address/port pair. When the number of packets exceeds this value within any 1-second period, the device generates an alarm and drops subsequent packets for the remainder of that second.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Security Configuration Statement Hierarchy

## udp-anticipated-timeout (Security IDP)

**Syntax** udp-anticipated-timeout *value*;

**Hierarchy Level** [edit security idp sensor-configuration flow]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Sets the maximum UDP anticipated timeout value (range: 1 through 65535).

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## udp-sweep

**Syntax**

```
udp-sweep {
  threshold number;
}
```

**Hierarchy Level** [edit security screen ids-option *screen-name* udp]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure the device to detect and prevent UDP sweep attack. In a UDP sweep attack, an attacker sends UDP packets to the target device. If the device responds to those packets, the attacker gets an indication that a port in the target device is open, which makes the port vulnerable to attack. If a remote host sends UDP packets to 10 addresses in 0.005 seconds (5000 microseconds), then the device flags this as an UDP sweep attack.

If the **alarm-without-drop** option is not set, the device rejects the eleventh and all further UDP packets from that host for the remainder of the specified threshold period.

**Options**

**threshold *number***—Maximum number of microseconds during which up to 10 UDP packets from the same host are allowed into the device. More than 10 requests from a host during this period triggers an UDP Sweep attack response on the device during the remainder of the second.

**Range:** 1000 through 1,000,000 microseconds

**Default:** 5000 microseconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Configuration Statement Hierarchy

Copyright © 2013, Juniper Networks, Inc.

## unified-access-control

**Syntax** unified-access-control (disable | priority *priority*);

**Hierarchy Level** [edit security user-identification authentication-source]

**Release Information** Statement introduced in Release 12.1 of Junos OS.

**Description** An authentication table pushed from a configured authentication device, such as the Junos Pulse Access Control Service.

**Options**

- **disable**—Disable the unified-access-control authentication table. Remove this keyword to re-enable the table.
- **priority *priority***—A unique value between 1 and 65535 that determines the sequence for searching multiple tables to retrieve a user role. Each authentication table is given a unique priority value. The lower the value, the higher the priority. A table with priority 120 is searched before a table with priority 200. The default priority value of the unified-access-control authentication table is 200.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Understanding User Role Firewalls
- Understanding the User Identification Table


Copyright © 2013, Juniper Networks, Inc.

## unknown-message (Security H323 ALG)

**Syntax**

```
unknown-message {
  permit-nat-applied;
  permit-routed;
}
```

**Hierarchy Level** [edit security alg h323 application-screen]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify how unidentified H.323 messages are handled by the device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown H.323 (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.

This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.

**Options**

- **permit-nat-applied**—Specify that unknown messages be allowed to pass if the session is in NAT mode.
- **permit-routed**—Specify that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- H.323 ALGs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## unknown-message (Security MGCP ALG)

**Syntax**

```
unknown-message {
  permit-nat-applied;
  permit-routed;
}
```

**Hierarchy Level** [edit security alg mgcp application-screen]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify how unidentified Media Gateway Control Protocol (MGCP) messages are handled by the device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown MGCP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.

This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.

**Options**

- **permit-nat-applied**—Specify that unknown messages be allowed to pass if the session is in NAT mode.
- **permit-routed**— Specify that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- MGCP ALGs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## unknown-message (Security SCCP ALG)

**Syntax**

```
unknown-message {
  permit-nat-applied;
  permit-routed;
}
```

**Hierarchy Level** [edit security alg sccp application-screen]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify how unidentified Skinny Client Control Protocol (SCCP) messages are handled by the device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown SCCP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.

This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.

**Options**

- **permit-nat-applied**—Specify that unknown messages be allowed to pass if the session is in NAT mode.
- **permit-routed**— Specify that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- SCCP ALGs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## unknown-message (Security SIP ALG)

**Syntax**

```
unknown-message {
  permit-nat-applied;
  permit-routed;
}
```

**Hierarchy Level** [edit security alg sip application-screen]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify how unidentified Session Initiation Protocol (SIP) messages are handled by the device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown SIP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.

This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.

**Options**

- **permit-nat-applied**—Specify that unknown messages be allowed to pass if the session is in NAT mode.
- **permit-routed**— Specify that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- SIP ALGs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## upload-profile (Security Antivirus FTP)

**Syntax** upload-profile *profile-name*;

**Hierarchy Level** [edit security utm utm-policy *policy-name* anti-virus ftp]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the antivirus FTP (upload) protocol and attach this policy to a security profile to implement it.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## upload-profile (Security Content Filtering FTP)

**Syntax** upload-profile *profile-name*;

**Hierarchy Level** [edit security utm utm-policy *policy-name* content-filtering ftp]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure a UTM policy for the content-filtering FTP (upload) protocol and attach this policy to a security profile to implement it.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM Content Filtering for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## urgent-pointer

**Syntax**

```
urgent-pointer {
  match (equal | greater-than | less-than | not-equal);
  value urgent-pointer;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the data in the packet is urgent; the URG flag must be set to activate this field.

**Options**

- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***urgent-pointer***—Match the value of the urgent pointer.

  **Range:** 0 through 65,535

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## uri-check

**Syntax** uri-check;

**Hierarchy Level** [edit security utm feature-profile anti-virus sophos-engine profile *profile-name* scan-options]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Perform Sophos antivirus Uniform Resource Identifier (URI) checking. URI checking is a way of analyzing URI content in HTTP traffic against a remote Sophos database to identify malware or malicious content. URI checking is on by default.

You can disable Sophos antivirus URI checking with the **no-uri-check** statement.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management


Copyright © 2013, Juniper Networks, Inc.

## url (Security Antivirus)

**Syntax** url *url*;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine pattern-update]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update]
[edit security utm feature-profile anti-virus sophos-engine pattern-update]

**Release Information** Statement introduced in Release 9.5 of Junos OS for Juniper Express engine and Kaspersky Lab engine. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description** Specify the URL for the pattern database. You should not change the default URL unless you are experiencing problems with it and have called for support.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM Express Antivirus Protection for Security Devices

## url (Security IDP)

**Syntax** url *url-name*;

**Hierarchy Level** [edit security idp security-package]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** Specify the URL to automatically download the updated signature database.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices
- IDP Signature Database for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## url-blacklist

**Syntax** url-blacklist *listname*;

**Hierarchy Level** [edit security utm feature-profile web-filtering]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** This is a global blacklist category, blocking content for web-filtering.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## url-pattern

**Syntax**

```
url-pattern object-name {
  value [value];
}
```

**Hierarchy Level** [edit security utm custom-objects]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Use URL pattern lists to create custom URL category lists. These are lists of patterns that bypass scanning.



WARNING: Custom category does not take precedence over pre-defined categories when it has the same name as one of the pre-defined categories. It is recommended not to have a custom category name be the same as the predefined category name.

**Options**

- ***object-name***—Name of the URL list object.
- **value *value***—Value of the URL list object. You can configure multiple values separated by spaces and enclosed in square brackets.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices
- Security Policy
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## url-whitelist (Security Antivirus)

**Syntax** url-whitelist *listname*;

**Hierarchy Level** [edit security utm feature-profile anti-virus]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** A URL white list is a unique custom list that you define in which all the URLs or IP addresses in that list for a specified category are always bypassed for scanning.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices

## url-whitelist (Security Web Filtering)

**Syntax** url-whitelist *listname*;

**Hierarchy Level** [edit security utm feature-profile web-filtering]

**Description** A URL white list is a unique custom list that you define in which all the URLs or IP addresses in that list for a specified category are always bypassed for filtering

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## user (Security Dynamic VPN)

**Syntax** user *username*;

**Hierarchy Level** [edit security dynamic-vpn client *configuration-name*]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Specify which users can access the selected dynamic VPN configuration.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Dynamic VPNs for Security Devices

## user-at-hostname

**Syntax** user-at-hostname *e-mail-address*;

**Hierarchy Level** [edit security group-vpn server ike gateway *gateway-name* dynamic]
[edit security ike gateway *gateway-name* dynamic]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn server** hierarchy added in Release 10.2 of Junos OS.

**Description** Configure an e-mail address. (This statement is not supported on dynamic VPN implementations.)

**Options** ***e-mail-address*** —Valid e-mail address.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## user-groups (Security Dynamic VPN)

**Syntax** user-groups *user-group-name*;

**Hierarchy Level** [edit security dynamic-vpn client *configuration-name*]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify which users can access the selected dynamic VPN configuration.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Dynamic VPNs for Security Devices

## user-identification

**Syntax**

```
user-identification {
  authentication-source {
    local-authentication-table (disable | priority priority);
    unified-access-control (disable | priority priority);
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Release 12.1 of Junos OS.

**Description** Identifies one or more tables to be used as the source for user role information.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Understanding User Role Firewalls
- Understanding the User Identification Table


Copyright © 2013, Juniper Networks, Inc.

## username (Security Antivirus)

**Syntax** username *name*;

**Hierarchy Level** [edit security utm feature-profile anti-virus juniper-express-engine pattern-update proxy]
[edit security utm feature-profile anti-virus kaspersky-lab-engine pattern-update proxy]
[edit security utm feature-profile anti-virus sophos-engine pattern-update proxy]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Set the username for the proxy server.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- Unified Threat Management
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## utm

**Syntax**

```
utm {
  application-proxy {
    traceoptions {
      flag flag;
    }
  }
  custom-objects {
    custom-url-category object-name {
      value [value];
    }
    filename-extension object-name {
      value [value];
    }
    mime-pattern object-name {
      value [value];
    }
    protocol-command object-name {
      value [value];
    }
    url-pattern object-name {
      value [value];
    }
  }
  feature-profile {
    anti-spam {
      address-blacklist list-name;
      address-whitelist list-name;
      sbl {
        profile profile-name {
          custom-tag-string [string];
          (sbl-default-server | no-sbl-default-server);
          spam-action (block | tag-header | tag-subject);
        }
      }
      traceoptions {
        flag flag;
      }
    }
    anti-virus {
      juniper-express-engine {
        pattern-update {
          email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
          }
          interval value;
          no-autoupdate;
          proxy {
            password password-string;
            port port-number;
            server address-or-url;
```


Copyright © 2013, Juniper Networks, Inc.

```
            username name;
          }
          url url;
        }
        profile profile-name {
          fallback-options {
            content-size (block | log-and-permit);
            default (block | log-and-permit);
            engine-not-ready (block | log-and-permit);
            out-of-resources (block | (log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
          }
          notification-options {
            fallback-block {
              administrator-email email-address;
              allow-email;
              custom-message message;
              custom-message-subject message-subject;
              display-host;
              (notify-mail-sender | no-notify-mail-sender);
              type (message | protocol-only);
            }
            fallback-non-block {
              custom-message message;
              custom-message-subject message-subject;
              (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
              custom-message message;
              custom-message-subject message-subject;
              (notify-mail-sender | no-notify-mail-sender);
              type (message | protocol-only);
            }
          }
          scan-options {
            content-size-limit value;
            (intelligent-prescreening | no-intelligent-prescreening);
            timeout value;
          }
          trickling {
            timeout value;
          }
        }
      }
      kaspersky-lab-engine {
        pattern-update {
          email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
          }
          interval value;
          no-autoupdate;
          proxy {
            password password-string;
```

```
            port port-number;
            server address-or-url;
            username name;
          }
          url url;
        }
        profile profile-name {
          fallback-options {
            content-size (block | log-and-permit);
            corrupt-file (block | log-and-permit);
            decompress-layer (block | log-and-permit);
            default (block | log-and-permit);
            engine-not-ready (block | log-and-permit);
            out-of-resources (block | (log-and-permit);
            password-file (block | (log-and-permit);
            timeout (block | log-and-permit);
            too-many-requests (block | log-and-permit);
          }
          notification-options {
            fallback-block {
              administrator-email email-address;
              allow-email;
              custom-message message;
              custom-message-subject message-subject;
              display-host;
              (notify-mail-sender | no-notify-mail-sender);
              type (message | protocol-only);
            }
            fallback-non-block {
              custom-message message;
              custom-message-subject message-subject;
              (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
              custom-message message;
              custom-message-subject message-subject;
              (notify-mail-sender | no-notify-mail-sender);
              type (message | protocol-only);
            }
          }
          scan-options {
            content-size-limit value;
            decompress-layer-limit value;
            (intelligent-prescreening | no-intelligent-prescreening);
            scan-extension filename;
            scan-mode (all | by-extension);
            timeout value;
          }
          trickling {
            timeout value;
          }
        }
      }
      mime-whitelist {
        exception listname;
        list listname {
```


Copyright © 2013, Juniper Networks, Inc.

```
        exception listname;
    }
}
sophos-engine {
    pattern-update {
        email-notify {
            admin-email email-address;
            custom-message message;
            custom-message-subject message-subject;
        }
        interval value;
        no-autoupdate;
        proxy {
            password password-string;
            port port-number;
            server address-or-url;
            username name;
        }
        url url;
    }
    profile <name> {
        fallback-options {
            content-size (block | log-and-permit | permit);
            default (block | log-and-permit | permit);
            engine-not-ready (block | log-and-permit | permit);
            out-of-resources (block | log-and-permit | permit);
            timeout (block | log-and-permit | permit);
            too-many-requests (block | log-and-permit | permit);
        }
        notification-options {
            fallback-block {
                administrator-email email-address;
                allow-email;
                custom-message message;
                custom-message-subject message-subject;
                display-host;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
            fallback-non-block {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-recipient | no-notify-mail-recipient);
            }
            virus-detection {
                custom-message message;
                custom-message-subject message-subject;
                (notify-mail-sender | no-notify-mail-sender);
                type (message | protocol-only);
            }
        }
        scan-options {
            content-size-limit value;
            (no-uri-check | uri-check);
            timeout value;
        }
```

```
        trickling {
          timeout value;
        }
      }
      sxl-retry value;
      sxl-timeout seconds;
    }
    traceoptions {
      flag flag;
    }
    type (juniper-express-engine | kaspersky-lab-engine | sophos-engine);
    url-whitelist listname;
  }
  content-filtering {
    profile profile-name {
      block-command protocol-command-list;
      block-content-type (activex | exe | http-cookie | java-applet | zip);
      block-extension extension-list;
      block-mime {
        exception list-name;
        list list-name;
      }
      notification-options {
        custom-message message;
        (notify-mail-sender | no-notify-mail-sender);
        type (message | protocol-only);
      }
      permit-command protocol-command-list;
    }
    traceoptions {
      flag flag;
    }
  }
  web-filtering {
    juniper-enhanced {
      cache {
        size value;
        timeout value;
      }
      profile profile-name {
        block-message {
          type {
            custom-redirect-url;
          }
          url url;
          }
        quarantine-message {
          type {
            custom-redirect-url;
          }
            url url;
            }
        category customurl-list name {
          action (block | log-and-permit | permit | quarantine);
        }
        custom-block-message value;
```


Copyright © 2013, Juniper Networks, Inc.

```
        custom-quarantine-message value;
        default (block | log-and-permit | permit | quarantine);
        fallback-settings {
          default (block | log-and-permit);
          server-connectivity (block | log-and-permit);
          timeout (block | log-and-permit);
          too-many-requests (block | log-and-permit);
        }
        no-safe-search;
        site-reputation-action {
          fairly-safe (block | log-and-permit | permit | quarantine);
          harmful (block | log-and-permit | permit | quarantine);
          moderately-safe (block | log-and-permit | permit | quarantine);
          suspicious (block | log-and-permit | permit | quarantine);
          very-safe (block | log-and-permit | permit |quarantine);
        }
        timeout value;
      }
      server {
        host host-name;
        port number;
      }
    }
    juniper-local {
      profile profile-name {
        custom-block-message value;
        default (block | log-and-permit | permit);
        fallback-settings {
          default (block | log-and-permit);
          server-connectivity (block | log-and-permit);
          timeout (block | log-and-permit);
          too-many-requests (block | log-and-permit);
        }
        timeout value;
      }
    }
    surf-control-integrated {
      cache {
        size value;
        timeout value;
      }
      profile profile-name {
        category customurl-list name {
          action (block | log-and-permit | permit);
        }
        custom-block-message value;
        default (block | log-and-permit | permit);
        fallback-settings {
          default (block | log-and-permit);
          server-connectivity (block | log-and-permit);
          timeout (block | log-and-permit);
          too-many-requests (block | log-and-permit);
        }
        timeout value;
      }
      server {
```

```
            host host-name;
            port number;
          }
        }
        traceoptions {
          flag flag;
        }
        type (juniper-enhanced | juniper-local | surf-control-integrated | websense-redirect);
        url-blacklist listname;
        url-whitelist listname;
        websense-redirect {
          profile profile-name {
            account value;
            custom-block-message value;
            fallback-settings {
              default (block | log-and-permit);
              server-connectivity (block | log-and-permit);
              timeout (block | log-and-permit);
              too-many-requests (block | log-and-permit);
            }
            server {
              host host-name;
              port number;
            }
            sockets value;
            timeout value;
          }
        }
      }
    }
    ipc {
      traceoptions flag flag;
    }
    traceoptions {
      flag flag;
    }
    utm-policy policy-name {
      anti-spam {
        smtp-profile profile-name;
      }
      anti-virus {
        ftp {
          download-profile profile-name;
          upload-profile profile-name;
        }
        http-profile profile-name;
        imap-profile profile-name;
        pop3-profile profile-name;
        smtp-profile profile-name;
      }
      content-filtering {
        ftp {
          download-profile profile-name;
          upload-profile profile-name;
        }
        http-profile profile-name;
```


Copyright © 2013, Juniper Networks, Inc.

```
        imap-profile profile-name;
        pop3-profile profile-name;
        smtp-profile profile-name;
      }
      traffic-options {
        sessions-per-client {
          limit value;
          over-limit (block | log-and-permit);
        }
      }
      web-filtering {
        http-profile profile-name;
      }
    }
  }
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure UTM features.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- UTM for Security Devices
- SMTP

Copyright © 2013, Juniper Networks, Inc.

## utm-policy

**Syntax**

```
utm-policy policy-name {
  anti-spam {
    smtp-profile profile-name;
  }
  anti-virus {
    ftp {
      download-profile profile-name;
      upload-profile profile-name;
    }
    http-profile profile-name;
    imap-profile profile-name;
    pop3-profile profile-name;
    smtp-profile profile-name;
  }
  content-filtering {
    ftp {
      download-profile profile-name;
      upload-profile profile-name;
    }
    http-profile profile-name;
    imap-profile profile-name;
    pop3-profile profile-name;
    smtp-profile profile-name;
  }
  traffic-options {
    sessions-per-client {
      limit value;
      over-limit (block | log-and-permit);
    }
  }
  web-filtering {
    http-profile profile-name;
  }
}
```

**Hierarchy Level** [edit security utm]

**Release Information** Statement introduced in Junos OS Release 9.5.

**Description** Configure a UTM policy for antivirus, antispam, content-filtering, traffic-options, and web-filtering protocols and attach this policy to a security profile to implement it.

**Options** *policy-name*—Specify name of the UTM policy.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

- Unified Threat Management
- UTM for Security Devices

## utm-policy (Application Services)

**Syntax** utm-policy *policy-name*;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services]

**Release Information** Statement introduced in Junos OS Release 11.1.

**Description** Configure a UTM policy for application services and attach this policy to a security profile to implement it.

**Options** ***policy-name***—Specify the name of the UTM policy.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM Content Filtering for Security Devices
- Unified Threat Management

Copyright © 2013, Juniper Networks, Inc.

## value-hit-rate-threshold

**Syntax** value-hit-rate-threshold *number*;

**Hierarchy Level** [edit security idp application-ddos *application-name* context *context-name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure the context-value-hit-rate threshold in tick interval. A tick is defined as 60 seconds by default. When the same context value is requested for more than value-hit-rate-threshold limit for a given context and application-level distributed denial-of-service (DDoS) application, the system will start bot client classification, if time-binding parameters are configured. If time-binding parameters are not configured, the configured policy actions are taken.



NOTE: If time-binding is not configured, the system will skip bot client classification, and the configured policy actions are taken. This could result in valid clients being applied with configured policy actions. Time-binding configuration (count and period) should be used for bot client classification. However, this feature can be used as an Application Layer screen to deny resource access for all clients when context value-hit-rate-threshold is exceeded.

**Options** *number*—Context value hit rate threshold.

**Range:**

- SRX3400– 1 to 250,000,000
- SRX3600–1 to 500,000,000
- SRX5600/5800–1 to 2,500,000,000

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application-Level Distributed Denial of Service


Copyright © 2013, Juniper Networks, Inc.

## version (Security GTP)

**Syntax**

```
version v1 {
  number ie-number;
  release (R6 | R7 | R8 | R9);
}
```

**Hierarchy Level** [edit security gprs gtp profile profile-name remove-ie]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Specify GTP version.

**Options**

- **v1**—GTP version 1.
- **release** —Specify release number. Available options are:
  - Release R6—Specify R6 IE removal.
  - Release R7—Specify R7 IE removal.
  - Release R8—Specify R8 IE removal.
  - Release R9—Specify R9 IE removal.
- **number** —Specify the user-configured IE number. IE removal by IE number supports all IEs, ranging from 1 to 255.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- General Packet Radio Service for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## version (Security IKE Gateway)

**Syntax** version (v1-only | v2-only);

**Hierarchy Level** [edit security ike gateway *gateway-name*]

**Release Information** Statement introduced in Release 11.3 of Junos OS.

**Description** Specify the IKE version to use to initiate the connection.

**Options** **v1-only**—The connection must be initiated using IKE version 1. This is the default.

**v2-only**—The connection must be initiated using IKE version 2.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## virus-detection (Security Antivirus)

**Syntax**

```
virus-detection {
    custom-message message;
    custom-message-subject message-subject;
    (notify-mail-sender | no-notify-mail-sender);
    type (message | protocol-only);
}
```

**Hierarchy Level**

[edit security utm feature-profile anti-virus juniper-express-engine profile *profile-name* notification-options]
[edit security utm feature-profile anti-virus kaspersky-lab-engine profile *profile-name* notification-options]
[edit security utm feature-profile anti-virus sophos-engine profile *profile-name* notification-options]

**Release Information**

Statement introduced in Release 9.5 of Junos OS. Support for Sophos engine added in Release 11.1 of Junos OS.

**Description**

Configure a notification to send when a virus is detected.

**Options**

The remaining statements are explained separately.

**Required Privilege Level**

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- UTM for Security Devices
- UTM Full Antivirus Protection for Security Devices
- Unified Threat Management
- UTM Express Antivirus Protection for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## vpn (Security)

**Syntax**

```
vpn vpn-name {
  bind-interface interface-name;
  df-bit (clear | copy | set);
  establish-tunnels (immediately | on-traffic);
  ike {
    gateway gateway-name;
    idle-time seconds;
    install-interval seconds;
    ipsec-policy ipsec-policy-name;
    no-anti-replay;
    proxy-identity {
      local ip-prefix;
      remote ip-prefix;
      service (any | service-name);
    }
  }
  manual {
    authentication {
      algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
      key (ascii-text key | hexadecimal key);
    }
    encryption {
      algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
      key (ascii-text key | hexadecimal key);
    }
    external-interface external-interface-name;
    gateway ip-address;
    protocol (ah | esp);
    spi spi-value;
  }
  vpn-monitor {
    destination-ip ip-address;
    optimized;
    source-interface interface-name;
  }
}
```

**Hierarchy Level** [edit security ipsec]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for IPv6 addresses added in Release 11.1 of Junos OS.

**Description** Configure an IPsec VPN.

**Options** *vpn-name* —Name of the VPN.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.


Copyright © 2013, Juniper Networks, Inc.

**Related Documentation**

- AutoVPNs for Security Devices
- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

## vpn-monitor

**Syntax**

```
vpn-monitor {
  destination-ip ip-address;
  optimized;
  source-interface interface-name;
}
```

**Hierarchy Level** [edit security ipsec vpn *vpn-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure settings for VPN monitoring. This feature cannot be configured simultaneously with the dead-peer-detection statement. (This statement is not supported on dynamic VPN implementations.)

**Options** The remaining statements are explained separately.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## vpn-monitor-options

**Syntax**

```
vpn-monitor-options {
    interval seconds;
    threshold number;
}
```

**Hierarchy Level** [edit security ipsec]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure VPN monitoring options. (This statement is not supported on dynamic VPN implementations.)

**Options**

- **interval** ***seconds*** —Interval at which to send ICMP requests to the peer.

  **Range:** 2 through 3600 seconds
  **Default:** 10 seconds

- **threshold** ***number*** —Number of consecutive unsuccessful pings before the peer is declared unreachable.

  **Range:** 1 through 65536 pings
  **Default:** 10 pings

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## web-authentication

**Syntax**

```
web-authentication {
    client-match user-or-group-name;
}
```

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit firewall-authentication]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify that the policy allows access to users who have previously been authenticated by Web authentication. Web authentication must be enabled on one of the addresses on the interface to which the HTTP request is redirected.

**Options** **client-match** ***user-or-group*** —(Optional) Username or user group name.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## web-filtering

**Syntax**

```
web-filtering {
  juniper-enhanced {
    cache {
      size value;
      timeout value;
    }
    profile profile-name {
      category customurl-list name {
        action (block | log-and-permit | permit | quarantine);
      }
      custom-block-message value;
      custom-quarantine-message value;
      default (block | log-and-permit | permit | quarantine);
      fallback-settings {
        default (block | log-and-permit);
        server-connectivity (block | log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
      }
      no-safe-search;
      site-reputation-action {
        fairly-safe (block | log-and-permit | permit | quarantine);
        harmful (block | log-and-permit | permit | quarantine);
        moderately-safe (block | log-and-permit | permit | quarantine);
        suspicious (block | log-and-permit | permit | quarantine);
        very-safe (block | log-and-permit | permit | quarantine);
      }
      timeout value;
    }
    server {
      host host-name;
      port number;
    }
  }
  juniper-local {
    profile profile-name {
      custom-block-message value;
      default (block | log-and-permit | permit);
      fallback-settings {
        default (block | log-and-permit);
        server-connectivity (block | log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
      }
      timeout value;
    }
  }
  surf-control-integrated {
    cache {
      size value;
      timeout value;
    }
```


Copyright © 2013, Juniper Networks, Inc.

```
    profile profile-name {
      category customurl-list name {
        action (block | log-and-permit | permit);
      }
      custom-block-message value;
      default (block | log-and-permit | permit);
      fallback-settings {
        default (block | log-and-permit);
        server-connectivity (block | log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
      }
      timeout value;
    }
    server {
      host host-name;
      port number;
    }
  }
  traceoptions flag flag;
  type (juniper-enhanced | juniper-local | surf-control-integrated | websense-redirect);
  url-blacklist listname;
  url-whitelist listname;
  websense-redirect {
    profile profile-name {
      account value;
      custom-block-message value;
      fallback-settings {
        default (block | log-and-permit);
        server-connectivity (block | log-and-permit);
        timeout (block | log-and-permit);
        too-many-requests (block | log-and-permit);
      }
      server {
        host host-name;
        port number;
      }
      sockets value;
      timeout value;
    }
  }
}
```

**Hierarchy Level** [edit security utm feature-profile]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure UTM web-filtering features.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Copyright © 2013, Juniper Networks, Inc.

**Related Documentation**

- Unified Threat Management
- Understanding Local Web Filtering
- Monitoring Web Filtering Configurations
- UTM for Security Devices

## web-redirect

**Syntax** web-redirect;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit firewall-authentication pass-through]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Optionally, redirect HTTP requests to the device's internal webserver by sending a redirect HTTP response to the client system to reconnect to the webserver for user authentication. The interface on which the client's request arrived is the interface to which the request is redirected.

Using this feature allows for a richer user login experience. For example. instead of a popup prompt asking for username and password, users can get the login page in a browser. Enabling **web-redirect** has the same effect as users typing the Web authentication IP address in a client browser. Using **web-redirect** provides a more seamless authentication experience because users do not need to know the Web authentication IP address but only the IP address of the resource they are trying to access. After the user has been authenticated this way, traffic from user's IP address is authenticated to go through the **web-redirect** method.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Policies for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## web-redirect-to-https

**Syntax** web-redirect-to-https;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit firewall-authentication pass-through]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Redirect unauthenticated HTTP requests to the internal HTTPS Web server of the device.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Unified Threat Management
- UTM for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## websense-redirect

**Syntax**

```
websense-redirect {
  profile profile-name {
    account value;
    custom-block-message value;
    fallback-settings {
      default (block | log-and-permit);
      server-connectivity (block | log-and-permit);
      timeout (block | log-and-permit);
      too-many-requests (block | log-and-permit);
    }
    server {
      host host-name;
      port number;
    }
    sockets value;
    timeout value;
  }
}
```

**Hierarchy Level** [edit security utm feature-profile web-filtering]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure the websense redirect engine features.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## weight (Security)

**Syntax** weight (equal | firewall | idp);

**Hierarchy Level** [edit security forwarding-process application-services maximize-idp-sessions]

**Release Information** Statement introduced in Release 9.6 of Junos OS.

**Description** If you are deploying IDP policies, you can tune the device to increase IDP session capacity. By using the provided commands to change the way the system allocates resources, you can achieve a higher IDP session capacity.

Devices ship with an implicit default session capacity setting. This default value gives more weight to firewall sessions. You can manually override the default by using the **maximize-idp-sessions** command. The command allows you to choose between these weight values: **equal**, **firewall**, and **idp**. The following table displays the available session capacity weight and approximate throughput for each.

### Table 6: Session Capacity and Resulting Throughput

| Weight Value | Firewall Capacity | IDP Capacity | Firewall Throughput | IDP Throughput |
|---|---|---|---|---|
| Default | 1,000,000 | 256,000 | 10 Gbps | 2.4 Gbps |
| **equal** | 1,000,000 | 1,000,000 | 8.5 Gbps | 2 Gbps |
| **firewall** | 1,000,000 | 1,000,000 | 10 Gbps | 2.4 Gbps |
| **idp** | 1,000,000 | 1,000,000 | 5.5 Gbps | 1.4 Gbps |

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Processing Overview for Security Devices
- IDP Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## white-list

**Syntax**

```
white-list name {
  destination-address [address];
  source-address [address];
}
```

**Hierarchy Level** [edit security screen ids-option *screen-name* tcp syn-flood]

**Release Information** Statement introduced in Release 12.1 of Junos OS.

**Description** Configure a whitelist of IP addresses that are to be exempt from the SYN cookie and SYN proxy mechanisms that occur during the SYN flood screen protection process.

Both IP version 4 (IPv4) and IP version 6 (IPv6) whitelists are supported. Addresses in a whitelist must be all IPv4 or all IPv6. Each whitelist can have up to 32 IP address prefixes.

**Options**

- **destination-address *address***—Destination IP address or an address prefix. You can configure multiple addresses or address prefixes separated by spaces and enclosed in square brackets.
- **source-address *address***—Source IP address or an address prefix. You can configure multiple addresses or address prefixes separated by spaces and enclosed in square brackets.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Configuration Statement Hierarchy


Copyright © 2013, Juniper Networks, Inc.

## wildcard

**Syntax** wildcard *string*;

**Hierarchy Level** [edit security group-vpn server ike gateway *gateway-name* dynamic distinguished-name]
[edit security ike gateway *gateway-name* dynamic distinguished-name]

**Release Information** Statement introduced in Release 8.5 of Junos OS. Support for **group-vpn server** hierarchy added in Release 10.2 of Junos OS.

**Description** Specify that the values of a dynamic virtual private network (VPN) endpoint user's distinguished name's identity fields match the values in the group IKE user's distinguished name's fields. The order of the identity fields in the distinguished name strings does not matter during a match. (This statement is not supported on dynamic VPN implementations.)

**Options** ***string***—Distinguished name identity values to be matched.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## window-scale

**Syntax**

```
window-scale {
  match (equal | greater-than | less-than | not-equal);
  value window-scale-factor;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the scale factor that the session of the attack will use. The window scale extension expands the definition of the TCP window to 32 bits and then uses a scale factor to carry this 32-bit value in the 16-bit window field of the TCP header.

**Options**

- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value *window-scale-factor***—Match the number of bytes.

  **Range:** 0 through 255

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## window-size

**Syntax**

```
window-size {
  match (equal | greater-than | less-than | not-equal);
  value window-size;
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol tcp]

**Release Information** Statement introduced in Release 9.3 of Junos OS.

**Description** Specify the number of bytes in the TCP window size.

**Options**

- **match** (**equal** | **greater-than** | **less-than** | **not-equal**)—Match an operand.
- **value** ***window-size***—Match the number of bytes.

  **Range:** 0 through 65,535

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

## winnuke

**Syntax** winnuke;

**Hierarchy Level** [edit security screen ids-option *screen-name* tcp]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable detection of attacks on Windows NetBios communications. Packets are modified as necessary and passed on. Each WinNuke attack triggers an attack log entry in the event alarm log.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Configuration Statement Hierarchy

Copyright © 2013, Juniper Networks, Inc.

## xauth

**Syntax**

```
xauth {
  access-profile profile-name;
}
```

**Hierarchy Level** [edit security ike gateway *gateway-name*]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify that Extended authentication (XAuth) is performed in addition to IKE authentication for remote users trying to access a VPN tunnel. Include a previously created access profile, created with the **edit access profile** statement, to specify the access profile to be used for authentication information.

**Options**

**access-profile** ***profile-name***—Name of previously created access profile to reference for authentication information.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Dynamic VPNs for Security Devices
- Group VPNs for Security Devices
- IPsec VPNs for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## zones

**Syntax**

```
zones {
  functional-zone {
    management {
      description text;
      host-inbound-traffic {
        protocols protocol-name {
          except;
        }
        system-services service-name {
          except;
        }
      }
      interfaces interface-name  {
        host-inbound-traffic {
          protocols protocol-name {
            except;
          }
          system-services service-name {
            except;
          }
        }
      }
      screen screen-name;
    }
  }
  security-zone zone-name {
    address-book {
      address address-name {
        ip-prefix {
          description text;
        }
        description text;
        dns-name domain-name {
          ipv4-only;
          ipv6-only;
        }
        range-address lower-limit to upper-limit;
        wildcard-address ipv4-address/wildcard-mask;
      }
      address-set address-set-name {
        address address-name;
        address-set address-set-name;
        description text;
      }
    }
    application-tracking;
    description text;
    host-inbound-traffic {
      protocols protocol-name {
        except;
      }
      system-services service-name {
```

```
            except;
          }
        }
        interfaces interface-name {
          host-inbound-traffic {
            protocols protocol-name {
              except;
            }
            system-services service-name {
              except;
            }
          }
        }
        screen screen-name;
        tcp-rst;
      }
    }
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Junos OS Release 8.5. Support for wildcard addresses added in Junos OS Release 11.1. The **description** option added in Junos OS Release 12.1.

**Description** A zone is a collection of interfaces for security purposes. All interfaces in a zone are equivalent from a security point of view. Configure the following zones:

- Functional zone—Special-purpose zone, such as a management zone that can host dedicated management interfaces.
- Security zone—Most common type of zone that is used as a building block in policies.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Tracking
- Security Zones and Interfaces for Security Devices
- Logical Systems for Security Devices


Copyright © 2013, Juniper Networks, Inc.

CHAPTER 20

# Services Hierarchy and Statements

This section contains the following topics:


- Services Configuration Statement Hierarchy on page 1133


## Services Configuration Statement Hierarchy

Use the statements in the **services** configuration hierarchy to configure application identification, RPM probes, and Unified Access Control.

```
services {
   application-identification {
      application application-name {
         address-mapping address-name {
            destination {
               ip ip-prefix | wildcard-address ip-addr wildcard-mask wildcard-mask;
               port-range {
                  tcp tcp-port-range;
                  udp udp-port-range;
               }
            }
            order number;
            source {
               ip ip-prefix | wildcard-address ip-addr wildcard-mask wildcard-mask;
               port-range {
                  tcp tcp-port-range;
                  udp udp-port-range;
               }
            }
         }
         icmp-mapping {
            code number;
            type number;
         }
         ip-protocol-mapping {
            protocol number;
         }
         signature {
            client-to-server {
               dfa-pattern pattern;
               regex reg-expression;
            }
```

Copyright © 2013, Juniper Networks, Inc.

```
      insert-before application-name;
      min-data bytes;
      port-range {
        tcp tcp-port-range;
        udp udp-port-range;
      }
      server-to-client {
        dfa-pattern pattern;
        regex reg-expression;
      }
    }
    tags {
      tag-name tag-value;
    }
    type type-name;
  }
  application-group group-name {
    application-groups [application-group-name];
    applications [application-name];
  }
  application-system-cache-timeout value;
  download {
    automatic {
      interval hours;
      start-time  MM-DD.hh:mm;
    }
    url url;
  }
  enable-heuristics;
  max-checked-bytes bytes;
  max-sessions value;
  nested-application name {
    protocol protocol-name;
    signature  signature-name {
      chain-order;
      insert-before application-name;
      maximum-transactions value;
      member name {
        context [http-get-url-parsed-param-parsed | http-header-content-type |
          http-header-cookie | http-header-host | http-header-user-agent |
          http-post-url-parsed-param-parsed | http-post-variable-parsed |
          http-url-parsed | http-url-parsed-param-parsed | ssl-server-name];
        direction [any | client-to-server | server-to-client];
        pattern dfa-pattern;
      }
    }
    type type-name;
  }
  nested-application-settings {
    no-application-system-cache;
    no-nested-application;
  }
  no-application-identification;
  no-application-system-cache;
  statistics {
    interval value;
```


Copyright © 2013, Juniper Networks, Inc.

```
    }
    traceoptions {
      file {
        filename ;
        files number;
        match regular-expression;
        size maximum-file-size;
        world-readable | no-world-readable;
      }
      flag all;
      no-remote-trace;
    }
  }
  ssl {
    proxy {
      profile-name profile-name {
        actions {
          disable-session-resumption;
          ignore-server-auth-failure;
          log [logging-options];
          renegotiation {
            allow | allow-secure | drop;
          }
        }
        custom-ciphers [cipher];
        enable-flow-tracing;
        global-config {
          session-cache-timeout seconds;
        }
        preferred-ciphers [cipher];
        root-ca certificate-id;
        trusted-ca [certificate-id];
        whitelist global-address-book-addresses;
      }
    }
  }
  unified-access-control {
    captive-portal redirect-policy-name{
      redirect-traffic (all | unauthenticated);
      redirect-url redirect-url;
    }
    certificate-verification [ optional | required | warning ];
    infranet-contoller host-name {
      address ip-address;
      ca-profile ca-profile;
      interface interface-name;
      password password;
      port port-number;
      server-certificate-subject subject;
    }
    timeout seconds;
    interval seconds;
    test-only-mode (true | false);
    timeout-action (close | no-change | open);
    traceoptions {
      flag [ (ipc | config | connect | all) ];
```

```
    }
  }
}
```

**Related Documentation**

- Application Identification for Security Devices

  Unified Access Control Solution for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## actions (Services)

**Syntax**

```
actions {
  disable-session-resumption;
  ignore-server-auth-failure;
  log {
    all;
    errors;
    info;
    sessions-allowed;
    sessions-dropped;
    sessions-ignored;
    sessions-whitelisted;
    warning;
  }
  renegotiation (allow | allow-secure | drop);
}
```

**Hierarchy Level** [edit services ssl proxy profile *profile-name*]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the logging and traffic related actions.

**Options**

- **disable-session-resumption**—Disable session resumption.
- **ignore-server-auth-failure**—Ignore server authentication failure.
- **log**—Specify the logging actions.
  - **all**—Log all events.
  - **errors**—Log all error events.
  - **info**—Log all information events.
  - **sessions-allowed**—Log SSL session allowed events after an error.
  - **sessions-dropped**—Log only SSL session dropped events.
  - **sessions-ignored**—Log session ignored events.
  - **sessions-whitelisted**—Log SSL session whitelisted events.
  - **warning**—Log all warning events.
- **renegotiation**—Specify the renegotiation options.
  - **allow**—Allow secure and nonsecure renegotiation.
  - **allow-secure**—Allow secure negotiation only.
  - **drop**—Drop session on renegotiation request.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Copyright © 2013, Juniper Networks, Inc.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## address (Services)

**Syntax** address *ip-address*;

**Hierarchy Level** [edit services unified-access-control infranet-controller *hostname*]

**Release Information** Statement introduced in Junos OS Release 9.4.

**Description** Specify the IP address of the IC Series device with which the SRX Series devices should communicate.

This statement is required when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series device.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- infranet-controller on page 1158
- Unified Access Control Solution for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## application (Services)

**Syntax**

```
application application-name {
  address-mapping address-name {
    destination {
      ip ip-prefix | wildcard-address ip-addr wildcard-mask wildcard-mask;
      port-range {
        tcp tcp-port-range;
        udp udp-port-range;
      }
    }
    order number;
    source {
      ip ip-prefix | wildcard-address ip-addr wildcard-mask wildcard-mask;
      port-range {
        tcp tcp-port-range;
        udp udp-port-range;
      }
    }
  }
  icmp-mapping {
    code number;
    type number;
  }
  ip-protocol-mapping {
    protocol number;
  }
  signature {
    client-to-server {
      dfa-pattern pattern;
      regex reg-expression;
    }
    insert-before application-name;
    min-data bytes;
    port-range {
      tcp tcp-port-range;
      udp udp-port-range;
    }
    server-to-client {
      dfa-pattern pattern;
      regex reg-expression;
    }
  }
  tags {
    tag-name tag-value;
  }
  type type-name;
}
```

**Hierarchy Level** [edit services application-identification]

**Release Information** Statement introduced in Junos OS Release 10.2. Statement updated in Junos Os Release 11.4. Statement updated in Junos OS Release 12.1X44-D10.

Copyright © 2013, Juniper Networks, Inc.

**Description** Configure a custom application definition for the desired application name that will be used by the system to identify the application as it passes through the device. Custom application definitions can be used for applications that are not part of the Juniper Networks predefined application database.

**Options** **type** ***name***—(Optional; used by IDP.) Well known application name, such as FTP, TELNET, HTTP. Must be a unique name with a maximum length of 32 characters.

The remaining statements are explained separately.

**Required Privilege Level** trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**
- Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## application-group (Services)

**Syntax**

```
application-group group-name {
  application-groups {
    app-group-name;
  }
  applications {
    app-name;
  }
}
```

**Hierarchy Level** [edit services application-identification]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify any number of associated predefined applications, user-defined applications, and other groups for ease of use in configuring application-based policies.

An application group is hierarchical: a tree structure of groups with applications as the leaf nodes.

**Options**

- ***group-name***—Name of the group. This name is used in policy configuration statements in place of multiple predefined applications, user-defined applications, or other groups.
- **application-groups *app-group-name***—Name of an application group to be assigned to this group. There is no maximum number of groups that can be assigned to a group. Use multiple commands to assign multiple groups.
- **applications *app-name***—Name of an application to be assigned to this group. An application can remain unassigned or be assigned to a group, but it cannot be assigned to more than one group. There is no maximum number of applications that can be assigned to a group. Use multiple commands to assign multiple groups.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## application-identification

**Syntax**

```
application-identification {
  application application-name {
    address-mapping address-name {
      destination {
        ip ip-prefix | wildcard-address ip-addr wildcard-mask wildcard-mask;
        port-range {
          tcp tcp-port-range;
          udp udp-port-range;
        }
      }
      order number;
      source {
        ip ip-prefix | wildcard-address ip-addr wildcard-mask wildcard-mask;
        port-range {
          tcp tcp-port-range;
          udp udp-port-range;
        }
      }
    }
    icmp-mapping {
      code number;
      type number;
    }
    ip-protocol-mapping {
      protocol number;
    }
    signature {
      client-to-server {
        dfa-pattern pattern;
        regex reg-expression;
      }
      insert-before application-name;
      min-data bytes;
      port-range {
        tcp tcp-port-range;
        udp udp-port-range;
      }
      server-to-client {
        dfa-pattern pattern;
        regex reg-expression;
      }
    }
    tags {
      tag-name tag-value;
    }
    type type-name;
  }
  application-group group-name {
    application-groups {
      application-group-name;
    }
    applications {
```


Copyright © 2013, Juniper Networks, Inc.

```
        application-name;
      }
    }
    application-system-cache-timeout value;
    download {
      automatic {
        interval hours;
        start-time  MM-DD.hh:mm;
      }
      url url;
    }
    enable-heuristics;
    max-checked-bytes bytes;
    max-sessions value;
    nested-application name {
      protocol protocol-name;
      signature signature-name {
        chain-order;
        insert-before application-name;
        maximum-transactions value;
        member name {
          check-bytes value;
          context [http-get-url-parsed-param-parsed | http-header-content-type |
            http-header-cookie | http-header-host | http-header-user-agent |
            http-post-url-parsed-param-parsed | http-post-variable-parsed | http-url-parsed
            | http-url-parsed-param-parsed | ssl-server-name | stream ];
          direction [any | client-to-server | server-to-client];
          pattern dfa-pattern;
        }
      }
      type name;
    }
    nested-application-settings {
      no-application-system-cache;
      no-nested-application;
    }
    no-application-identification;
    no-application-system-cache;
    statistics {
      interval value;
    }
    traceoptions {
      file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
      }
      flag flag;
      no-remote-trace;
    }
  }
```

**Hierarchy Level** [edit services]

Copyright © 2013, Juniper Networks, Inc.

**Release Information** Statement introduced in Junos OS Release 10.2. Statement updated in Junos OS Release 11.4. Statement updated in Junos OS Release 12.1X44-D10.

**Description** Configure application identification options to identify the TCP/UDP application session running on nonstandard ports to match the application properties of transiting network traffic.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Identification for Security Devices

## application-system-cache

**Syntax** application-system-cache;

**Hierarchy Level** [edit services application-identification]

**Release Information** Statement introduced in Release 9.2 of Junos OS.

**Description** When a session is created, specify an application ID to match the application properties of transiting network traffic. The application port mappings are saved in the application system cache.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## application-system-cache-timeout (Services)

**Syntax** application-system-cache-timeout *value* ;

**Hierarchy Level** [edit services application-identification]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for application identification in the services hierarchy added in 10.2.

**Description** Specify the timeout value in seconds for the application system cache entries. Note the cache is not cleared when IDP policy is loaded. Users need to manually clear or wait for the cache entries to expire.

**Options** *value* —Timeout value for the application system cache entries.

**Range:** 0 through 1,000,000 seconds

**Default:** 3600 seconds

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Application Identification for Security Devices

## ca-profile (Services)

**Syntax** ca-profile *ca-profile*;

**Hierarchy Level** [edit services unified-access-control infranet-controller *hostname*]

**Release Information** Statement introduced in Junos OS Release 9.4.

**Description** Specify the certificate authority (CA) of the certificate that the SRX Series device should use in communications with an Infranet Enforcer. The SRX Series device uses the CA to validate the IC Series UAC Appliance server certificate.

Use this statement if you have loaded certificates from multiple certificate authorities (CAs) onto your SRX Series device and you need to configure the device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series appliance .

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- server-certificate-subject on page 1176
- Unified Access Control Solution for Security Devices

Copyright © 2013, Juniper Networks, Inc. 

## captive-portal (Services UAC)

**Syntax**

```
captive-portal policy {
  redirect-traffic (all | unauthenticated);
  redirect-url url;
}
```

**Hierarchy Level** [edit services unified-access-control]

**Release Information** Statement introduced in Junos OS Release 10.2.

**Description** Specify the preconfigured security policy for captive portal on the Junos OS Enforcer to enable the captive portal feature. The captive portal policy is configured as part of the UAC policy.

By configuring the captive portal feature, you can redirect traffic destined for protected resources to the IC Series device or to the URL you configure on the Junos OS Enforcer.

**Options** The remaining statements are explained separately.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- captive-portal (Services UAC Policy) on page 1147
- redirect-traffic on page 1173
- redirect-url on page 1174
- Unified Access Control Solution for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## captive-portal (Services UAC Policy)

**Syntax** captive-portal *captive-portal-policy-name*;

**Hierarchy Level** [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then permit application-services uac-policy]

**Release Information** Statement introduced in Junos OS Release 10.2.

**Description** Create the captive portal policy in the UAC security policy. You use the captive portal policy to configure the captive portal feature on the Junos OS Enforcer. By configuring the captive portal feature, you can redirect traffic destined for protected resources to the IC Series device or to the URL you configure on the Junos OS Enforcer.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- captive-portal (Services UAC) on page 1146
- redirect-traffic on page 1173
- redirect-url on page 1174
- Security Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## certificate-verification

**Syntax** certificate-verification [ optional | required | warning ]

**Hierarchy Level** [edit services unified-access-control]

**Release Information** Statement introduced in Junos OS Release 12.1.

**Description** This option determines whether server certificate verification is required when initiating a connection between an SRX Series or J Series device and a Junos Pulse Access Control Service in a UAC configuration. If no CA profile contains the certificate authority (CA) that signed the configured server certificate for the Access Control Service, this option determines whether the commit check should fail, a warning should be displayed, or the connection should be made without any warning.

By default, an administrator is warned if the CA certificate is not configured in the **ca-profile**.



NOTE: For strict security, this option should be reset to required, and the proper CA certificate should be specified in the CA profile.

**Options**

- **optional**—Certificate verification is not required. If the CA certificate is not specified in the **ca-profile** option, the commit check passes and no warning is issued.
- **required**—Certificate verification is required. If the CA certificate is not specified in the **ca-profile** option, an error message is displayed, and the commit check fails. Use this option to ensure strict security.
- **warning**—(Default) Certificate verification is not required, however, a warning message is displayed during commit check if the CA certificate is not specified in the **ca-profile** option.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Understanding Communications Between the Junos OS Enforcer and the IC Series UAC Appliance
- Understanding User Role Firewalls
- Unified Access Control Solution for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## custom-ciphers

**Syntax** custom-ciphers [ rsa-with-rc4-128-md5 RSA | 128bit rc4 | md5 hash rsa-with-rc4-128-sha RSA | 128bit rc4 |sha hash rsa-with-des-cbc-sha RSA | des cbc | sha hash rsa-with-3des-ede-cbc-sha RSA | 3des ede/cbc | sha hash rsa-with-aes-128-cbc-sha RSA | 128 bit aes/cbc | sha hash rsa-with-aes-256-cbc-sha RSA | 256 bit aes/cbc |sha hash rsa-export-with-rc4-40-md5 RSA-export | 40 bit rc4 | md5 hash rsa-export-with-des40-cbc-sha RSA-export | 40 bit des/cbc | sha hash rsa-export1024-with-des-cbc-sha RSA 1024 bit export | des/cbc | sha hash rsa-export1024-with-rc4-56-md5 RSA 1024 bit export | 56 bit rc4 | md5 hash rsa-export1024-with-rc4-56-sha RSA 1024 bit export | 56 bit rc4 | sha hash rsa-with-null-md5 RSA | no symmetric cipher | md5 hash rsa-with-null-sha RSA | no symmetric cipher | sha hash];

**Hierarchy Level** [edit services ssl proxy profile *profile-name*]
[edit services ssl termination profile *profile-name*]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Display the custom cipher list.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## download (Services)

**Syntax**

```
download {
  automatic {
    interval hours;
    start-time MM-DD.hh:mm;
  }
url url;
```

**Hierarchy Level** [edit services application-identification]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure automatic download for the application identification services application package. The application package contains definitions for known applications, such as: DNS, Facebook, FTP, Skype, and SNMP. The application package is extracted from the IDP signature database located at https://services.netscreen.com/cgi-bin/index.cgi. If you do not have access to the default download site from your device, you can use the URL option to download from a different location.



NOTE: You need to download the application package before configuring application identification services.

**Options**

- automatic—Download the application package automatically at a certain time of day or at intervals.
- *interval*—Download the application package at intervals.

  **Range:** 6 through 720 hours

- *start-time*—Start time in which the application package will be download. Format is MM-DD.hh:mm. Example: 04-15.09:00 will start the download on April 15 at 9 AM.
- *url*—Use this option to change the default download location of the application package.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## dscp-rewrite

**Syntax**
```
dscp-rewrite {
  code-point 6 bit patterns;
}
```

**Hierarchy Level**
[edit security alg sip]
[edit security alg h323]
[edit security alg mgcp]
[edit security alg sccp]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Specify a rewrite-rule for the traffic that passes through a voice over IP Application Layer Gateway ( VoIP ALG).

**Options** **6-bit patterns**—Value of the code point in binary form.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Layer Gateways for Security Devices

## enable-flow-tracing (Services)

**Syntax**
```
enable-flow-tracing;
```

**Hierarchy Level**
[edit services ssl proxy profile *profile-name*]
[edit services ssl termination profile *profile-name*]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Enable flow tracing for the profile.

**Required Privilege Level**
services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## enable-heuristics (Services)

**Syntax** enable-heuristics;

**Hierarchy Level** [edit services application-identification]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** The **enable-heuristics** command is an optional command and is off by default. It enables encryption and P2P detection.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Identification for Security Devices

## enable-session-cache

**Syntax** enable-session-cache;

**Hierarchy Level** [edit services ssl termination profile *profile-name*]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Enable SSL session cache.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## file (Services)

**Syntax**

```
file file-name; {
  files;
  match;
  no-world-readable size;
  world-readable;
}
```

**Hierarchy Level** [edit services ssl traceoptions]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the trace file information.

**Options**

- **files**—Specify the maximum number of trace files. Range: 2 to 1000.
- **match**—Specify the regular expression for lines to be logged.
- **no-world-readable size**—Do not allow any user to read the log file.
- **size**—Specify the maximum trace file size. Range: 10,240 to 1,073,741,824.
- **world-readable**—Allow any user to read the log file.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*

## files (Services)

**Syntax** files *files*;

**Hierarchy Level** [edit services ssl traceoptions file *file-name*]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the maximum number of trace files.

**Options** **files**—Specify the maximum number of trace files.

**Range**: 2 to 1000

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## flag (Services)

**Syntax** flag (*all* | *cli-configuration* | *initiation* | *proxy* | *selected-profile* | *termination*);

**Hierarchy Level** [edit services ssl traceoptions]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the tracing flag parameters.

**Options**
- *all*—Trace all the parameters.
- *cli-configuration*—Trace CLI configuration events.
- *initiation*—Trace initiation service events.
- *proxy*—Trace proxy service events.
- *selected-profile*—Trace events for profiles with enable-flow-tracing set.
- *termination*—Trace termination service events.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## flow-monitoring (Services)

**Syntax** flow-monitoring

**Hierarchy Level** [edit services]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Configure flow monitoring.

**Options**
- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Donot inherit configuration data from these groups.
- **version9**—Version 9 configuration.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## flow-monitoring version 9

**Syntax** version9

**Hierarchy Level** [edit services flow-monitoring]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Version 9 configuration.

**Options**
- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Donot inherit configuration data from these groups.
- **template**—One or more version 9 templates.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## flow-monitoring version 9 template

**Syntax** template *name*

**Hierarchy Level** [edit services flow-monitoring version9]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** One or more version 9 templates.

**Options**
- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Donot inherit configuration data from these groups.
- **flow-active-timeout (10...600)**—Interval after which active flow is exported.
- **flow-inactive-timeout (10...600)**—Period of inactivity that marks a flow inactive.
- **ipv4-template**—IPv4 template configuration.
- **option-refresh-rate**—Option template refresh rate.
- **template-refresh-rate**—Template refresh rate.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## flow-server (Forwarding Options)

**Syntax** flow-server *address*

**Hierarchy Level** [edit forwarding-options sampling family inet output flow-server]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Configure sending traffic aggregates in cflowd format.

**Options**

- **aggregation (version 8 only)**—Aggregations to perform for exported flows.
- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Do not inherit configuration data from these groups.
- **autonomous-system-type**—Type of autonomous system number to export.
- **local-dump**—Dump cflowd records to log file before exporting.
- **no-local-dump**—Do not dump cflowd records to log file before exporting.
- **port**—UDP port number on host collecting cflowd packets.
- **source-address**—Source IPv4 address for cflowd packets.
- **version**—Format of exported cflowd aggregates.
- **version9**—Exported data in version 9 format.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## global-config (Services)

**Syntax**

```
global-config {
  session-cache-timeout session-cache-timeout;
}
```

**Hierarchy Level** [edit services ssl proxy]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10..

**Description** Specify the global proxy configuration.

**Options** *session-cache-timeout*—Specify the session cache timeout.

**Range**: 300 to 3600 seconds

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## flow-server version 9

**Syntax** version9

**Hierarchy Level** [edit forwarding-options sampling family inet output flow-server ]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Export data in version 9 format.

**Options**
- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Do not inherit configuration data from these groups.
- **template**—Template configuration.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## infranet-controller

**Syntax**

```
infranet-contoller hostname {
   address ip-address;
   port port-number;
   interface interface-name;
   password password;
   ca-profile ca-profile;
   server-certificate-subject subject;
}
```

**Hierarchy Level** [edit services unified-access-control ]

**Release Information** Statement introduced in Junos OS Release 9.4.

**Description** Specify the hostname of the IC Series device with which the SRX Series devices should communicate. Possible values for this statement range from 1 to 31 characters.

This statement is required when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series device.

**Options** The remaining statements are explained separately.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- address (Services) on page 1138
- Unified Access Control Solution for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## inline-jflow (Forwarding Options)

**Syntax** inline-jflow

**Hierarchy Level** [edit forwarding-options sampling family inet output ]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Inline processing of sampled packets.

**Options**
- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Do not inherit configuration data from these groups.
- **source-address**—Address to use for generating monitored packets.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## interface (Services)

**Syntax** interface *interface-name*;

**Hierarchy Level** [edit services unified-access-control infranet-controller *hostname*]

**Release Information** Statement introduced in Junos OS Release 9.4.

**Description** Specify the SRX Series interface through which the IC Series device should connect.

This statement is required when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series device.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- port (Services) on page 1169
- password (Services) on page 1168
- Unified Access Control Solution for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## interval (Services)

**Syntax** interval *seconds*;

**Hierarchy Level** [edit services unified-access-control ]

**Release Information** Statement introduced in Junos OS Release 9.4.

**Description** Specify the value in seconds that the SRX Series device should expect to receive a heartbeat signal from the IC Series device (default 30). This configuration statement is used in conjunction with the **timeout** statement to test active communications with the IC Series device. The value of the **interval** statement must be smaller than the value of **timeout** statement.

Use this statement when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series device.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- timeout (Services) on page 1185
- timeout-action on page 1186
- Unified Access Control Solution for Security Devices

## level (Services)

**Syntax** level [*brief* | *detail* | *extensive* | *verbose*];

**Hierarchy Level** [edit services ssl traceoptions]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the level of debugging the output.

**Options**

- *brief*—Specify brief debugging output.
- *detail*—Specify detailed debugging output.
- *extensive*—Specify extensive debugging output.
- *verbose*—Specify verbose debugging output.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## log (Services)

**Syntax**

```
log {
    all;
    errors;
    info;
    sessions-allowed;
    sessions-dropped;
    sessions-ignored;
    sessions-whitelisted;
    warning;
}
```

**Hierarchy Level** [edit services ssl proxy profile *profile-name* actions]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the logging actions.

**Options**

- **all**—Log all events.
- **errors**—Log all error events.
- **info**—Log all information events.
- **sessions-allowed**—Log SSL session allowed events after an error.
- **sessions-dropped**—Log only SSL session dropped events.
- **sessions-ignored**—Log session ignored events.
- **sessions-whitelisted**—Log SSL session whitelisted events.
- **warning**—Log all warning events.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## match (Services)

**Syntax** match *match*;

**Hierarchy Level** [edit services ssl traceoptions file *file-name*]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the regular expression for lines to be logged.

**Options** **match**—Specify the regular expression for lines to be logged.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## max-checked-bytes (Services)

**Syntax** max-checked-bytes *bytes*;

**Hierarchy Level** [edit services application-identification]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** The maximum number of bytes to be applied with the application signatures.

**Options** *bytes*—Maximum bytes.
**Range:** 0 through 100000 bytes
**Default:** 100000 bytes

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## max-sessions (Services)

**Syntax** max-sessions *value*;

**Hierarchy Level** [edit services application-identification]

**Release Information** Statement introduced in Release 9.2 of Junos OS. Support for application identification in the services hierarchy added in 10.2.

**Description** Specify the maximum number of sessions application identification maintains. If the value reaches the maximum, all new sessions are dropped.

**Options** *value*—Maximum number of sessions.

**Range:** 0 through 500000

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## nested-application (Services)

**Syntax**

```
nested-application name {
  protocol protocol-name;
  signature signature-name {
    chain-order;
    insert-before application-name;
    maximum-transactions value;
    member name {
      context [http-get-url-parsed-param-parsed | http-header-content-type |
        http-header-cookie | http-header-host | http-header-user-agent |
        http-post-url-parsed-param-parsed | http-post-variable-parsed | http-url-parsed |
        http-url-parsed-param-parsed | ssl-server-name];
      direction [any | client-to-server | server-to-client];
      pattern dfa-pattern;
    }
  }
  type name;
}
```

**Hierarchy Level** [edit services application-identification]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure a custom nested application definition for the desired application name that will be used by the system to identify the nested application as it passes through the device. Custom nested application definitions can be used for nested applications that are not part of the Juniper Networks predefined nested application database.

**Options**

- **protocol**—The protocol that will be monitored to identify nested applications. HTTP is supported.
- **signature** *name*—Name of the custom nested application signature definition. Must be a unique name with a maximum length of 32 characters. (Required)
- **chain-order**—Signatures can contain multiple members. If chain-order is on, those members are read in order. The default for this option is no chain order. If a signature only contains one member, this option is ignored.
- **insert-before** *application-name*—When there are multiple patterns matched for the same session, the lowest order number takes the highest priority. Must be unique.
- **maximum-transactions**—The maximum number of transactions that should occur before a match is made.
- **member** *name*—Defines a member name for a custom nested application signature definition. Custom definitions can contain multiple members that define attributes for an application.
- **context**—Define a service specific context, such as http-url.
- **direction**—The connection direction of the packets to apply pattern matching. The options are client-to-server, server-to-client, or any.


Copyright © 2013, Juniper Networks, Inc.

- **pattern** *dfa-pattern*—Define the DFA pattern to match in the context. See Understanding Custom Application Signature Patterns for valid signature language conventions.
- **type**—Well known application name for this application definition, such as Facebook and Kazza. Must be a unique name with a maximum length of 32 characters. (Optional; used by IDP.)

**Required Privilege Level**
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**
- Application Identification for Security Devices

## nested-application-settings (Services)

**Syntax**

```
nested-application-settings {
  no-application-system-cache;
  no-nested-application;
}
```

**Hierarchy Level**
[edit services application-identification]

**Release Information**
Statement introduced in Release 10.2 of Junos OS.

**Description**
Configure nested application options for application identification services.

**Options**
- **no-application-system-cache**—Nested application identification information is saved in the application system cache to improve performance. This cache is updated when a different application is identified. This caching is turned on by default. Use the no-application-system-cache statement to turn it off.
- **no-nested-application**—Sometimes there is a need to identify multiple different applications running on the same Layer 7 protocols. For example, both Facebook and Yahoo Messenger can run over HTTP, but there is a need to identify them as two different applications. To do this, the application layer is split into two layers: Layer 7 applications and Layer 7 protocols. This function is turned on by default. Use the no-nested-application statement to turn it off.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## nested-application-system-cache

**Syntax** nested-application-system-cache
no-nested-application-system-cache

**Hierarchy Level** [edit services application-identification no-nested-application-system-cache]

**Release Information** Statement introduced in Release 10.1 of Junos OS.

**Description** Nested application identification information is saved in the application system cache to improve performance. This cache is updated when a different application is identified. This caching is turned on by default. Use the **no-nested-application-system-cache** statement to turn it off.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- Application Identification for Security Devices

## no-application-identification (Services)

**Syntax** no-application-identification;

**Hierarchy Level** [edit services application-identification]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Disable the TCP/UDP application identification of applications running on nonstandard ports.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## no-application-system-cache (Services)

**Syntax** no-application-system-cache;

**Hierarchy Level** [edit services application-identification]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Application identification information is saved in the application system cache to improve performance. This cache is updated when a different application is identified. This caching is turned on by default. Use the **no-application-system-cache** statement to turn it off.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Application Identification for Security Devices

## no-remote-trace (Services)

**Syntax** no-remote-trace;

**Hierarchy Level** [edit services ssl traceoptions]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Disable remote tracing.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## option-refresh-rate (Services)

**Syntax** option-refresh-rate

**Hierarchy Level** [edit services flow-monitoring version9 template]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Option template refresh rate.

**Options**
- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Do not inherit configuration data from these groups.
- **packets**—In number of packets (1...480000).
- **seconds**—In number of seconds (10...600).

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## password (Services)

**Syntax** password *password*;

**Hierarchy Level** [edit services unified-access-control infranet-controller *hostname*]

**Release Information** Statement introduced in Junos OS Release 9.4.

**Description** Specify the password that the SRX Series device should send to the IC Series device to establish communications. The SRX Series device sends the password in its first message to the IC Series device.

This statement is required when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series device.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- ca-profile (Services) on page 1145
- server-certificate-subject on page 1176
- Unified Access Control Solution for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## port (Services)

**Syntax** port *port-number*;

**Hierarchy Level** [edit services unified-access-control infranet-controller *hostname*]

**Release Information** Statement introduced in Junos OS Release 9.4.

**Description** Specify the port on the IC Series device through which the SRX Series device should establish connections (default 11123). Possible values for this statement range from 1 through 65,535.

Use this statement when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series device.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- interface (Services) on page 1159
- password (Services) on page 1168
- Unified Access Control Solution for Security Devices

## preferred-ciphers

**Syntax** preferred-ciphers (custom | medium | strong | weak);

**Hierarchy Level** [edit services ssl proxy profile *profile-name* ]
[edit services ssl termination profile *profile-name* ]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Select the preferred ciphers.

**Options**

- **custom**—Configure custom cipher suite and order of preference.
- **medium**—Use ciphers with key strength of 128-bits or greater.
- **strong**—Use ciphers with key strength of 168-bits or greater.
- **weak**—Use ciphers with key strength of 40-bits or greater.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## profile (Services)

**Syntax**

```
profile profile-name {
  enable-flow-tracing;
  preferred-ciphers (custom | medium | strong | weak);;
  custom-ciphers [ rsa-with-rc4-128-md5 RSA | 128bit rc4 | md5 hash rsa-with-rc4-128-sha
    RSA | 128bit rc4 |sha hash rsa-with-des-cbc-sha RSA | des cbc | sha hash
    rsa-with-3des-ede-cbc-sha RSA | 3des ede/cbc | sha hash rsa-with-aes-128-cbc-sha
    RSA | 128 bit aes/cbc | sha hash rsa-with-aes-256-cbc-sha RSA | 256 bit aes/cbc |sha
    hash rsa-export-with-rc4-40-md5 RSA-export | 40 bit rc4 | md5 hash
    rsa-export-with-des40-cbc-sha RSA-export | 40 bit des/cbc | sha hash
    rsa-export1024-with-des-cbc-sha RSA 1024 bit export | des/cbc | sha hash
    rsa-export1024-with-rc4-56-md5 RSA 1024 bit export | 56 bit rc4 | md5 hash
    rsa-export1024-with-rc4-56-sha RSA 1024 bit export | 56 bit rc4 | sha hash
    rsa-with-null-md5 RSA | no symmetric cipher | md5 hash rsa-with-null-sha RSA | no
    symmetric cipher | sha hash];
  trusted-ca ( [ | ] | all);
  root-ca root-ca;
  whitelist whitelist-address;
  actions {
    ignore-server-auth-failure;
    log {
      all;
      sessions-dropped;
      sessions-allowed;
      sessions-ignored;
      sessions-whitelisted;
      errors;
      warning;
      info;
    }
    renegotiation (allow | allow-secure | drop);
    disable-session-resumption;
  }
}
```

**Hierarchy Level** [edit services ssl proxy]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the SSL server profile.

**Options** *profile-name*—Specify the profile identifier.

The remaining statements are explained separately.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## protocol-version

**Syntax** protocol-version (all | ssl3 | tls1);

**Hierarchy Level** [edit services ssl termination profile *profile-name*]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the accepted SSL protocol version.

**Options**
- **all**—Accept SSL version 3 or TLS version 1.
- **ssl3**—Accept SSL version 3.
- **tls1**—Accept TLS version 1.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## proxy (Services)

**Syntax**

```
proxy {
  global-config {
    session-cache-timeout session-cache-timeout;
  }
  profile profile-name {
    enable-flow-tracing;
    preferred-ciphers (custom | medium | strong | weak);
    custom-ciphers [ rsa-with-rc4-128-md5 RSA | 128bit rc4 | md5 hash rsa-with-rc4-128-sha
      RSA | 128bit rc4 |sha hash rsa-with-des-cbc-sha RSA | des cbc | sha hash
      rsa-with-3des-ede-cbc-sha RSA | 3des ede/cbc | sha hash rsa-with-aes-128-cbc-sha
      RSA | 128 bit aes/cbc | sha hash rsa-with-aes-256-cbc-sha RSA | 256 bit aes/cbc |sha
      hash rsa-export-with-rc4-40-md5 RSA-export | 40 bit rc4 | md5 hash
      rsa-export-with-des40-cbc-sha RSA-export | 40 bit des/cbc | sha hash
      rsa-export1024-with-des-cbc-sha RSA 1024 bit export | des/cbc | sha hash
      rsa-export1024-with-rc4-56-md5 RSA 1024 bit export | 56 bit rc4 | md5 hash
      rsa-export1024-with-rc4-56-sha RSA 1024 bit export | 56 bit rc4 | sha hash
      rsa-with-null-md5 RSA | no symmetric cipher | md5 hash rsa-with-null-sha RSA | no
      symmetric cipher | sha hash];
    trusted-ca ( [ | ] | all);
    root-ca root-ca;
    whitelist whitelist-address;
    actions {
      ignore-server-auth-failure;
      log {
        all;
        sessions-dropped;
        sessions-allowed;
        sessions-ignored;
        sessions-whitelisted;
        errors;
        warning;
        info;
      }
      renegotiation (allow | allow-secure | drop);
      disable-session-resumption;
    }
  }
}
```

**Hierarchy Level** [edit services ssl]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the configuration for Secure Socket Layer (SSL) proxy support service.

**Options** The remaining statements are explained separately.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.


Copyright © 2013, Juniper Networks, Inc.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## redirect-traffic

**Syntax** redirect-traffic (all | unauthenticated);

**Hierarchy Level** [edit services unified-access-control captive-portal *policy*]

**Release Information** Statement introduced in Junos OS Release 10.2.

**Description** Specify to redirect traffic destined for protected sources to the IC Series device. You can choose to redirect all traffic or only unauthenticated traffic.

**Options**
- **all**—Redirect all traffic destined for the protected sources to the IC Series device. Specify this option if you want to redirect all traffic (IPsec or source IP) to the currently connected IC Series device or to an IP address or domain name that you specify in a redirect URL
- **unauthenticated**—Redirect unauthenticated traffic destined for the protected sources to the IC Series device. Select this option if your deployment uses source IP only or a combination of source IP and IPsec. The Junos OS Enforcer redirects clear-text traffic from unauthenticated users to the currently connected IC Series device or to an IP address or domain name that you specify in a redirect URL.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- captive-portal (Services UAC) on page 1146
- captive-portal (Services UAC Policy) on page 1147
- redirect-url on page 1174
- Unified Access Control Solution for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## redirect-url

**Syntax** redirect-url *url*;

**Hierarchy Level** [edit services unified-access-control captive-portal *policy*]

**Release Information** Statement introduced in Junos OS Release 10.2.

**Description** Specify to redirect traffic destined for protected sources to a specified URL.

You can configure the following options in the redirect URL string:

- ***%dest-url%***—Specifies the protected resource which the user is trying to access.
- ***%enforcer-id%***—Specifies the ID assigned to the Junos OS Enforcer by the IC Series device.
- ***%policy-id%***—Specifies the encrypted policy ID for the security policy that redirected the traffic.
- ***%dest-ip%***—Specifies the IP address or hostname of the protected resource that the user is trying to access.
- ***%ic-ip%***—Specifies the IP address or hostname of the IC Series device to which the Junos OS Enforcer is currently connected to.

If you do not specify the redirect URL, the Junos OS Enforcer uses the following default configuration:

```
https://%ic-ip%/?target = %dest-url%  &enforcer = %enforcer-id%  &policy =
%policy-id%  &dest-ip = %dest-ip%
```



NOTE: The maximum size of a redirect payload is 1450 bytes. The size of the redirect URL is restricted to 1407 bytes (excluding a few HTTP headers). If a user accesses a destination URL that is larger than 1407 bytes, the Infranet Controller authenticates the payload, calculates the exact length of the redirect URL, and trims the destination URL so that it can fit into the redirect URL. The destination URL can be fewer than 1407 bytes based on what else is present in the redirect URL (for example, policy ID). The destination URL in the default redirect URL is trimmed so that the redirect packet payload size is limited to 1450 bytes. If the length of the payload is larger than 1450 bytes, the excess length is trimmed and the user is directed to the destination URL that has been resized to 1450 bytes.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- captive-portal (Services UAC) on page 1146
- captive-portal (Services UAC Policy) on page 1147


Copyright © 2013, Juniper Networks, Inc.

- redirect-traffic on page 1173
- Unified Access Control Solution for Security Devices

## renegotiation (Services)

**Syntax** renegotiation (allow | allow-secure | drop);

**Hierarchy Level** [edit services ssl proxy profile *profile-name* actions]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the renegotiation options.

**Options**
- **allow**—Allow secure and nonsecure renegotiation.
- **allow-secure**—Allow secure negotiation only.
- **drop**—Drop session on renegotiation request.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## root-ca (Services)

**Syntax** root-ca *root-ca-name*;

**Hierarchy Level** [edit services ssl proxy profile *profile-name*]
[edit services ssl termination profile *profile-name*]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Root certificate for interdicting server certificates in proxy mode.

**Options** *root-ca-name*—Specify root certificate for interdicting server certificates in proxy mode.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## server-certificate (Services)

**Syntax** server-certificate *server-certificate*;

**Hierarchy Level** [edit services ssl termination profile *profile-name* server-certificate]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the local certificate identifier.

**Options** **server-certificate**—Specify the name of the local certificate identifier.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## server-certificate-subject

**Syntax** server-certificate-subject *subject*;

**Hierarchy Level** [edit services unified-access-control infranet-controller *hostname*]

**Release Information** Statement introduced in Junos OS Release 9.4.

**Description** Optionally specify the full subject name of the certificate that the SRX Series device should use to validate the IC Series device's server certificate.

Use this statement when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series device.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- ca-profile (Services) on page 1145
- password (Services) on page 1168
- Unified Access Control Solution for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## signature (Services)

**Syntax**

```
signature {
  client-to-server {
    dfa-pattern pattern;
    regex reg-expression;
  }
  insert-before application-name;
  min-data bytes;
  port-range {
    tcp tcp-port-range;
    udp udp-port-range;
  }
  server-to-client {
    dfa-pattern pattern;
    regex reg-expression;
  }
}
```

**Hierarchy Level** [edit services application-identification application *application-name*]

**Release Information** Statement introduced in Release 10.2 of Junos OS. Statement modified in Release 11.4 of Junos OS.

**Description** Configure the signature attributes for a custom application definition.

**Options**

- **client-to-server**—Define the attributes for traffic in the client to server direction.
- **dfa-pattern**—Define the dfa pattern for the application traffic in the client-to-server direction. Maximum length is 1023.
- **regex**—Enter a regular expression that should be matched for client to server traffic.
- **insert-before**—When there are multiple patterns matched for the same session, the lowest order number takes the highest priority. Must be unique.
- **min-data**—The minimum number of bytes or packets to apply to the dfa-pattern. Default is 10, range is 4 through 1024 (bytes).
- **port-range** [*tcp* | *udp*]—Define the port range for the application. Default ranges: TCP/0 through 65,535, UDP/0 through 65,535. (Optional)
- **server-to-client**—Define the attributes for traffic in the server to client direction.
- **dfa-pattern**—Define the dfa pattern for the application traffic in the server to client direction. Maximum length is 1023. See Understanding Custom Application Signature Patterns for valid signature language conventions.
- **regex**—Enter a regular expression that should be matched for server to client traffic.

**Required Privilege Level** trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Copyright © 2013, Juniper Networks, Inc.

**Related Documentation**

- Application Identification for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ssl (Services)

**Syntax**

```
ssl {
  traceoptions {
    file file-name; {
    files;
    match;
    no-world-readable size;
    world-readable;
    }
    flag;
    level;
    no-remote-trace;
  }
  termination {
    profile profile-name {
      custom-ciphers [ rsa-with-rc4-128-md5 RSA | 128bit rc4 | md5 hash
        rsa-with-rc4-128-sha RSA | 128bit rc4 |sha hash rsa-with-des-cbc-sha RSA | des
        cbc | sha hash rsa-with-3des-ede-cbc-sha RSA | 3des ede/cbc | sha hash
        rsa-with-aes-128-cbc-sha RSA | 128 bit aes/cbc | sha hash
        rsa-with-aes-256-cbc-sha RSA | 256 bit aes/cbc |sha hash
        rsa-export-with-rc4-40-md5 RSA-export | 40 bit rc4 | md5 hash
        rsa-export-with-des40-cbc-sha RSA-export | 40 bit des/cbc | sha hash
        rsa-export1024-with-des-cbc-sha RSA 1024 bit export | des/cbc | sha hash
        rsa-export1024-with-rc4-56-md5 RSA 1024 bit export | 56 bit rc4 | md5 hash
        rsa-export1024-with-rc4-56-sha RSA 1024 bit export | 56 bit rc4 | sha hash
        rsa-with-null-md5 RSA | no symmetric cipher | md5 hash rsa-with-null-sha RSA
        | no symmetric cipher | sha hash];
      enable-flow-tracing;
      enable-session-cache;
      preferred-ciphers (custom | medium | strong | weak);
      protocol-version (all | ssl3 | tls1);
      server-certificate server-certificate;
    }
  }
}
proxy {
  global-config {
    session-cache-timeout session-cache-timeout;
  }
  profile profile-name {
    enable-flow-tracing;
    preferred-ciphers (custom | medium | strong | weak);
    custom-ciphers [ rsa-with-rc4-128-md5 RSA | 128bit rc4 | md5 hash rsa-with-rc4-128-sha
      RSA | 128bit rc4 |sha hash rsa-with-des-cbc-sha RSA | des cbc | sha hash
      rsa-with-3des-ede-cbc-sha RSA | 3des ede/cbc | sha hash rsa-with-aes-128-cbc-sha
      RSA | 128 bit aes/cbc | sha hash rsa-with-aes-256-cbc-sha RSA | 256 bit aes/cbc |sha
      hash rsa-export-with-rc4-40-md5 RSA-export | 40 bit rc4 | md5 hash
      rsa-export-with-des40-cbc-sha RSA-export | 40 bit des/cbc | sha hash
      rsa-export1024-with-des-cbc-sha RSA 1024 bit export | des/cbc | sha hash
      rsa-export1024-with-rc4-56-md5 RSA 1024 bit export | 56 bit rc4 | md5 hash
      rsa-export1024-with-rc4-56-sha RSA 1024 bit export | 56 bit rc4 | sha hash
      rsa-with-null-md5 RSA | no symmetric cipher | md5 hash rsa-with-null-sha RSA | no
      symmetric cipher | sha hash];
```

Copyright © 2013, Juniper Networks, Inc.

```
        trusted-ca ( [ | ] | all);
        root-ca root-ca;
        whitelist whitelist-address;
        actions {
            ignore-server-auth-failure;
            log {
                all;
                sessions-dropped;
                sessions-allowed;
                sessions-ignored;
                sessions-whitelisted;
                errors;
                warning;
                info;
            }
            renegotiation (allow | allow-secure | drop);
            disable-session-resumption;
        }
    }
}
```

**Hierarchy Level** [edit services]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the configuration for Secure Socket Layer (SSL) support service.

**Options** The remaining statements are explained separately.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## size (Services)

**Syntax** size *size*;

**Hierarchy Level** [edit services ssl traceoptions file *file-name*]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the maximum trace file size.

**Options** **size**—Specify the maximum trace file size.

**Range**: 10,240 to 1,073,741,824.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## statistics (Services)

**Syntax**
```
statistics {
  interval interval-number;
}
```

**Hierarchy Level** [edit services application-identification]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Specify the interval, in minutes, for statistics collection.

**Options** **interval** *interval-number*—Length of time, in minutes, that application statistics are collected.

**Range:** 1 through 1440 minutes

**Default:** 1 minute



NOTE: For SRX Series devices, the maximum number of interval periods for which statistics is stored is 8.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- Application Identification for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## template-refresh-rate (Services)

**Syntax** template-refresh-rate

**Hierarchy Level** [edit services flow-monitoring version9 template]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Template refresh rate.

**Options**

- **apply-groups**—Groups from which to inherit configuration data.
- **apply-groups-except**—Do not inherit configuration data from these groups.
- **packets**—In number of packets (1...480000).
- **seconds**—In number of seconds (10...600).

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## termination (Services)

**Syntax**

```
termination {
  profile profile-name {
    custom-ciphers [ rsa-with-rc4-128-md5 RSA | 128bit rc4 | md5 hash rsa-with-rc4-128-sha
      RSA | 128bit rc4 |sha hash rsa-with-des-cbc-sha RSA | des cbc | sha hash
      rsa-with-3des-ede-cbc-sha RSA | 3des ede/cbc | sha hash rsa-with-aes-128-cbc-sha
      RSA | 128 bit aes/cbc | sha hash rsa-with-aes-256-cbc-sha RSA | 256 bit aes/cbc |sha
      hash rsa-export-with-rc4-40-md5 RSA-export | 40 bit rc4 | md5 hash
      rsa-export-with-des40-cbc-sha RSA-export | 40 bit des/cbc | sha hash
      rsa-export1024-with-des-cbc-sha RSA 1024 bit export | des/cbc | sha hash
      rsa-export1024-with-rc4-56-md5 RSA 1024 bit export | 56 bit rc4 | md5 hash
      rsa-export1024-with-rc4-56-sha RSA 1024 bit export | 56 bit rc4 | sha hash
      rsa-with-null-md5 RSA | no symmetric cipher | md5 hash rsa-with-null-sha RSA | no
      symmetric cipher | sha hash];
    enable-flow-tracing;
    enable-session-cache;
    preferred-ciphers (custom | medium | strong | weak);
    protocol-version (all | ssl3 | tls1);
    server-certificate server-certificate;
  }
}
```

**Hierarchy Level** [edit services ssl]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the configuration for Secure Socket Layer (SSL) termination support service.

**Options** The remaining statements are explained separately.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## test-only-mode

**Syntax** test-only-mode (true | false):

**Hierarchy Level** [edit services unified-access-control ]

**Release Information** Statement introduced in Junos OS Release 9.4.

**Description** Configure the device in test-only mode to log access decisions from the IC Series device without actually enforcing the decisions. When configured in test-only mode, the SRX Series device enables all UAC traffic to go through so you can test the implementation without impeding traffic.

Use this statement when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series device.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- Unified Access Control Solution for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## timeout (Services)

**Syntax** timeout *seconds*;

**Hierarchy Level** [edit services unified-access-control ]

**Release Information** Statement introduced in Junos OS Release 9.4.

**Description** Specify the value, in seconds, that the SRX Series device should wait to get a heartbeat response from an IC Series UAC Appliance (default is 60). If the SRX Series device does not receive a response in the specified time, it takes the action specified by the **timeout-action** configuration statement. It also tries again to make a connection to the IC Series appliance. After the second failed attempt, the SRX Series device fails over to the next IC Series appliance in the cluster. The SRX Series device continues trying to reach IC Series appliances in the cluster until a connection is established.

Use this statement when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series appliance. When working with a cluster of IC Series appliances, the Junos OS Enforcer connects to one at a time, failing over to other IC Series appliances in the cluster as required.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- interval (Services) on page 1160
- timeout-action on page 1186
- Unified Access Control Solution for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## timeout-action

**Syntax** timeout-action (close | no-change | open):

**Hierarchy Level** [edit services unified-access-control ]

**Release Information** Statement introduced in Junos OS Release 9.4.

**Description** Specify what the SRX Series device should do when a timeout occurs and the device cannot connect to an Infranet Enforcer.

Use this statement when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series UAC Appliance.

**Options**

- **close**—Close existing sessions and block any further traffic. This is the default option.
- **no-change**—Preserve existing sessions and require authentication for new sessions.
- **open**—Preserve existing sessions and allow new sessions access.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- interval (Services) on page 1160
- timeout (Services) on page 1185
- Unified Access Control Solution for Security Devices

 Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Services)

**Syntax**

```
traceoptions {
  file file-name; {
  files;
  match;
  no-world-readable size;
  world-readable;
  }
  flag {
  all;
    cli-configuration;
    initiation;
    proxy;
    selected-profile;;
  termination
  }
  level;
  no-remote-trace;
}
```

**Hierarchy Level** [edit services ssl]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the trace file information.

**Options**

- *file-name*—Specify the name of file in which to write trace information.
- **files**—Specify the maximum number of trace files. Range: 2 to 1000.
- **match**—Specify the regular expression for lines to be logged.
- **no-world-readable size**—Do not allow any user to read the log file.
- **size**—Specify the maximum trace file size. Range: 10,240 to 1,073,741,824.
- **world-readable**—Allow any user to read the log file.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Services Application Identification)

**Syntax**

```
traceoptions {
  file filename <files number> <match regular-expression>
  <size maximum-file-size> <world-readable | no-world-readable>
  flag all;
  no-remote-trace;
}
```

**Hierarchy Level** [edit services application-identification]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure tracing operations for application identification services.

**Options**

- **file** *filename*—By default, the name of the log file that records trace output is the name of the process being traced. Use this option to specify another name.
- **files** *number*—(Optional) Specify the maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed to *trace-file*.0, then *trace-file*.1, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

  If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

  **Range:** 2 through 1000 files

  **Default:** 10 files

- **match** *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.
- **size** *maximum-file-size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file.0*. When the **trace-file** again reaches its maximum size, *trace-file.0* is renamed *trace-file.1*. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

  If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

  **Syntax:** *x* **k** to specify KB, *x* **m** to specify MB, or *x* **g** to specify GB

  **Range:** 10 KB through 1 GB

  **Default:** 128 KB

- **world-readable | no-world-readable**—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag all**—Perform all tracing options for application identification services.


Copyright © 2013, Juniper Networks, Inc.

**Required Privilege Level**
trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**
- Application Identification for Security Devices

## traceoptions (Services UAC)

**Syntax**
```
traceoptions {
  flag [ (ipc | config | connect | all) ];
}
```

**Hierarchy Level**
[edit services unified-access-control ]

**Release Information**
Statement introduced in Junos OS Release 9.4.

**Description**
Define Unified Access Control (UAC) tracing options.

Use this statement when you are configuring the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series UAC Appliance.

**Options**
**flag**—Trace operation to perform. To specify more than one trace option, include multiple flag statements.

- **all**—Trace with all flags enabled
- **config**—Trace configuration information for all UAC-related configurations. This includes all configuration controlled through the **unified-access-control** statements at the **edit services** hierarchy level. It also includes other standard Junos OS configurations required for UAC enforcement such as zones, policies, and interfaces.
- **connect**—Trace communications between the Junos OS Enforcer and the IC Series appliance, including SSL handshakes and timeouts.
- **ipc**—Trace inter-process communications. Use this option to trace communications between the Routing Engine (RE) and the UACD enforcement plugin inside the Packet Forwarding Engine (PFE).

**Required Privilege Level**
services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- Unified Access Control Solution for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## trusted-ca (Services)

**Syntax** trusted-ca *trusted-ca-name* ([ | ] | all);

**Hierarchy Level** [edit services ssl proxy profile *profile-name*]
[edit services ssl termination profile *profile-name*]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the list of trusted certificate authority profiles.

**Options**
- *trusted-ca-name*—Specify the certificate authority profile name.
- **[**—Open a set of values.
- **]**—Close a set of values.
- **all**—Select all certificate authority profiles.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## unified-access-control

**Syntax**

```
unified-access-control {
  certificate-verification (optional | required | warning)
  infranet-contoller hostname {
    address ip-address;
    port port-number;
    interface interface-name;
    password password;
    ca-profile ca-profile;
    server-certificate-subject subject;
  }
  test-only-mode (true | false);
  timeout seconds;
  interval seconds;
  timeout-action (close | no-change | open);
  traceoptions {
    flag [ (ipc | config | connect | all) ];
  }
```

**Hierarchy Level** [edit services]

**Release Information** Statement introduced in Junos OS Release 9.4.

**Description** Use this statement to configure the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series device.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**

- Unified Access Control Solution for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## whitelist (Services)

**Syntax** whitelist *whitelist-address* ([ | ]);

**Hierarchy Level** [edit services ssl proxy profile *profile-name*]
[edit services ssl termination profile *profile-name*]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the addresses exempted from the SSL proxy.

**Options**
- *whitelist-address*—Specify address from the global address book.
- **[**—Open a set of values.
- **]**—Close a set of values.

**Required Privilege Level** services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## wireless-wan

**Syntax**

```
wireless-wan {
  adapter <adapter-name> {
    ip-address <IP address>;
    adapter-type cx-bridge;
    modem {
      usb1 description <description>;
      usb2 description <description>;
      usb3 description <description>;
      expresscard description <description>;
    }
  }
}
```

**Hierarchy Level** [edit services wireless-wan]

**Release Information** Statement introduced in Release 11.4R2 of Junos OS.

**Description** Assign a name to an adapter to differentiate between multiple adapters connected to an SRX Series device. You must configure an adapter IP address for each adapter name. The IP address of an adapter is used for all communications between the adapter and the SRX Series device. A maximum of 4 adapters can be connected to an SRX Series device. The management functions for the CX111 adapter now include CLI commands. You can now monitor and manage this adapter using these CLI commands.

**Options**

- **adapter name**—Name of the CX111 adapter.
- **ip-address**—Management IP address used for all communications between the adapter and an SRX Series device.
- **adapter-type**—(optional) Type of adapter; “cx-bridge” is the only type of adapter supported.
- **modem**—Type of modem. Text descriptions are defined for each modem port.



NOTE: **The CLI management of the CX111 3G adapter is not supported with Virtual routing instance.**

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 21

# SMTP Hierarchy and Statements

Use the statements in the **smtp** configuration hierarchy to configure Simple Mail Transfer Protocol (SMTP) to send an e-mail message to a local or a remote mail server to forward an e-mail message.

This chapter contains the following sections:


- SMTP Configuration Statement Hierarchy on page 1195


## SMTP Configuration Statement Hierarchy

```
smtp {
    primary-server {
    address IPv4 address;
    login sender-email {
    password password;
    }
}
secondary-server {
    address IPv4 address;
    login sender-email;
    password password ;
    }
}
traceoptions {
    flag flag ;
    }
}
```

**Related Documentation**

- UTM for Security Devices
- SMTP

Copyright © 2013, Juniper Networks, Inc.

## flag (SMTP)

**Syntax**

```
traceoptions {
flag  flag;
}
```

**Hierarchy Level** [edit **smtp traceoptions flag**]

**Release Information** Statement added in Release 10.0 of Junos OS.

**Description** Set flag for the SMTP traceoptions.

**Options** The following flag options are supported:

- **IPC**—Trace inter-processs communication.
- **all**—Trace everything.
- **configuration**—Trace configuration event.
- **protocol-exchange**—Trace SMTP protocol exchanges.
- **send-request**—Trace send mail request event.

**Required Privilege Level** SMTP—To view this statement in the configuration.

**Related Documentation**

- Unified Threat Management
- UTM for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## primary-server

**Syntax**

```
primary-server {
address IPv4 address;
login sender-email {
password password;  }
}
```

**Hierarchy Level** [edit **smtp primary-server address** ]

**Release Information** Statement added in Release 10.0 of Junos OS.

**Description** Set access authorization for SMTP requests.

**Options** **address**—SMTP server's IPv4 address.

**login**—Configure a mail sender account to the server.

**Required Privilege Level** SMTP—To view this statement in the configuration.

**Related Documentation**

- SMTP
- UTM for Security Devices

## secondary-server

**Syntax**

```
secondary-server {
address IPv4 address;
login sender-email {
password password;
}
```

**Hierarchy Level** [edit **smtp secondary-server address** ]

**Release Information** Statement added in Release 10.0 of Junos OS.

**Description** Set the access authorization for SMTP requests.

**Options** **address**—SMTP server's IPv4 address.

**login**—Configure a mail sender account to the server.

**Required Privilege Level** SMTP—To view this statement in the configuration.

**Related Documentation**

- UTM for Security Devices
- SMTP

Copyright © 2013, Juniper Networks, Inc.

## traceoptions (SMTP)

**Syntax**

```
traceoptions {
flag flag;
}
```

**Hierarchy Level** [edit **smtp traceoptions** ]

**Release Information** Statement added in Release 10.0 of Junos OS.

**Description** Set the SMTP traceoptions.

**Options**

**apply-groups**—Groups from which SMTP inherits configuration data.

**apply-groups-except**— Groups from which SMTP restricts inheriting configuration data from these groups.

**Required Privilege Level** SMTP—To view this statement in the configuration.

**Related Documentation**

- UTM for Security Devices
- SMTP


Copyright © 2013, Juniper Networks, Inc.

CHAPTER 22

# SNMP Hierarchy and Statements

This section contains the following topics:


- SNMP Configuration Statement Hierarchy on page 1199


## SNMP Configuration Statement Hierarchy

Use the statements in the **snmp** configuration hierarchy to configure the Simple Network Management Protocol (SNMP) for monitoring device operation and performance.

```
snmp {
  client-list list-name;
  community community-name {
    authorization (read-only | read-write);
    client-list-name client-list-name;
    clients {
      address < restrict>;
    }
    routing-instances routing-instances {
      client-list-name client-list-name ;
      clients {
        address < restrict>;
      }
    }
    view view-name ;
  }
  contact contact-information ;
  description description ;
  engine-id {
    (local engine-id | use-default-ip-address | use-mac-address);
  }
  filter-duplicates;
  health-monitor {
    falling-threshold percentage ;
    interval seconds;
    rising-threshold percentage ;
  }
  interface [ interface-names ];
  location location ;
  logical-system-trap-filter;
  name system-name ;
  nonvolatile {
```

Copyright © 2013, Juniper Networks, Inc.

```
    commit-delay seconds ;
}
rmon {
    alarm index {
        description description ;
        falling-event-index index ;
        falling-threshold integer ;
        falling-threshold-interval seconds ;
        interval seconds ;
        request-type (get-next-request | get-request | walk-request);
        rising-event-index index ;
        rising-threshold integer ;
        sample-type (absolute-value | delta-value);
        startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm);
        syslog-subtag text-string ;
        variable oid-variable ;
    }
    event index {
        community community-name ;
        description description ;
        type (log | log-and-trap | none | snmptrap);
    }
}
routing-instance access {
    access-list {
        routing-instance-name ;
    }
}
traceoptions {
    file filename <files number > <match regular-expression >
    <size maximum-file-size > <world-readable | no-world-readable>;
    flag flag ;
}
trap-group group-name {
    categories {
        authentication;
        chassis;
        chassis-cluster;
        configuration;
        link;
        remote-operations;
        rmon-alarm;
        routing;
        services;
        sonet-alarms {
            alarm-name ;
        }
        startup;
        vrrp-events;
    }
    destination-port port-number ;
    routing-instance instance-name ;
    targets {
    address ;
    }
    version (all | v1 | v2);
```


Copyright © 2013, Juniper Networks, Inc.

```
}
trap-options {
  agent-address outgoing-interface;
  routing-instances instance-name {
    source-address address ;
  }
  source-address address ;
}
v3 {
  notify notify-name {
    tag tag-name ;
    type (inform | trap);
  }
  notify-filter notify-filter-name {
    oid oid-name <exclude | include>;
  }
  snmp-community community-index {
    community-name community-name ;
    context context ;
    security-name security-name ;
    tag tag-name ;
  }
  target-address target-address-name {
    address address ;
    address-mask address-mask ;
    port port-number ;
    retry-count number ;
    routing-instance instance-name ;
    tag-list tag-list ;
    target-parameters parameter-name ;
    timeout seconds ;
  }
  target-parameters target-parameters-name {
    notify-filter notify-filter-name ;{
      parameters {
        message-processing-model (v1 | v2c | v3);
        security-level (authentication | none | privacy);
        security-model (usm | v1 | v2c);
        security-name security-name ;
      }
    }
    usm {
      local-engine {
        user user-name {
          authentication-md5 {
            authentication-password password ;
          }
          authentication-none;
          authentication-sha {
            authentication-password password ;
          }
          privacy-3des {
            privacy-password password ;
          }
          privacy-aes128 {
            privacy-password password ;
```

```
        }
        privacy-des {
          privacy-password password ;
        }
        privacy-none;
      }
    }
    remote-engine {
      user user-name {
        authentication-md5 {
          authentication-password password ;
        }
        authentication-none;
        authentication-sha {
          authentication-password password ;
        }
        privacy-3des {
          privacy-password password ;
        }
        privacy-aes128 {
          privacy-password password ;
        }
        privacy-des {
          privacy-password password ;
        }
        privacy-none;
      }
    }
  }
  vacm {
    access {
      group group-name {
        context-prefix prefix {
          security-model (any | usm | v1 | v2c) {
            security-level (authentication | none | privacy) {
              context-match (exact | prefix);
              notify-view notify-view-name ;
              read-view read-view-name ;
              write-view write-view-name ;
            }
          }
        }
        default-context-prefix {
          security-model (any | usm | v1 | v2c) {
            security-level (authentication | none | privacy) {
              context-match (exact | prefix);
              notify-view notify-view-name ;
              read-view read-view-name ;
              write-view write-view-name ;
            }
          }
        }
      }
    }
    security-to-group {
      security-model (usm | v1 | v2c) {
```


Copyright © 2013, Juniper Networks, Inc.

```
            security-name security-name {
              group group-name ;
            }
          }
        }
      }
    }
    view view-name {
      oid oid-name {
        <exclude | include>;
      }
    }
  }
}
```

**Related Documentation**

- *Junos OS Monitoring and Troubleshooting Guide for Security Devices*
- *Junos OS Initial Configuration Guide for Security Devices*
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Network Management Configuration Guide

## authorization (SNMP)

**Syntax** **authorization (read-only | read-write);**

**Hierarchy Level** [edit **snmp community** *community-name* ]

**Release Information** Statement modified in Release 8.5 of Junos OS.

**Description** Set the access authorization for SNMP Get, GetBulk, GetNext, and Set requests.

**Options**

- **read-write**—Enable all requests, including Set requests. You must configure a view to enable Set requests.
- **read-only**—Enable Get, GetNext, and GetBulk requests. This is the default option.

**Required Privilege Level** snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Monitoring and Troubleshooting Guide for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

## client-list-name (SNMP)

**Syntax** client-list-name *client-list-name* ;

**Hierarchy Level** [edit snmp community *community-name* ]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Specify the name of the list of SNMP network management system (NSM) clients that are authorized to collect information about network operations. You cannot use an SNMP client list and individually configured SNMP clients in the same configuration.

**Options** ***client-list-name*** — Name of the client list. Client list is the list of IP address prefixes defined with the **prefix-list** statement in the policy-options hierarchy.

**Required Privilege Level** snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

CHAPTER 23

# System Hierarchy and Statements

This section includes the following topics:


- System Configuration Statement Hierarchy on page 1205


## System Configuration Statement Hierarchy

Use the statements in the **system** configuration hierarchy to configure system management functions including addresses of the Domain Name System (DNS) servers; device's hostname, address, and domain name; health monitoring; interface filtering; properties of the device's auxiliary and console ports; security profiles for logical systems; time zones and Network Time Protocol (NTP) properties; trace options; and user login accounts, including user authentication and the root-level user account. Statement descriptions that are exclusive to the J Series and SRX Series devices running Junos OS are described in this section.

```
system {
    accounting {
        destination {
            radius {
                server {
                    server-address {
                        accounting-port port-number;
                        retry number;
                        secret password;
                        source-address address;
                        timeout seconds;
                    }
                }
            }
            tacplus {
                server server-address {
                    port port-number;
                    secret password;
                    single-connection;
                    timeout seconds;
                }
            }
        }
        events [login change-log interactive-commands];
        traceoptions {
```

Copyright © 2013, Juniper Networks, Inc.

```
      file filename <files number > <size maximum-file-size>
      <world-readable | no-world-readable>;
      flag flag;
    }
}
archival {
    configuration {
        archive-sites {
            ftp://<username>:<password>@<host>:<port>/<url-path>;
            scp: // < username >:< password >@< host >:< port >/< url-path >;
        }
        transfer-interval interval;
        transfer-on-commit;
    }
}
arp {
    aging-timer minutes;
    passive-learning;
}
authentication-order [ authentication-methods ];
autoinstallation {
    configuration-servers url {
        password password;
    }
    interfaces interface-name {
        bootp;
        rarp;
        slarp;
    }
}
backup-router address <destination destination-address>;
building name;
commit synchronize;
(compress-configuration-files | no-compression-configuration-files);
default-address-selection;
diag-port-authentication (encrypted-password "password" | plain-text-password);
domain-name domain-name;
domain-search [domain-list];
dump-device {
    boot-device;
    compact-flash;
    removable-compact-flash;
    usb;
}
encrypt-configuration-files;
host-name hostname;
inet6-backup-router address <destination destination-address>;
internet-options address <destination destination-address>;
internet-options {
    (gre-path-mtu-discovery | no-gre-path-mtu-discovery);
    icmpv4-rate-limit {
        bucket-size seconds;
        packet-rate packet-rate;
    }
    icmpv6-rate-limit {
        bucket-size seconds;
```


Copyright © 2013, Juniper Networks, Inc.

```
      packet-rate packet-rate;
    }
    (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
    no-tcp-rfc1323;
    no-tcp-rfc1323-paws;
    (path-mtu-discovery | no-path-mtu-discovery);
    source-quench;
    source-port upper-limit <upper-limit>;
    (source-quench | no-source-quench);
    tcp-drop-synfin-set;
  }
  location {
    altitude feet;
    building name;
    country-code code;
    floor number;
    hcoord horizontal-coordinate;
    lata service-area;
    latitude degrees;
    longitude degrees;
    npa-nxx number;
    postal-code postal-code;
    rack  number ;
    vcoord vertical-coordinate;
  }
  login {
    announcement text;
    class class-name {
      allow-commands "regular-expression";
      allow-configuration "regular-expression";
      deny-commands "regular-expression";
      deny-configuration "regular-expression";
      idle-timeout minutes;
      login-alarms;
      login-tip;
      permissions [ permissions ];
    }
    message text;
    password {
      change-type (set-transitions | character-set);
      format (md5 | sha1 | des);
      maximum-length length;
      minimum-changes number;
      minimum-length length;
    }
    user username  {
      authentication {
        (encrypted-password"password""" | plain-text-password);
        ssh-dsa "public-key";
        ssh-rsa "public-key";
      }
      class class-name;
      full-name complete-name;
      uid uid-value;
    }
    retry-options {
```

```
        backoff-threshold number;
        backoff-factor seconds;
        minimum-time seconds;
        tries-before-disconnect number;
    }
}
max-configurations-on-flash number;
mirror-flash-on-disk;
name-server ip-address;
no-compress-configuration-files;
no-multicast-echo;
no-redirects;
no-saved-core-context;
ntp {
    authentication-key key-number type type value password;
    boot-server (NTP) address;
    broadcast <address> <key key-number > <version value> <ttl value >;
    broadcast-client;
    multicast-client <address>;
    peer address <key key-number > <version value> <prefer>;
    server address <key key-number > <version value> <prefer>;
    source-address source-address;
    trusted-key [ key-numbers ];
}
pic-console-authentication {
    encrypted-password encrypted-password;
    plain-text-password;
}
ports {
    auxiliary {
        disable;
        insecure;
        type terminal-type;
    }
    console {
        disable;
        insecure;
        log-out-on-disconnect;
        type terminal-type;
    }
}
processes {
    audit-process;
    bootp;
    chassis-control (enable | disable) failover failover-option;
    class-of-service (enable | disable) failover failover-option;
    craft-control (enable | disable) failover failover-option;
    dfc-daemon;
    dhcp (enable | disable) failover failover-option;
    dialer-services;
    disk-monitoring (enable | disable) failover failover-option;
    ecc-error-logging (enable | disable) failover failover-option;
    event-processing (enable | disable) failover failover-option;
    firewall (enable | disable) failover failover-option;
    firewall-authentication-service (enable | disable);
    forwarding;
```


Copyright © 2013, Juniper Networks, Inc.

```
general-authentication-service {
  (enable | disable);
  traceoptions {
    file filename {
      files number;
      match regular-expression;
      size maximum-file-size;
      <world-readable | no-world-readable>;
    }
    flag flag;
  }
}
ilmi;
inet-process (enable | disable) failover failover-option;
init;
interface-control (enable | disable) failover failover-option;
isdn-signaling;
kernel-replication (enable | disable) failover failover-option;
l2ald-service;
l2tp-service (enable | disable) failover failover-option;
lacp;
link-management (enable | disable) failover failover-option;
logical-system-mux;
mib-process (enable | disable) failover failover-option;
named;
network-security (enable | disable);
ntp (enable | disable) failover failover-option;
periodic-packet-services;
pfe;
pgm (enable | disable) failover failover-option;
pic-services-logging (enable | disable) failover failover-option;
ppp;
pppoe (enable | disable) failover failover-option;
redundancy-device (enable | disable) failover failover-option;
remote-operations (enable | disable) failover failover-option;
routing (enable | disable) failover failover-option;
sampling (enable | disable) failover failover-option;
service-deployment (enable | disable) failover failover-option;
snmp (enable | disable)  failover failover-option;
sonet-aps;
usb-control (enable | disable) failover failover-option;
vrrp;
watchdog (enable | disable) failover failover-option;
wan-acceleration {
  (enable | disable);
  traceoptions {
    file filename {
      files number;
      match regular-expression;
      size maximum-file-size;
      <world-readable | no-world-readable>;
    }
    flag flag;
  }
}
web-management (enable | disable) failover failover-option;
```

Copyright © 2013, Juniper Networks, Inc.

```
}
radius-options {
   attributes {
      nas-ip-address nas-ip-address ;
   }
}
radius-server server-address {
   accounting-port number;
   port number;
   retry number;
   secret password;
   source-address source-address;
   timeout seconds;
}
root-authentication {
   (encrypted-password "password" | plain-text-password);
   ssh-dsa "public-key";
   ssh-rsa "public-key";
}
(saved-core-context | no-saved-core-context);
saved-core-files number;
scripts {
   commit {
      allow-transients;
      file filename.xsl {
         optional;
         refresh;
         refresh-from url;
         source url;
      }
      refresh;
      refresh-from url;
      traceoptions {
         file filename <files number > <size maximum-file-size >
         <world-readable | no-world-readable>;
         flag flag ;
      }
   }
   load-scripts-from-flash;
   op {
      file filename.xsl {
         arguments name {
            description cli-help-text;
         }
         command filename-alias ;
         description cli-help-text;
         refresh;
         refresh-from url;
         source url;
      }
      refresh;
      refresh-from url;
      traceoptions {
         file filename <files number> <size maximum-file-size>;
         flag flag;
      }
```


Copyright © 2013, Juniper Networks, Inc.

```
    }
}
security-profile security-profile-name {
    address-book {
        maximum amount;
        reserved amount;
    }
    appfw-rule-set {
        maximum amount;
        reserved amount;
    }
    appfw-rule {
        maximum amount;
        reserved amount;
    }
    auth-entry {
        maximum amount;
        reserved amount;
    }
    cpu {
        reserved percent;
    }
    dslite-softwire-initiator {
        maximum amount;
        reserved amount;
    }
    flow-gate {
        maximum amount;
        reserved amount;
    }
    flow-session {
        maximum amount;
        reserved amount;
    }
    idp-policy idp-policy-name;
    logical-system logical-system-name;
    nat-cone-binding {
        maximum amount;
        reserved amount;
    }
    nat-destination-pool {
        maximum amount;
        reserved amount;
    }
    nat-destination-rule {
        maximum amount;
        reserved amount;
    }
    nat-nopat-address {
        maximum amount;
        reserved amount;
    }
    nat-pat-address {
        maximum amount;
        reserved amount;
    }
```

Copyright © 2013, Juniper Networks, Inc.

```
        nat-pat-portnum {
            maximum amount
            reserved amount
        }
        nat-port-ol-ipnumber {
            maximum amount;
            reserved amount;
        }
        nat-source-pool {
            maximum amount;
            reserved amount;
        }
        nat-source-rule {
            maximum amount;
            reserved amount;
        }
        nat-static-rule {
            maximum amount;
            reserved amount;
        }
        policy {
            maximum amount;
            reserved amount;
        }
        policy-with-count {
            maximum amount;
            reserved amount;
        }
        root-logical-system;
        scheduler {
            maximum amount;
            reserved amount;
        }
        zone {
            maximum amount;
            reserved amount;
        }
    security-profile resources {
      cpu-control;
      cpu-control-target percent;
    }
    services {
      dhcp {
        boot-file filename;
        boot-server (address | hostname);
        domain-name domain-name;
        domain-search [domain-list];
        default-lease-time seconds;
        maximum-lease-time seconds;
        name-server {
          address;
        }
        option {
          [ (id-number option-type option-value) | (id-number array option-type
          option-values) ];
        }
```


Copyright © 2013, Juniper Networks, Inc.

```
    pool {
      subnet-address  ( address/netmask) {
        address-range {
          high address;
          low address;
        }
        exclude-address {
          address;
        }
      }
      propagate-settings propagate-settings;
    }
    propagate-settings propagate-settings;
    router {
      address;
    }
    static-binding MAC-address {
      fixed-address {
        address;
      }
      host hostname;
      client-identifier (ascii client-id | hexadecimal client-id);
    }
    server-identifier address;
    wins-server {
      address;
    }
  }
  dhcp-local-server {
    dhcpv6 {
      authentication {
        password password-string;
        username-include {
          circuit-type;
          client-id;
          delimiter delimiter-character;
          domain-name domain-name-string;
          relay-agent-interface-id;
          relay-agent-remote-id;
          relay-agent-subscriber-id;
          routing-instance-name;
          user-prefix user-prefix-string;
        }
      }
      dynamic-profile {
        junos-default-profile;
        use-primary dynamic-profile-name-string;
      }
      group group-name {
        authentication {
          password password-string;
          username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name-string;
```

Copyright © 2013, Juniper Networks, Inc.

```
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
          }
        }
        dynamic-profile {
          junos-default-profile;
          use-primary dynamic-profile-name-string;
        }
        interface interface-name {
          exclude;
          overrides {
            interface-client-limit number;
          }
          trace;
          upto upto-interface-name;
        }
        overrides {
          interface-client-limit number;
        }
        reconfigure {
          attempts number;
          clear-on-abort;
          strict;
          timeout number;
          token token-name;
          trigger {
            radius-disconnect;
          }
        }
      }
      overrides {
        interface-client-limit number;
      }
      reconfigure {
        attempts number;
        clear-on-abort;
        strict;
        timeout number;
        token token-name;
        trigger {
          radius-disconnect;
        }
      }
    }
    duplicate-clients-on-interface;
    forward-snooped-clients {
      all-interfaces;
      configured-interfaces;
      non-configured-interfaces;
    }
    interface-traceoptions {
      file filename {
        files number;
```


Copyright © 2013, Juniper Networks, Inc.

```
            match regular-expression;
            size maximum-file-size;
            <world-readable | no-world-readable>;
        }
        flag {
            all;
            dhcpv6-packet;
            dhcpv6-packet-option;
            dhcpv6-state;
            packet;
            packet-option;
            state;
        }
        no-remote-trace;
    traceoptions {
        file filename {
            files number;
            match regular-expression;
            size maximum-file-size;
            <world-readable | no-world-readable>;
        }
        flag {
            all;
            auth;
            database;
            dhcpv6-general;
            dhcpv6-io;
            dhcpv6-packet;
            dhcpv6-packet-option;
            dhcpv6-rpd;
            dhcpv6-session-db;
            dhcpv6-state;
            fwd;
            general;
            ha;
            interface;
            io;
            packet;
            packet-option;
            performance;
            profile;
            rpd;
            rtsock;
            session-db
            state;
            statistics;
            ui;
        }
        no-remote-trace;
}
dns {
    dnssec {
        disable;
        dlv {
            domain-name domain-name {
                trusted-anchor trusted-anchor;
```

```
        }
      }
      secure-domains [domain-name];
      trusted-keys {
        key key;
        load-key-file {
          dns-keys;
        }
      }
    }
    max-cache-ttl;
    max-ncache-ttl;
    traceoptions {
      category {
        category-type;
      }
      file;
    }
  }
  finger {
    <connection-limit limit>;
    <rate-limit limit>;
  }
  ftp {
    <connection-limit limit>;
    <rate-limit limit>;
  }
  netconf {
    ssh {
      <connection-limit number>;
      <rate-limit number>;
    }
  }
  outbound-ssh {
    application-id application-id {
      device-id device-id;
      ip-address {
        port port-number;
        retry number;
        timeout value;
      }
      keep-alive number;
      reconnect-strategy (in-order | sticky);
      secret secret;
      services {
        netconf;
      }
    }
    traceoptions {
      file filename {
        <files number>;
        <match regular-expression>;
        <size maximum-file-size>;
        <world-readable | no-world-readable>;
      }
      flag flag;
```


Copyright © 2013, Juniper Networks, Inc.

```
    }
  }
  service-deployment {
    local-certificate certificate-name;
    servers server-address {
      port-number port-number;
    }
    source-address source-address;
    traceoptions {
      flag flag;
    }
  }
  ssh {
    <connection-limit limit>;
    protocol-version [v1 v2];
    <rate-limit limit>;
    root-login (allow | deny | deny-password);
  }
  telnet {
    <connection-limit limit>;
    <rate-limit limit>;
  }
  web-management {
    http {
      interface [interface-names];
      port port;
    }
    https {
      interface [interface-names];
      local-certificate name;
      pki-local-certificate name;
      port port;
      system-generated-certificate;
    }
    session {
      idle-timeout [ minutes ];
      session-limit [ session-limit ];
    }
    run-mode {
      module;
    }
  }
  xnm-clear-text {
    connection-limit limit;
    rate-limit limit;
  }
  xnm-ssl {
    connection-limit limit;
    local-certificate name;
    rate-limit limit;
  }
}
static-host-mapping hostname {
  alias [ alias ];
  inet [ address ];
  inet6 [address];
```

```
    sysid system-identifier ;
}
syslog {
    allow-duplicates
    archive {
    archive-sites url;
    <files number>;
    <size maximum-file-size>;
    <world-readable | no-world-readable>;
  }
  console {
    facility severity;
  }
  file filename {
    allow-duplicates
    facility severity;
    explicit-priority;
    match "regular-expression";
    archive {
      files number;
      size maximum-file-size;
      start-time;
      transfer-interval;
      <world-readable | no-world-readable>;
    }
  }
  host (hostname | other-routing-engine | scc-master) {
    allow-duplicates
    any;
    authorization;
    change-log;
    conflict-log;
    daemon;
    dfc;
    external;
    firewall;
    ftp;
    interactive-commands;
    kernel;
    pfe;
    user;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
  }
  source-address source-address {
    archive;
    console;
    file;
    host;
    time-format;
    user;
  }
  time-format (year | millisecond | year millisecond);
  user (username | *) {
```


Copyright © 2013, Juniper Networks, Inc.

```
        allow-duplicates
        match < regular-expression >;
      }
    }
    tacplus-options service-name service-name;
    tacplus-server server-address {
      port port-number;
      secret password;
      single-connection;
      source-address source-address;
      timeout seconds;
    }
    time-zone (GMThour-offset | time-zone);
  }
```

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices
- Device Configuration
- Upgrades and Downgrades

Copyright © 2013, Juniper Networks, Inc.

## address-book

**Syntax**

```
address-book {
    maximum amount;
    reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the number of address books that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## after-keygeneration

**Syntax** after-keygeneration (disable | enable);

**Hierarchy Level** [edit system fips self-test]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** This statement is no longer supported or needed. Known answer test (KAT) self-tests are run automatically after an OpenSSL key generation.

## allow-duplicates

**Syntax** allow-duplicates

**Hierarchy Level** [edit logical-systems *logical-system-name* system syslog],
[edit logical-systems *logical-system-name* system syslog file *file-name*],
[edit logical-systems *logical-system-name* system syslog host *host-name*],
[edit logical-systems *logical-system-name* system syslog user *user-name*],
[edit system syslog],
[edit system syslog file *file-name*],
[edit system syslog host *host-name*],
[edit system syslog user *user-name*],

**Release Information** Statement introduced in Release 11.1 of Junos OS.
Logical systems support introduced in Release 11.4 of Junos OS.

**Description** Specify whether to allow the repeated messages in the system log output files. This can be set either at global configuration level or for individual file, host, or user. By default, this parameter is set to disable.

**Options** **file**—Name of the file to log messages

**host** —Host to receive the messages

**user**—User to receive the notification of the event

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Monitoring and Troubleshooting Guide for Security Devices*
- Example: Configuring System Logging on Logical Systems

Copyright © 2013, Juniper Networks, Inc.

## appfw-rule-set

**Syntax**

```
appfw-rule-set {
    maximum amount
    reserved amount
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name* ]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Specify the number of application firewall rule set configurations that a master administrator can configure for a master logical system or user logical system when the security profile is bound to the logical systems.

The master administrator:

- Uses security profiles to provision logical systems with resources
- Binds security profiles to the master logical system and the user logical systems
- Can configure more than one security profile, allocating different numbers of resources in various profiles

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can use resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*
- *Junos OS Logical Systems Configuration Guide for Security Devices*


Copyright © 2013, Juniper Networks, Inc.

## appfw-rule

**Syntax**

```
appfw-rule {
  maximum amount
  reserved amount
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name* ]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Specify the number of application firewall rule configurations that a master administrator can configure for a master logical system or user logical system when the security profile is bound to the logical systems.

The master administrator:

- Uses security profiles to provision logical systems with resources
- Binds security profiles to the master logical system and the user logical systems
- Can configure more than one security profile, allocating different numbers of resources in various profiles

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can use resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices

Copyright © 2013, Juniper Networks, Inc.

## auth-entry

**Syntax**

```
auth-entry {
  maximum amount;
  reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the number of firewall authentication entries that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## ciphers

**Syntax** ciphers [ *cipher-1 cipher-2 cipher-3* ...]

**Hierarchy Level** [edit system services ssh]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the set of ciphers the SSH server can use to perform encryption and decryption functions.

**Options**

- **3des-cbc**—Triple Data Encryption Standard (DES) in Cipher Block Chaining (CBC) mode.
- **aes128-cbc**—128-bit Advanced Encryption Standard (AES) in CBC mode.
- **aes256-cbc**—256-bit AES in CBC mode.
- **aes128-ctr**—128-bit AES in CBC mode.
- **aes192-ctr**—192-bit AES in counter mode.
- **aes256-ctr**—256-bit AES in counter Mode.
- **arcfour128**—128-bit RC4-stream cipher in CBC mode.
- **arcfour256**—256-bit RC4-stream cipher in CBC mode.
- **blowfish128-cbc**—128-bit blowfish-symmetric block cipher in CBC mode.
- **cast128-cbc**—128-bit cast in CBC mode.



NOTE: Ciphers represent a set. To configure ssh ciphers:

user@host#**set system services ssh ciphers [ aes256-cbc aes192-cbc ]**

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Configuring SSH Service for Remote Access to the Router or Switch
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## cpu

**Syntax**

```
cpu {
  reserved percent;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Specify the percentage of CPU utilization that is always available to a logical system. This value is configured in a security profile that is bound to a logical system.

Only the master administrator can create security profiles and bind them to logical systems.



NOTE: The cpu-control option at the [edit system security-profile resources] hierarchy level must be specified for the reserved value to take effect.

**Options**

**reserved *percent***—A reserved quota that guarantees that the percentage of CPU specified is always available to the logical system.

**Range:** 0 through 100 percent (decimal point allowed).

**Default:** 1 percent for the master logical system and 0 percent for user logical systems.



CAUTION: The master logical system must not be bound to a security profile that is configured with a 0 percent reserved CPU quota as traffic loss could occur.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## day-of-month

**Syntax** day-of-month *day*;

**Hierarchy Level** [edit system fips self-test periodic]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Specify a day of the month to run the periodic FIPS self-test.

**Default** If you omit the **day-of-month** statement, the self-test runs every day at the specified start time.

**Options** ***day***—Day of the month to run the FIPS self-test.
**Range:** 1 through 31

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring FIPS Self-Tests
- month on page 1254
- self-test on page 1240
- start-time on page 1282

Copyright © 2013, Juniper Networks, Inc.

## day-of-week

**Syntax** day-of-week *day*;

**Hierarchy Level** [edit system fips self-test periodic]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Specify a day of the week to run periodic known answer test (KAT) self-tests for FIPS.

**Default** If you omit the **day-of-week** statement, the self-test runs every day at the specified start time.

**Options** ***day***—Number of the day of the week to run the FIPS self-test.
**Range:** 1 through 7 (Monday through Sunday)

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring FIPS Self-Tests
- day-of-month on page 1227
- periodic on page 1267
- self-test on page 1240
- start-time on page 1282


Copyright © 2013, Juniper Networks, Inc.

## dhcpv6 (System Services)

**Syntax**

```
dhcpv6 {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  dynamic-profile {
    junos-default-profile;
    use-primary dynamic-profile-name-string;
  }
  group group-name {
    authentication {
      password password-string;
      username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name-string;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix-string;
      }
    }
    dynamic-profile {
      junos-default-profile;
      use-primary dynamic-profile-name-string;
    }
    interface interface-name {
      exclude;
      overrides {
        interface-client-limit number;
      }
      trace;
      upto upto-interface-name;
    }
    overrides {
      interface-client-limit number;
    }
    reconfigure {
      attempts number;
      clear-on-abort;
```

Copyright © 2013, Juniper Networks, Inc.

```
        strict;
        timeout number;
        token token-name;
        trigger {
          radius-disconnect;
        }
      }
    }
    overrides {
      interface-client-limit number;
    }
    reconfigure {
      attempts number;
      clear-on-abort;
      strict;
      timeout number;
      token token-name;
      trigger {
        radius-disconnect;
      }
    }
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Configure DHCPv6 server to provide IPv6 addresses to clients.



NOTE: SRX Series and J Series devices do not support client authentication.

**Options**

- **duplicate-clients-on-interface**—Allow duplicate clients on different interfaces in a subnet.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

## dhcp-local-server (System Services)

**Syntax**

```
dhcp-local-server {
  dhcpv6 {
    authentication {
      password password-string;
      username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name-string;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix-string;
      }
    }
    dynamic-profile {
      junos-default-profile;
      use-primary dynamic-profile-name-string;
    }
    group group-name {
      authentication {
        password password-string;
        username-include {
          circuit-type;
          client-id;
          delimiter delimiter-character;
          domain-name domain-name-string;
          relay-agent-interface-id;
          relay-agent-remote-id;
          relay-agent-subscriber-id;
          routing-instance-name;
          user-prefix user-prefix-string;
        }
      }
      dynamic-profile {
        junos-default-profile;
        use-primary dynamic-profile-name-string;
      }
      interface interface-name {
        exclude;
        overrides {
          interface-client-limit number;
        }
        trace;
        upto upto-interface-name;
      }
      overrides {
        interface-client-limit number;
      }
      reconfigure {
        attempts number;
```

Copyright © 2013, Juniper Networks, Inc.

```
            clear-on-abort;
            strict;
            timeout number;
            token token-name;
            trigger {
              radius-disconnect;
            }
          }
        }
        overrides {
          interface-client-limit number;
        }
        reconfigure {
          attempts number;
          clear-on-abort;
          strict;
          timeout number;
          token token-name;
          trigger {
            radius-disconnect;
          }
        }
      }
      duplicate-clients-on-interface;
      forward-snooped-clients {
        all-interfaces;
        configured-interfaces;
        non-configured-interfaces;
      }
      interface-traceoptions {
        file filename {
          files number;
          match regular-expression;
          size maximum-file-size;
          <world-readable | no-world-readable>;
        }
        flag {
          all;
          dhcpv6-packet;
          dhcpv6-packet-option;
          dhcpv6-state;
          packet;
          packet-option;
          state;
        }
        no-remote-trace;
      traceoptions {
        file filename {
          files number;
          match regular-expression;
          size maximum-file-size;
          <world-readable | no-world-readable>;
        }
        flag {
          all;
          auth;
```


Copyright © 2013, Juniper Networks, Inc.

```
        database;
        dhcpv6-general;
        dhcpv6-io;
        dhcpv6-packet;
        dhcpv6-packet-option;
        dhcpv6-rpd;
        dhcpv6-session-db;
        dhcpv6-state;
        fwd;
        general;
        ha;
        interface;
        io;
        packet;
        packet-option;
        performance;
        profile;
        rpd;
        rtsock;
        session-db
        state;
        statistics;
        ui;
    }
    no-remote-trace;
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Configure DHCP Local Server for DHCPv6, forwarding snoop (unicast) packets, and setting traceoptions.



NOTE: SRX Series and J Series devices do not support client authentication.

**Options**

- **duplicate-clients-on-interface**—Allow duplicate clients on different interfaces in a subnet.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Device Configuration

Copyright © 2013, Juniper Networks, Inc.

## disable (System Services)

**Syntax** disable

**Hierarchy Level** [edit system services dns dnssec]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Disables DNSSEC in the DNS server.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

## dlv

**Syntax**
```
dlv {
  domain-name domain-name {
    trusted-anchor trusted-anchor;
  }
}
```

**Hierarchy Level** [edit system services dns dnssec]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configures DNS Lookaside Validation (DLV) in the DNS server.

**Options** **domain-name**—Name of the domain.

**trusted-anchor**—Name of the trusted DLV anchor.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## dns (System Services)

**Syntax**

```
dns {
  dnssec {
    disable;
    dlv {
      domain-name domain-name {
        trusted-anchor trusted-anchor;
      }
    }
    secure-domains [domain-name];
    trusted-keys {
      key key;
      load-key-file {
        dns-keys;
      }
    }
  }
  max-cache-ttl;
  max-ncache-ttl;
  traceoptions {
    category {
      category-type;
    }
    file;
  }
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configures the DNS server.

**Options**

- **dnssec**—This option is explained separately.
- **max-cache-ttl**—Maximum time-to-live (TTL) for cached responses, in seconds. The configurable range varies from 0 through 604800 seconds.
- **max-ncache-ttl**—Maximum time-to-live (TTL) for cached negative responses, in seconds. The configurable range varies from 0 through 604800 seconds.
- **traceoptions**—DNS server trace options. This option is explained separately.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## dns-proxy

**Syntax**

```
dns-proxy
{
  cache;
  default-domain;
  interfaces;
  view;
}
```

**Hierarchy Level** [edit system services dns dns-proxy]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Configure the device as a DNS proxy server by enabling DNS proxy on a logical interface.

**Options**

- **cache**—Configure DNS proxy static cache entries.
- **default-domain**—Configure the domain for split DNS.
- **interfaces**—Configure the interface for a DNS proxy.
- **view**—Configure the view for split DNS.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Zones and Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## dnssec

**Syntax**

```
dnssec {
  disable;
  dlv {
    domain-name domain-name {
      trusted-anchor trusted-anchor;
    }
  }
  secure-domains [domain-name];
  trusted-keys {
    key key;
    load-key-file {
    dns-keys;
    }
  }
}
```

**Hierarchy Level** [edit system services dns]

**Release Information** Statement introduced in Release 10.2 of Junos OS.

**Description** Configure DNSSEC in the DNS server.

**Options** The options are explained separately

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## dslite-softwire-initiator

**Syntax**

```
dslite-softwire-initiator {
  maximum amount;
  reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 12.1 of Junos OS.

**Description** Specify the number of IPv6 dual-stack lite (DS-Lite) softwire initiators that can connect to the softwire concentrator configured in either a user logical system or the master logical system. This statement is configured in the security profile that is bound to the logical system.

Only the master administrator can create security profiles and bind them to logical systems. The master administrator:

- Uses security profiles to provision logical systems with resources
- Binds security profiles to user logical systems and the master logical system
- Configures more than one security profile, specifying different amounts of resource allocations in various profiles

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources. The default is the system maximum.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system. The default is 0.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## dynamic-dns

**Syntax**

```
dynamic-dns
{
  client <client name>
  {
    server;
    agent;
    username;
    password;
    interface;
  }
}
```

**Hierarchy Level** [edit system services dynamic-dns]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Configure the device as a dynamic DNS server that maintains the list of the changed addresses and their associated domain names registered with it. The device updates these DDNS servers with this information periodically or whenever there is a change in IP addresses.

**Options**

- **client** —Specifies the hostname of the registered client.
- **server**—Specifies the name of the dynamic DNS server that allows dynamic DNS clients to update the IP address changes associated with the registered hostname.
- **agent**—Specifies the name of the dynamic DNS agent.
- **username**—Specifies the dynamic DNS username.
- **password**—Specifies the password.
- **interface** —Specifies the interface whose IP address is mapped to the registered domain name.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Security Zones and Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## self-test

**Syntax**

```
self-test {
  periodic {
    day-of-month day;
    day-of-week day;
    month month;
    start-time time;
  }
}
```

**Hierarchy Level** [edit system fips]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Schedule periodic known answer test (KAT) self-tests to validate the output of cryptographic algorithms approved for the Federal Information Processing Standard (FIPS) and to test the integrity of some system modules.

If a manually executed KAT fails, the system writes a log message to the system log messages file with details of the failure. Then the system enters FIPS error state (panic) and reboots.

If the KATs succeed, the system displays "Passed" for each successful test and updates the system log file to display the tests that were executed.

To display the system log file, enter the **file show /var/log/messages** command.

**Default** If you omit the **self-test** statement, the self-tests do not run unless you run them manually by issuing the **request system fips self-test** command.

**Options** Configuration options are explained separately.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring FIPS Self-Tests
- day-of-month on page 1227
- day-of-week on page 1228
- month on page 1254
- periodic on page 1267
- request system fips self-test on page 1543
- start-time on page 1282


Copyright © 2013, Juniper Networks, Inc.

## firewall-authentication-service

**Syntax** firewall-authentication-service (enable | disable);

**Hierarchy Level** [edit system processes]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable or disable the firewall authentication service process.

**Options**
- **enable**—Start the firewall authentication service process.
- **disable**—Stop the firewall authentication service process.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## flow-gate

**Syntax**

```
flow-gate {
  maximum amount;
  reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the number of flow gates, also known as *pinholes*, that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## flow-session

**Syntax**

```
flow-session {
  maximum amount;
  reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the number of flow sessions that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.



NOTE: An IPv6 session consumes twice the memory of an IPv4 session. Therefore the number of sessions available for IPv6 is half the reserved and maximum quotas configured for the flow session resource in a security profile. Use the vty command **show usp flow resource usage cp-session** to check flow session usage.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Copyright © 2013, Juniper Networks, Inc.

**Related Documentation**
- Master Administrator for Logical Systems on Security Devices

## general-authentication-service

**Syntax**

```
general-authentication-service {
  (enable | disable);
  traceoptions {
    file filename {
      <files number >;
      <match regular-expression>;
      <size maximum-file-size>;
      <world-readable | no-world-readable>;
    }
    flag flag ;
  }
}
```

**Hierarchy Level** [edit system processes]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable or disable the general authentication process.

**Options**
- **enable**—Start the general authentication service process.
- **disable**—Stop the general authentication service process.

The remaining statements are explained separately.

**Required Privilege Level**
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## group (System Services DHCP)

**Syntax**

```
group group-name {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  dynamic-profile {
    junos-default-profile;
    use-primary dynamic-profile-name-string;
  }
  interface interface-name {
    exclude;
    overrides {
      interface-client-limit number;
    }
    trace;
    upto upto-interface-name;
  }
  overrides {
    interface-client-limit number;
  }
  reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
      radius-disconnect;
    }
  }
}
```

**Hierarchy Level** [edit system services dhcp-local-server dhcpv6]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Configure a group of interfaces that have a common configuration. The remaining statements are explained separately.

**Options**

- *group-name*—Name of the group.

Copyright © 2013, Juniper Networks, Inc.



NOTE: SRX Series and J Series devices do not support DHCP client authentication.

**Required Privilege Level**
access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration

## hostkey-algorithm

**Syntax**
hostkey-algorithm <*algorithm* | *no-algorithm*>

**Hierarchy Level**
[edit system services ssh]

**Release Information**
Statement introduced in Release 11.2 of Junos OS.
<*algorithm* | *no algorithm*> statements introduced in Release 12.2 of Junos OS.

**Description**
Allow or disallow a host-key signature algorithm for the SSH host to use to authenticate another host.

**Options**
- **ssh-dss**—Allow generation of a 1024-bit Digital Signature Algorithm (DSA) host-key.
- **no-ssh-dss**—Do not allow generation of a 1024-bit Digital Signature Algorithm (DSA) host-key.
- **ssh-ecdsa**—Allow generation of an Elliptic Curve Digital Signature Algorithm (ECDSA) host-key.
- **no-ssh-ecdsa**—Do not allow generation of an Elliptic Curve Digital Signature Algorithm (ECDSA) host-key.
- **ssh-rsa**—Allow generation of an RSA host-key.
- **no-ssh-rsa**—Do not allow generation of an RSA host-key.

**Required Privilege Level**
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Configuring SSH Service for Remote Access to the Router or Switch
- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

## idp-policy

**Syntax** idp-policy *idp-policy-name*;

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Specify the IDP policy for the security profile.

**Options** *idp-policy-name*—Name of the IDP policy.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- IDP Policies for Security Devices
- Master Administrator for Logical Systems on Security Devices

Copyright © 2013, Juniper Networks, Inc.

## interface (System Services DHCP)

**Syntax**

```
interface interface-name {
  exclude;
  overrides {
    interface-client-limit number;
  }
  trace;
  upto upto-interface-name;
}
```

**Hierarchy Level** [edit system services dhcp-local-server dhcpv6 group*group-name*]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP local server is enabled. You can repeat the interface interface-name statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group.

**Options**

- *interface-name*—Name of the interface.
- **trace**—Enable tracing of the interface specified by the *interface-name* argument.
- **upto** *upto-interface-name*—The upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the *upto-interface-name* must be the same as the device name of the *interface-name*.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**

- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

## interface-traceoptions (System Services DHCP)

**Syntax**

```
interface-traceoptions {
  file <filename> <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  no-remote-trace;
}
```

**Hierarchy Level** [edit routing-instances *routing-instance-name* system services dhcp-local-server], [edit system services dhcp-local-server]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Configure extended DHCP local server tracing operations that can be enabled on a specific interface or group of interfaces. You use the **interface *interface-name* trace** statement at the **[edit system services group *group-name*]** hierarchy level to enable the tracing operation on the specific interfaces.

**Options** ***file-name***—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (“ ”). All files are placed in a file named **jdhcpd** in the directory **/var/log**. If you include the **file** statement, you must specify a filename.

**files *number***—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

**Range:** 2 through 1000

**Default:** 3 files

**flag *flag***—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all events
- **dhcpv6-packet**—Trace DHCPv6 packet decoding operations.
- **dhcpv6-packet-option**—Trace DHCPv6 option decoding operations.
- **dhcpv6-state**—Trace changes in state for DHCPv6 operations.
- **packet**—Trace packet decoding operations
- **packet-option**—Trace DHCP option decoding operations
- **state**—Trace changes in state

**match *regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

**no-remote-trace**—Disable remote tracing.

Copyright © 2013, Juniper Networks, Inc.

**no-world-readable**—(Optional) Disable unrestricted file access.

**size *size***—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**Syntax:** **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

**Range:** 10 KB through 1 GB

**Default:** 128 KB

**world-readable**—(Optional) Enable unrestricted file access.

**Required Privilege Level**

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

## key-exchange

**Syntax** key-exchange <*algorithm*>

**Hierarchy Level** [edit system services ssh]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the set of Diffie-Hellman key exchange methods that the SSH server can use.

**Options**

- **ecdh-sha2-nistp256**—The ECDH key exchange method with ephemeral keys generated on the nistp256 curve.
- **ecdh-sha2-nistp384**—The ECDH key exchange method with ephemeral keys generated on the nistp384 curve.
- **ecdh-sha2-nistp521**—The ECDH key exchange method with ephemeral keys generated on the nistp521 curve.
- **group-exchange-sha2**—The group exchange algorithm using SHA-2.
- **group-exchange-sha1**—The group exchange algorithm using SHA-1.
- **dh-group14-sha1**—The Diffie-Hellman group14 algorithm using SHA-1.
- **dh-group1-sha1**—The Diffie-Hellman group1 algorithm using SHA-1.



NOTE: **The key-exchange represents a set. To configure key-exchange:**

```
user@host#set system services ssh key-exchange [ecdh-sha2-nistp256
  group-exchange-sha1]
```

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Configuring SSH Service for Remote Access to the Router or Switch
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## logical-system (System Security Profile)

**Syntax** logical-system *logical-system-name*;

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the user logical system to bind the security profile to.

The master administrator uses security profiles to provision logical systems with resources. You can bind security profiles to user logical systems and the master logical system. The master administrator can configure more than one security profile allocating different amounts of a resource in various ones.

Only the master administrator can create security profiles and bind them to logical systems.

**Options** ***logical-system-name***—Name of the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Master Administrator for Logical Systems on Security Devices

## lockout-period

**Syntax** lockout-period *minutes*;

**Hierarchy Level** **[edit system login retry-options]**

**Release Information** Statement introduced in Junos OS Release 11.2.

**Description** Configure the amount of time before the user can attempt to log in to the router after being locked out due to the number of failed login attempts specified in the **tries-before-disconnect** statement.

**Options** *minutes*—Amount of time before the user can attempt to log in after being locked out.
**Default:** 120
**Range:** 1 through 43200

**Required Privilege Level** admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Documentation**
- Limiting the Number of User Login Attempts for SSH and Telnet Sessions
- retry-options
- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

## macs

**Syntax** macs <*algorithm*>

**Hierarchy Level** [edit system services ssh]

**Release Information** Statement introduced in Release 11.2 of Junos OS.
SHA-2 options introduced in Release 12.1 of Junos OS.

**Description** Specify the set of message authentication code (MAC) algorithms that the SSH server can use to authenticate messages.

**Options**

- **hmac-md5**—Hash-based MAC using Message-Digest 5 (MD5).
- **hmac-md5-96**—96-bits of Hash-based MAC using MD5.
- **hmac-ripemd160**—Hash-based MAC using RIPEMD.
- **hmac-sha1**—Hash-based MAC using Secure Hash Algorithm (SHA-1).
- **hmac-sha1-96**—96-bits of Hash-based MAC using SHA-1.
- **hmac-sha2-256**—256-bits of Hash-based MAC using SHA-2.
- **hmac-sha2-256-96**—first 96-bits of hmac-sha2-256.
- **hmac-sha2-512**—96-bits of Hash-based MAC using SHA-1.
- **umac-64**—Message Authentication Code using Universal Hashing.



NOTE: The *macs* configuration statement represents a set. Therefore, it should be configured as in the following.

```
user@host#set system services ssh macs [hmac-md5 hmac-sha1]
```

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Configuring SSH Service for Remote Access to the Router or Switch
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## month

**Syntax** month *month*;

**Hierarchy Level** [edit system fips self-test periodic]

**Release Information** Statement introduced in Release 11.1 Junos OS.

**Description** Specify a month to run periodic known answer test (KAT) self-tests for FIPS.

**Default** If you omit the **month** statement, the self-tests run every month on the specified day and at the specified start time.

**Options** *month*—Number of the month in which to run the FIPS self-tests.
**Range:** 1 through 12

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring FIPS Self-Tests
- day-of-month on page 1227
- day-of-week on page 1228
- self-test on page 1240
- start-time on page 1282

 Copyright © 2013, Juniper Networks, Inc.

## nat-cone-binding

**Syntax**

```
nat-cone-binding {
    maximum amount;
    reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the number of NAT cone binding configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices

Copyright © 2013, Juniper Networks, Inc.

## nat-destination-pool

**Syntax**

```
nat-destination-pool {
  maximum amount;
  reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the number of NAT destination pool configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## nat-destination-rule

**Syntax**

```
nat-destination-rule {
    maximum amount;
    reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the number of NAT destination rule configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices

Copyright © 2013, Juniper Networks, Inc.

## nat-nopat-address

**Syntax**

```
nat-nopat-address {
  maximum amount;
  reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the number of NAT without port address translation configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## nat-pat-address

**Syntax**

```
nat-pat-address {
  maximum amount;
  reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the number of NAT with port address translation (PAT) configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Application Layer Gateways for Security Devices
- Master Administrator for Logical Systems on Security Devices

Copyright © 2013, Juniper Networks, Inc.

## nat-pat-portnum

**Syntax**

```
nat-pat-portnum {
  maximum amount
  reserved amount
}
```

**Hierarchy Level** [edit system security-profile *profile-name*]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Specify the maximum quantity and the reserved quantity of ports for the logical system as part of its security profile. The total number of PAT pools must not exceed the configured maximum ports for the logical system.

**Options**

**maximum *amount***—Specify the maximum number of ports allowed for a logical system. The maximum quantity is not guaranteed and is shared among multiple logical systems.

**reserved *amount***—Specify the number of resources guaranteed for a logical system.

**Range:** For SRX1400, SRX3400, and SRX3600 devices, up to 268,435,456 ports are supported. For SRX5600 and SRX5800 devices, up to 402,653,184 ports are supported.. Pool specifications for logical systems can be viewed using the **show security nat source summary logical-system all** command.

**Required Privilege Level** system—To view this statement in the configuration.
system—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## nat-port-ol-ipnumber

**Syntax**

```
nat-port-ol-ipnumber {
    maximum amount;
    reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the number of NAT port overloading IP number configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices

Copyright © 2013, Juniper Networks, Inc.

## nat-source-pool

**Syntax**

```
nat-source-pool {
  maximum amount;
  reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the NAT source pool configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## nat-source-rule

**Syntax**

```
nat-source-rule {
  maximum amount;
  reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the NAT source rule configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices

Copyright © 2013, Juniper Networks, Inc.

## nat-static-rule

**Syntax**

```
nat-static-rule {
  maximum amount;
  reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the number of NAT static rule configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## network-security

**Syntax** network-security (enable | disable);

**Hierarchy Level** [edit system processes]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable or disable the network security process on the device.

**Options**
- **enable**—Start the network security process.
- **disable**—Stop the network security process.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## overrides (System Services DHCP)

**Syntax**

```
overrides {
  interface-client-limit number
}
```

**Hierarchy Level**

[edit system services dhcp-local-server dhcpv6]
[edit system services dhcp-local-server dhcpv6 group *group-name*]
[edit system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name*]

**Release Information**

Statement introduced in Release 10.4 of Junos OS.

**Description**

Override the default configuration settings for the extended DHCP local server. Specifying the **overrides** statement with no subordinate statements removes all DHCP local server overrides at that hierarchy level.

- To override global DHCP local server configuration options, include the **overrides** statement and its subordinate statements at the **[edit system services dhcp-local-server]** hierarchy level.
- To override configuration options for a named group of interfaces, include the statements at the **[edit system services dhcp-local-server dhcpv6 group *group-name*]** hierarchy level.
- To override configuration options for a specific interface within a named group of interfaces, include the statements at the **[edit system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name*]** hierarchy level.
- Use the DHCPv6 hierarchy levels to override DHCPv6 configuration options.

**Options**

**interface-client-limit *number***—Sets the maximum number of DHCP clients per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group.

**Range:** 1 through 500,000

**Default:** No limit

**Required Privilege Level**

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

## periodic

**Syntax**

```
periodic {
  day-of-month day;
  day-of-week day;
  month month;
  start-time time;
}
```

**Hierarchy Level** [edit system fips self-test]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Specify a day, month, and time to run periodic known answer test (KAT) self-tests for FIPS.

**Default** If you omit the **periodic** statement, the self-tests do not run unless you run them manually by issuing the **request system fips self-test** command.

**Options** The configuration options are explained separately.

**Required Privilege Level**
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring FIPS Self-Tests
- day-of-week on page 1228
- day-of-month on page 1227
- month on page 1254
- request system fips self-test on page 1543
- self-test on page 1240
- start-time on page 1282

Copyright © 2013, Juniper Networks, Inc.

## pki-local-certificate

**Syntax** pki-local-certificate *name*;

**Hierarchy Level** [edit system services web-management https]

**Release Information** Statement introduced in Release 9.1 of Junos OS.

**Description** Specify the name of the certificate that is generated by public key infrastructure (PKI) and authenticated by certificate authority (CA).

**Options** ***name*** —Name of certificate.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## policy (System Security Profile)

**Syntax**

```
policy {
  maximum amount;
  reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Junos OS Release 11.2.

**Description** Specify the number of security policies that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices

Copyright © 2013, Juniper Networks, Inc.

## policy-with-count

**Syntax**

```
policy-with-count {
  maximum amount;
  reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the number of security policies with a count that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## propagate-settings

**Syntax** propagate-settings *logical-interface-name* ;

**Hierarchy Level** [edit system **services dhcp**],
[edit system **services dhcp** pool]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable or disable the propagation of TCP/IP settings received on the device acting as Dynamic Host Configuration Protocol (DHCP) client. The settings can be propagated to the server pool running on the device. Use the **system services dhcp** statement to set this feature globally. Use the **system services dhcp pool** statement to set the feature for the address pool and override the global setting.

**Options** *logical-interface-name* —Name of the logical interface to receive TCP/IP settings from the external network for propagation to the DHCP pool running on the device.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Initial Configuration Guide for Security Devices*

Copyright © 2013, Juniper Networks, Inc.

## reconfigure (System Services DHCP)

**Syntax**

```
reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout seconds;
    token token-name;
}
```

**Hierarchy Level**

[edit system services dhcp-local-server dhcpv6]
[edit system services dhcp-local-server group *group-name*]
[edit system services dhcp-local-server dhcpv6 group *group-name*]

**Release Information**

Statement introduced in Release 10.4 of Junos OS.

**Description**

Enable dynamic reconfiguration triggered by the DHCP local server of all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. A group configuration takes precedence over a DHCP local server configuration.

**Options**

**attempts *number***—Configure maximum number of attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces before reconfiguration is considered to have failed. A group configuration takes precedence over a DHCP local server configuration.

**Range:** 1 through 10 attempts

**Default:** 8 attempts

**clear-on-abort** —Delete all DHCP clients or only the DHCP clients serviced by the specified group of interfaces when reconfiguration fails; that is, when the maximum number of retry attempts have been made without success. A group configuration takes precedence over a DHCP local server configuration.

**strict** —Configure the system to only allow packets that contain the reconfigure accept option.

**timeout *seconds***—Configure the initial value in seconds between attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. Each successive attempts doubles the interval between attempts. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on. A group configuration takes precedence over a DHCP local server configuration.

**Range:** 1 through 10 seconds

**Default:** 2 seconds

**token *token-name***—Configure a plain-text token for all DHCP clients or only the clients specified by the specified group of interfaces. The default is null (empty string).

**Required Privilege Level**

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.


Copyright © 2013, Juniper Networks, Inc.

**Related Documentation**
- Device Configuration

## reverse ssh

**Syntax** reverse ssh

**Hierarchy Level** [edit system services reverse ssh]

**Release Information** Statement introduced in Release 9.6 of Junos OS.

**Description** Reverse Telnet allows you to configure a device to listen on a specific port for telnet and SSH (secure shell) services. When you connect to that port, the device provides an interface to the auxiliary port on the device. Use reverse SSH to encrypt the reverse telnet communication between the device and the client.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration

## reverse ssh port

**Syntax** reverse ssh port *5000*

**Hierarchy Level** [edit system services reverse ssh port 5000]

**Release Information** Statement introduced in Release 9.6 of Junos OS.

**Description** Reverse SSH allows you to configure a device to listen on a specific port for telnet and SSH (secure shell) services. When you connect to that port, the device provides an interface to the auxiliary port on the device. You can control the port that is used. By default, port 2901 is used.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration

Copyright © 2013, Juniper Networks, Inc.

## reverse telnet

**Syntax** reverse telnet

**Hierarchy Level** [edit system services reverse telnet]

**Release Information** Statement introduced in Release 9.6 of Junos OS.

**Description** Reverse Telnet allows you to configure a device to listen on a specific port for telnet and SSH (secure shell) services. When you connect to that port, the device provides an interface to the auxiliary port on the device.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration

## reverse telnet port

**Syntax** reverse telnet port *6000*

**Hierarchy Level** [edit system services reverse telnet port 6000]

**Release Information** Statement introduced in Release 9.6 of Junos OS.

**Description** Reverse Telnet allows you to configure a device to listen on a specific port for telnet and SSH (secure shell) services. When you connect to that port, the device provides an interface to the auxiliary port on the device. You can control the port that is used. By default, port 2900 is used.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

## root-logical-system

**Syntax** root-logical-system;

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify root-logical-system to bind the security profile to the master logical system.

The master administrator uses security profiles to provision logical systems with resources. The security profile containing this statement must be bound to root-logical-system only.

Only the master administrator can create security profiles and bind them to logical systems.

**Options** none

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Master Administrator for Logical Systems on Security Devices

## run-mode

**Syntax**
```
web-management {
  module-mode;
    http;
  }
}
```

**Hierarchy Level** [edit system services web-management]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Configure the run mode module.

**Options** ***module***—Specify the module as PHP.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- *Junos OS Security Configuration Guide*

Copyright © 2013, Juniper Networks, Inc.

## scheduler (System Security Profile)

**Syntax**

```
scheduler {
    maximum amount;
    reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Release 11.2 of Junos OS.

**Description** Specify the number of schedulers that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## secure-domains

**Syntax** secure-domains [*domain-name*];

**Hierarchy Level** **[edit system services dns dnssec]**

**Release Information** Statement introduced in Junos OS Release 10.2.

**Description** Configure secure domains in the DNS server. The server accepts only signed responses for this domain. For unsigned responses, the server returns SERVFAIL error to the client.

**Options** **domain-name**—Name of the domain.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Security Zones and Interfaces for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## security-profile

**Syntax**

```
security-profile security-profile-name {
    address-book {
      maximum amount;
      reserved amount;
    }
    appfw-rule {
      maximum amount;
      reserved amount;
    }
    appfw-rule-set {
      maximum amount;
      reserved amount;
    }
    auth-entry {
      maximum amount;
      reserved amount;
    }
    cpu {
      reserved percent;
    }
    dslite-softwire-initiator {
      maximum amount;
      reserved amount;
    }
    flow-gate {
      maximum amount;
      reserved amount;
    }
    flow-session {
      maximum amount;
      reserved amount;
    }
    idp-policy idp-policy-name;
    logical-system logical-system-name;
    nat-cone-binding {
      maximum amount;
      reserved amount;
    }
    nat-destination-pool {
      maximum amount;
      reserved amount;
    }
    nat-destination-rule {
      maximum amount;
      reserved amount;
    }
    nat-nopat-address {
      maximum amount;
      reserved amount;
    }
    nat-pat-address {
      maximum amount;
```


Copyright © 2013, Juniper Networks, Inc.

```
    reserved amount;
}
nat-pat-portnum {
    maximum amount
    reserved amount
}
nat-port-ol-ipnumber {
    maximum amount;
    reserved amount;
}
nat-source-pool {
    maximum amount;
    reserved amount;
}
nat-source-rule {
    maximum amount;
    reserved amount;
}
nat-static-rule {
    maximum amount;
    reserved amount;
}
policy {
    maximum amount;
    reserved amount;
}
policy-with-count {
    maximum amount;
    reserved amount;
}
root-logical-system;
scheduler {
    maximum amount;
    reserved amount;
}
zone {
    maximum amount;
    reserved amount;
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced in Release 11.2 of Junos OS. The **dslite-softwire-initiator** option introduced in Release 12.1 of Junos OS.

Copyright © 2013, Juniper Networks, Inc.

**Description** Create a security profile and specify the kinds and amounts of resources to allocate to a logical system to which the security profile is bound.

As a master administrator, you can create a security profile and bind it to more than one logical system if you want to allocate the same kinds and amounts of resources to them. For details on how many security profiles you can create, see Understanding Logical System Security Profiles. When you reach the limit, you must delete a security profile and commit the configuration before you can create and commit the configuration for another security profile.

Only the master administrator can create security profiles.

**Options**

- ***security-profile-name***—Name of the security profile.

The remaining statements are explained separately.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices


Copyright © 2013, Juniper Networks, Inc.

## security-profile resources

**Syntax**

```
security-profile resources {
  cpu-control;
  cpu-control-target percent;
}
```

**Hierarchy Level** [edit system]

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Configure global settings that apply to all logical systems in the device.

**Options**

**cpu-control**—Enable CPU utilization control.

**cpu-control-target** ***percent***—Specify the upper limit for CPU utilization on the device under normal operating conditions.

**Range:** 0 through 100 percent (decimal point allowed).

**Default:** 80 percent.



NOTE: **The cpu-control option must be specified for the cpu-control-target value to take effect.**

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Master Administrator for Logical Systems on Security Devices

Copyright © 2013, Juniper Networks, Inc.

## start-time (FIPS)

**Syntax** start-time *time*;

**Hierarchy Level** [edit system fips self-test periodic]

**Release Information** Statement introduced in Release 11.1 Junos OS.

**Description** Specify a time to run periodic known answer test (KAT) self-tests for FIPS.

**Default** If you omit the **start-time** statement, the self-tests do not run . You can execute them manually by issuing the **request system fips self-test** command.

**Options** ***time***—Start time for FIPS self-test. Enter the hour and minutes in hh:mm format. For example, to schedule the self-tests to start at 9:00 AM PST, you enter **09:00**.

**Syntax:** *hh:mm*

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring FIPS Self-Tests
- day-of-week on page 1228
- day-of-month on page 1227
- month on page 1254
- periodic on page 1267
- request system fips self-test on page 1543
- self-test on page 1240

## system-generated-certificate (System Services)

**Syntax** system-generated-certificate;

**Hierarchy Level** [edit system services web-management https]

**Description** Automatically generated self-signed certificate

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (System Services DHCP)

**Syntax**

```
traceoptions {
  file <filename> <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  no-remote-trace;
}
```

**Hierarchy Level** [edit routing-instances *routing-instance-name* system services dhcp-local-server], [edit system services dhcp-local-server]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Configure extended DHCP local server tracing operations for DHCP processes.

**Options**

- ***file-name***—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" "). All files are placed in a file named **jdhcpd** in the directory **/var/log**. If you include the **file** statement, you must specify a filename.
- **files *number***—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

  **Range:** 2 through 1000

  **Default:** 3 files

- **match *regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.
- **size *maximum-file-size***—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

  **Syntax:** **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

  **Range:** 10 KB through 1 GB

  **Default:** 128 KB

- **world-readable**—(Optional) Enable unrestricted file access.
- **no-world-readable**—(Optional) Disable unrestricted file access.
- **flag *flag***—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:
  - **all**—Trace all events.
  - **database**—Trace database operations.
  - **dhcpv6-general**—Trace operations for DHCPv6.
  - **dhcpv6-io**—Trace input/output operations for DHCPv6.

Copyright © 2013, Juniper Networks, Inc.

- **dhcpv6-packet**—Trace DHCPv6 packet decoding operations.
- **dhcpv6-packet-option**—Trace DHCPv6 option decoding operations.
- **dhcpv6-rpd**—Trace routing protocol process operations.
- **dhcpv6-session-db**—Trace session database operations for DHCPv6.
- **dhcpv6-state**—Trace changes in state for DHCPv6 operations.
- **fwd**—Trace firewall process operations.
- **general**—Trace miscellaneous general operations.
- **ha**—Trace high-availability related operations.
- **interface**—Trace interface operations.
- **io**—Trace input/output operations.
- **packet**—Trace packet decoding operations.
- **packet- option**—Trace DHCP option decoding operations.
- **performance**—Trace DHCP performance measurement operations.
- **profile**—Trace DHCP profile operations.
- **rpd**—Trace routing protocol process operations.
- **rtsock**—Trace routing socket operations.
- **session-db**—Trace session database operations.
- **state**—Trace changes in state.
- **statistics**—Trace changes in statistics.
- **ui**—Trace changes in user interface operations.

- **no remote-trace**—Disable remote tracing.

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (System Services DNS)

**Syntax**

```
traceoptions {
  category {
    category-type;
  }
  file;
}
```

**Hierarchy Level** [edit system services dns]

**Release Information** Statement introduced in Junos OS Release 10.2.

**Description** Defines tracing options for DNS services.

**Options**

**category**—Specifies the logging category. SeeTable 7 on page 1286 for the different logging categories and their descriptions.

**file**—Trace file information.

Copyright © 2013, Juniper Networks, Inc.

### Table 7: Category Names

| Category Name | Description |
|---|---|
| client | Processing of client requests |
| config | Configuration file parsing and processing |
| database | Messages relating to the databases |
| default | Categories for which there is no specific configuration |
| delegation-only | Delegation only |
| dispatch | Dispatching of incoming packets to the server |
| dnssec | DNSSEC and TSIG protocol processing |
| edns-disabled | Log query using plain DNS |
| general | General information |
| lame-servers | Lame servers |
| network | Network options |
| notify | NOTIFY protocol |
| queries | DNS query resolver |
| resolver | DNS resolution security |
| security | Approval and denial of requests |
| unmatched | Unable to determine the class for messages named |
| update | Dynamic updates |
| update-security | Approval and denial of update requests |
| xfer-in | Zone transfers that the server is receiving xfer-out |
| xfer-out | Zone transfers that the server is sending |

**Required Privilege Level**
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Security Zones and Interfaces for Security Devices


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (System Processes General Authentication)

**Syntax**

```
traceoptions {
  file filename {
    <files number;
    <match regular-expression>;
    <size maximum-file-size>;
    <world-readable | no-world-readable>;
  }
  flag flag;
}
```

**Hierarchy Level** [edit system processes general-authentication-service]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure tracing operations for general-authentication-service processes.

**Options**

**file** *filename* —By default, the name of the log file that records trace output is the name of the process being traced. Use this option to specify another name.

**files** *number* —(Optional) Specify the maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed to *trace-file* **.0,** then *trace-file.1* , and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

**Range:** 2 through 1000 files

**Default:** 10 files

**match** *regular-expression* —(Optional) Refine the output to include lines that contain the regular expression.

**size** *maximum-file-size* —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file* **.0**. When the **trace-file** again reaches its maximum size, *trace-file* **.0** is renamed *trace-file* **.1** and *trace-file* is renamed *trace-file* **.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

**Syntax:** *x* **k** to specify KB, *x* **m** to specify MB, or *x* **g** to specify GB

**Range:** 10 KB through 1 GB

**Default:** 128 KB

**world-readable | no-world-readable**—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option

Copyright © 2013, Juniper Networks, Inc.

enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

**flag** *flag* —Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags.

- **all** —Trace with all flags enabled
  - **configuration** —Trace configuration events
  - **framework**—Trace authentication framework events
  - **ldap** —Trace ldap authentication events
  - **local-authentication**—Trace local authentication events
  - **radius** —Trace radius authentication events

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (System Processes WAN Acceleration)

**Syntax**

```
traceoptions {
  file filename {
    <files number> ;
    <match regular-expression>;
    <size maximum-file-size>;
    <world-readable | no-world-readable>;
  }
  flag flag ;
}
```

**Hierarchy Level** [edit *system* **processes** wan-acceleration]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Configure tracing operations for WXC Integrated Services Module (ISM 200) processes.

**Options**

**file** *filename* —By default, the name of the log file that records trace output is the name of the process being traced. Use this option to specify another name.

**files** *number* —(Optional) Specify the maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed to *trace-file* **.0,** then *trace-file.1* , and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

**Range:** 2 through 1000 files

**Default:** 10 files

**match** *regular-expression* —(Optional) Refine the output to include lines that contain the regular expression.

**size** *maximum-file-size* —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file* **.0**. When the **trace-file** again reaches its maximum size, *trace-file* **.0** is renamed *trace-file* **.1** and *trace-file* is renamed *trace-file* **.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

**Syntax:** *x* **k** to specify KB, *x* **m** to specify MB, or *x* **g** to specify GB

**Range:** 10 KB through 1 GB

**Default:** 128 KB

**world-readable | no-world-readable**—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option

Copyright © 2013, Juniper Networks, Inc.

enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

**flag** *flag* —Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags.

- **all**—Trace all options
  - **configuration** — Trace configuration events
  - **fpc-ipc**—Trace FPC interprocess communication messages
  - **fpc-ipc-heart-beat**—Trace FPC interprocess heart beat messages
  - **memory**—Trace memory allocation or deallocation messages
  - **ssam**—Trace state synchronization and management events
  - **wx-login**—Trace WXC ISM200 login events

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- WX and WXC Application Acceleration hardware and software documentation


Copyright © 2013, Juniper Networks, Inc.

## traceoptions (Wireless WAN Service)

**Syntax**

```
traceoptions {
  file filename {
    <files number> ;
    <match regular-expression>;
    <size maximum-file-size>;
    <world-readable | no-world-readable>;
  }
  flag flag;
}
```

**Hierarchy Level** [edit *system* processes wireless-wan-service ]

**Release Information** Statement introduced in Release 9.5 of Junos OS.

**Description** Configure tracing operations for Wireless WAN Services.

**Options**

**file** *filename* —By default, the name of the log file that records trace output is the name of the process being traced. Use this option to specify another name.

**files** *number* —(Optional) Specify the maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed to *trace-file* **.0,** then *trace-file.1* , and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

**Range:** 2 through 1000 files

**Default:** 10 files

**match** *regular-expression* —(Optional) Refine the output to include lines that contain the regular expression.

**size** *maximum-file-size* —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file* **.0**. When the **trace-file** again reaches its maximum size, *trace-file* **.0** is renamed *trace-file* **.1** and *trace-file* is renamed *trace-file* **.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

**Syntax:** *x* **k** to specify KB, *x* **m** to specify MB, or *x* **g** to specify GB

**Range:** 10 KB through 1 GB

**Default:** 128 KB

**world-readable | no-world-readable**—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option

Copyright © 2013, Juniper Networks, Inc.

enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

**flag *flag***—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags.

- **all**—Trace all options.
  - **config** —Trace configuration events.
  - **debug** —Trace WAN interface specific debug messages.
  - **fpc-ipc**—Trace FPC inter process communication messages.
  - **memory**—Trace Memory allocation or deallocation messages.
  - **sdk-api**—Trace WAN interface specific library messages.
  - **snmp**—Trace SNMP communication specific debug messages.



NOTE: To monitor trace for CX111 management enable the flag snmp option.

**Required Privilege Level**

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## trusted-keys

**Syntax**

```
trusted-keys {
    key dns-key;
    load-key-file {
    load-key-file;
    }
}
```

**Hierarchy Level** [edit system services dns dnssec]

**Release Information** Statement introduced in Junos OS Release 10.2.

**Description** Configure trusted keys in the DNS server.

**Options** **key *dns-key***—Trusted key

**load-key-file *load-key-file***—Specifies the URL containing the DNS keys.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Security Zones and Interfaces for Security Devices

## wan-acceleration

**Syntax** wan-acceleration (enable | disable);

**Hierarchy Level** [edit system processes]

**Release Information** Statement introduced in Release 8.5 of Junos OS.

**Description** Enable or disable the WXC Integrated Services Module (ISM 200) for WAN acceleration.

**Options** **enable**—Turn on the WXC ISM200.

**disable**—Turn off the WXC ISM200.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- WX and WXC Application Acceleration hardware and software documentation

Copyright © 2013, Juniper Networks, Inc.

## web-management (System Services)

**Syntax**

```
web-management {
  http {
    interfaces interface-names ;
    port port;
  }
  https {
    interfaces interface-names;
    system-generated-certificate name;
    port port;
  }
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced in Release 9.0 of Junos OS.

**Description** Configure settings for HTTP or HTTPS access. HTTP access allows management of the device using the J-Web interface. HTTPS access allows secure management of the device using the J-Web interface. With HTTPS access, communication is encrypted between your browser and the webserver for your device.

**Options** The remaining statements are explained separately.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Security Configuration Guide*


Copyright © 2013, Juniper Networks, Inc.

## zone (System Security Profile)

**Syntax**

```
zone {
  maximum amount;
  reserved amount;
}
```

**Hierarchy Level** [edit system security-profile *security-profile-name*]

**Release Information** Statement introduced in Junos OS Release 11.2.

**Description** Specify the zones that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.
- binds security profiles to user logical systems and the master logical system.
- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

**Options**

- **maximum *amount***—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows, it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.
- **reserved *amount***—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

**Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**

- Security Zones and Interfaces for Security Devices
- Master Administrator for Logical Systems on Security Devices

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 24

# WLAN Hierarchy and Statements

This section contains the following topics:


- WLAN Configuration Statement Hierarchy on page 1297


## WLAN Configuration Statement Hierarchy

Use the statements in the **wlan** configuration hierarchy to configure wireless LAN features on the SRX210, SRX240, or SRX650 Services Gateway running Junos OS.

```
wlan {
  access-point name {
    description description;
    access-point-options {
      country country-code;
      station-mac-filter {
        ( allow-list | deny-list );
        mac-address addr1 addr2;
      }
    }
    external {
      dot1x-supplicant {
        username username;
        password password;
      }
      system {
        console {
          baud-rate ( 9600 | 19200 | 38400 | 57600 | 115200 );
        }
        ntp-server name;
        ports {
          ethernet {
            management-vlan vlan-id;
            name-server {
              ip-address1 ip-address2;
            }
            static {
              address ip-address/mask;
              default-gateway ip-address;
            }
            untagged-vlan vlan-id;
          }
```

Copyright © 2013, Juniper Networks, Inc.

```
    }
  }
}
location location;
logging-options {
  enable-persistent;
  enable-remote;
  log-server-address <ip-address>;
  log-server-port <port-number>;
}
mac-address mac-address;
radio ( 1 | 2 ){
  quality-of-service {
    access-point-queues {
      background-queue {
        arbitration-inter-frame-space slots;
        maximum-burst microseconds;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      }
      best-effort-queue {
        arbitration-inter-frame-space slots;
        maximum-burst microseconds;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      }
      video-queue {
        arbitration-inter-frame-space slots;
        maximum-burst microseconds;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      }
      voice-queue {
        arbitration-inter-frame-space slots;
        maximum-burst microseconds;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      }
    }
    no-acknowledgement;
    no-auto-power-save;
    no-wifi-multimedia;
    station-queues {
      background-queue {
        arbitration-inter-frame-space slots;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
      best-effort-queue {
        arbitration-inter-frame-space slots;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
      video-queue {
```


Copyright © 2013, Juniper Networks, Inc.

```
            arbitration-inter-frame-space slots;
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
          }
          voice-queue {
            arbitration-inter-frame-space slots;
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
          }
        }
      }
      radio-options {
        beacon-interval ms;
        broadcast-multicast-rate-limit {
          rate-limit packets-per-second;
          rate-limit-bursts packets-per-second;
        }
        channel {
          number ( auto | channel-number );
          bandwidth (20 | 40 );
          primary ( lower | upper );
        }
        disable-dot11d;
        dtim-period beacons;
        fixed-multicast-rate ( auto | rate );
        fragmentation-threshold size;
        maximum-stations number;
        mode (2.4GHz | 5GHz | a | an | bg | bgn);
        protection ( auto | off );
        radio-off;
        rts-threshold size;
        space-time-block-coding;
        transmit-power percent;
        transmit-rate-sets {
          supported-rates rate1 rate2 ... rate-n;
          supported-basic-rates rate1 rate2 ... rate-n;
        }
      }
      station-isolation;
      virtual-access-point id {
        description description;
        http-redirect {
          redirect-url url;
        }
        no-broadcast-ssid;
        security {
          dot1x {
            radius-server ip-address;
            radius-key secret-key;
            broadcast-key-refresh-rate minutes;
            session-key-refresh-rate minutes;
          }
          mac-authentication-type ( disabled | local | radius );
          none;
```

```
            static-wep {
              authentication-type (open | shared | both);
              key-length (64bits | 128bits);
              key-type ( ascii | hex );
              transfer-key-index id;
              wep-key-1 key-1;
              wep-key-2 key-2;
              wep-key-3 key-3;
              wep-key-4 key-4;
            }
            wpa-enterprise {
              cipher-suites (tkip | ccmp | both);
              pre-authenticate;
              radius {
                radius-server ip-address;
                radius-key secret-key;
                broadcast-key-refresh-rate minutes;
                session-key-refresh-rate minutes;
              }
              wpa-version (v1 | v2 | both);
            }
            wpa-personal {
              broadcast-key-refresh-rate minutes;
              cipher-suites (tkip | ccmp | both);
              key key;
              wpa-version (v1 | v2 | both);
            }
          }
          ssid ssid;
          vlan vlan-id;
        }
      }
      syslog-options {
        log-size <number>;
        period <number>;
      }
    }
      radio ( 1 | 2 ) {
        radio-options {
          beacon-interval ms;
          broadcast-multicast-rate-limit {
            rate-limit packets-per-second;
            rate-limit-bursts packets-per-second;
          }
          channel {
            number ( auto | channel-number );
            bandwidth (20 MHz | 40 MHz );
            primary-channel ( lower | upper );
          }
          dtim-period beacons;
          fixed-multicast-rate ( auto | rate );
          fragmentation-threshold size;
          max-stations number;
          mode ( a | bg | an | bgn | 5GHz-n | 2.4GHz-n );
          no-short-guard-interval-supported;
          protection ( auto | off );
```


Copyright © 2013, Juniper Networks, Inc.

```
    radio-off;
    rts-threshold size;
    space-time-block-coding;
    transmit-power percent;
    transmit-rate-sets {
      supported-rates rate1 rate2 ... rate-n;
      supported-basic-rates rate1 rate2 ... rate-m;
    }
  }
  quality-of-service {
    access-point-queues {
      background-queue {
        arbitration-inter-frame-space ms;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-burst ms;
      }
      best-effort-queue {
        arbitration-inter-frame-space ms;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-burst ms;
      }
      video-queue {
        arbitration-inter-frame-space ms;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-burst ms;
      }
      voice-queue {
        arbitration-inter-frame-space ms;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-burst ms;
      }
    }
    no-acknowledgement;
    no-auto-power-save;
    no-wifi-multimedia;
    station-queues {
      background-queue {
        arbitration-inter-frame-space ms;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
      best-effort-queue {
        arbitration-inter-frame-space ms;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
      video-queue {
        arbitration-inter-frame-space ms;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
```

```
            transmit-opportunity-limit ms;
        }
        voice-queue {
            arbitration-inter-frame-space ms;
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
        }
    }
}
virtual-access-point id {
    description description;
    http-redirect {
        redirect-url url;
    }
    no-broadcast-ssid;
    security {
        mac-authentication-type ( disabled | local | radius );
        none;
        dot1x {
            radius {
                radius-server ip-address;
                radius-key secret-key;
                broadcast-key-refresh-rate minutes;
                session-key-refresh-rate minutes;
            }
        }
        static-wep {
            authentication-type ( open | shared );
            key-length ( 64-bit | 128-bit );
            key-type ( ascii | hex );
            transfer-key-index id;
            wep-key-1 key-1;
            wep-key-2 key-2;
            wep-key-3 key-3;
            wep-key-4 key-4;
        }
        wpa-enterprise {
            wpa-version ( 1 | 2 | both );
            cipher-suites (tkip | ccmp | both );
            pre-authenticate;
            radius {
                radius-server ip-address;
                radius-key secret-key;
                broadcast-key-refresh-rate minutes;
                session-key-refresh-rate minutes;
            }
        }
        wpa-personal {
            wpa-version ( 1 | 2 | both );
            cipher-suites ( tkip | ccmp | both );
            key key;
            broadcast-key-refresh-rate minutes;
        }
    }
    ssid ssid;
```


Copyright © 2013, Juniper Networks, Inc.

```
            vlan vlan-id;
        }
    }
  }
}
```

**Related Documentation**

- WLAN Configuration and Administration

## access-point

**Syntax**

```
access-point name {
  access-point-options {
    country country-code;
    station-mac-filter {
      ( allow-list | deny-list );
      mac-address addr1 addr2 ... addrn;
    }
  }
  description description;
  external {
    dot1x-supplicant {
      username username;
      password password;
    }
    system {
      console {
        baud-rate ( 9600 | 19200 | 38400 | 57600 | 115200 );
      }
      ntp-server name;
      ports {
        ethernet {
          management-vlan vlan-id;
          name-server {
            ip-address1 ip-address2;
          }
          static {
            address ip-address/mask;
            default-gateway ip-address;
          }
          untagged-vlan vlan-id;
        }
      }
    }
  }
  location location;
  mac-address mac-address;
  radio ( 1 | 2 ){
    quality-of-service {
      access-point-queues {
        background-queue {
          arbitration-inter-frame-space slots;
          minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-burst microseconds;
        }
        best-effort-queue {
          arbitration-inter-frame-space slots;
          minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
          maximum-burst microseconds;
        }
        video-queue {
```


Copyright © 2013, Juniper Networks, Inc.

```
        arbitration-inter-frame-space slots;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-burst microseconds;
      }
      voice-queue {
        arbitration-inter-frame-space slots;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-burst microseconds;
      }
    }
    no-acknowledgement;
    no-auto-power-save;
    no-wifi-multimedia;
    station-queues {
      background-queue {
        arbitration-inter-frame-space slots;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
      best-effort-queue {
        arbitration-inter-frame-space slots;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
      video-queue {
        arbitration-inter-frame-space slots;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
      voice-queue {
        arbitration-inter-frame-space slots;
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
    }
  }
  radio-options {
    beacon-interval ms;
    broadcast-multicast-rate-limit {
      rate-limit packets-per-second;
      rate-limit-bursts packets-per-second;
    }
    channel {
      number ( auto | channel-number );
      bandwidth (20 | 40 );
      primary ( lower | upper );
    }
    disable-dot11d;
    dtim-period beacons;
    fixed-multicast-rate ( auto | rate );
```

```
    fragmentation-threshold size;
    maximum-stations number;
    mode (2.4GHz | 5GHz | a | an | bg | bgn);
    no-short-guard-interval-supported;
    protection ( auto | off );
    radio-off;
    rts-threshold size;
    space-time-block-coding;
    transmit-power percent;
    transmit-rate-sets {
      supported-rates rate1 rate2 ... rate-n;
      supported-basic-rates rate1 rate2 ... rate-n;
    }
  }
  station-isolation;
  virtual-access-point id {
    description description;
    http-redirect {
      redirect-url url;
    }
    no-broadcast-ssid;
    security {
      dot1x {
        radius-server ip-address;
        radius-key secret-key;
        broadcast-key-refresh-rate minutes;
        session-key-refresh-rate minutes;
      }
      mac-authentication-type ( disabled | local | radius );
      none;
      static-wep {
        authentication-type (open | shared | both);
        key-length (64bits | 128bits);
        key-type ( ascii | hex );
        transfer-key-index id;
        wep-key-1 key-1;
        wep-key-2 key-2;
        wep-key-3 key-3;
        wep-key-4 key-4;
      }
      wpa-enterprise {
        cipher-suites (tkip | ccmp | both);
        pre-authenticate;
        radius {
          radius-server ip-address;
          radius-key secret-key;
          broadcast-key-refresh-rate minutes;
          session-key-refresh-rate minutes;
        }
        wpa-version (v1 | v2 | both);
      }
      wpa-personal {
        broadcast-key-refresh-rate minutes;
        cipher-suites (tkip | ccmp | both);
        key key;
        wpa-version (v1 | v2 | both);
```


Copyright © 2013, Juniper Networks, Inc.

```
        }
      }
      ssid ssid;
      vlan vlan-id;
    }
  }
}
```

**Hierarchy Level** [edit wlan]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure WLAN access points.

**Options** **access-point**—Name of the access point. Enter a string of up to 20 characters. The name must start with a letter and end with a letter or a number. Only letters, numbers, and dashes are allowed.

**description**—Descriptive text about the access point.

**location**—Descriptive text about the location of the access point.

**mac-address**—MAC address of the Ethernet port on the access point.



NOTE: **The MAC address uniquely identifies the access point and must be configured before you can change the default configuration of the access point.**

If the access point is connected to the SRX Series device and powered on, the MAC address is displayed with the **show wlan access-points** or **show wlan access-points *ap-name* detail** operational mode commands.

The remaining statements are explained separately.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## access-point-options

**Syntax**

```
access-point-options {
  country country-code;
  station-mac-filter {
    ( allow-list | deny-list );
    mac-address addr1 addr2 ... addrn;
  }
}
```

**Hierarchy Level** [edit wlan access-point *name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure access point options.

**Options** The remaining statements are explained separately.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## access-point-queues

**Syntax**

```
access-point-queues {
  background-queue {
    arbitration-inter-frame-space slots;
    maximum-burst microseconds;
    maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  }
  best-effort-queue {
    arbitration-inter-frame-space slots;
    maximum-burst microseconds;
    maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  }
  video-queue {
    arbitration-inter-frame-space slots;
    maximum-burst microseconds;
    maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  }
  voice-queue {
    arbitration-inter-frame-space slots;
    maximum-burst microseconds;
    maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  }
}
```

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) quality-of-service]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure enhanced distributed channel access (EDCA) parameters for downstream traffic from the access point to the client for the following queues:

**Options** Options can be configured for the following queues:

- **voice-queue**—Highest priority queue with minimum delay.
- **video-queue**—High priority queue with minimum delay.
- **best-effort-queue**—Medium priority queue with medium throughput and delay.
- **background-queue**—Lowest priority queue with high throughput.

The remaining statements are explained separately.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## arbitration-inter-frame-space

**Syntax** arbitration-inter-frame-space *slots*;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) quality-of-service (access-point-queues | station-queues) *queue*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure wait time, in number of slots, for data frames. The length of a slot time is a constant that depends on the physical characteristics of the 802.11 PHY.

**Options** **arbitration-inter-frame-space**—Specify a value from 1 to 255. The defaults are 2 slots for **voice-queue** and **video-queue**, 3 slots for **best-effort-queue**, and 7 slots for **background-queue**.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## background-queue

**Syntax**

For access-point-queues:

```
background-queue {
  arbitration-inter-frame-space slots;
  maximum-burst microseconds;
  maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
}
```

For station-queues:

```
background-queue {
  arbitration-inter-frame-space slots;
  maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  transmit-opportunity-limit ms;
}
```

**Hierarchy Level**

[edit wlan access-point *name* radio (1 | 2) quality-of-service (access-point-queues | station-queues)]

**Release Information**

Statement introduced in Release 10.0 of Junos OS.

**Description**

Configure lowest priority queue with high throughput.

**Options**

The remaining statements are explained separately.

**Required Privilege Level**

wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

## beacon-interval

**Syntax**

beacon-interval *ms*;

**Hierarchy Level**

[edit wlan access-point *name* radio (1 | 2) radio-options]

**Release Information**

Statement introduced in Release 10.0 of Junos OS.

**Description**

Configure interval, in milliseconds, at which the radio transmits beacons.

**Options**

**beacon-interval**—Specify a value from 20 to 2000. The default is 100 milliseconds.

**Required Privilege Level**

wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## best-effort-queue

**Syntax**

For access-point-queues:

```
best-effort-queue {
  arbitration-inter-frame-space slots;
  maximum-burst microseconds;
  maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
}
```

For station-queues:

```
best-effort-queue {
  arbitration-inter-frame-space slots;
  maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  transmit-opportunity-limit ms;
}
```

**Hierarchy Level**

[edit wlan access-point *name* radio (1 | 2) quality-of-service (access-point-queues | station-queues)]

**Release Information**

Statement introduced in Release 10.0 of Junos OS.

**Description**

Configure medium priority queue with medium throughput and delay.

**Options**

The remaining statements are explained separately.

**Required Privilege Level**

wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## broadcast-multicast-rate-limit

**Syntax**

```
broadcast-multicast-rate-limit {
  rate-limit packets-per-second;
  rate-limit-bursts packets-per-second;
}
```

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) radio-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Enable broadcast and multicast rate limiting.

**Options**

**rate-limit**—Packet rate, in packets per second, below which frames are forwarded. Specify a value from 1 to 50. The default is 50 packets per second.

**rate-limit-bursts**—Intermittent packet burst rate, in packets per second, below which frames are forwarded. Specify a value from 1 to 75. The default is 75 packets per second.

**Required Privilege Level**

wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## channel

**Syntax**

```
channel {
  number ( auto | channel-number );
  bandwidth (20 | 40 );
  primary ( lower | upper );
}
```

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) radio-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure channel used for transmitting and receiving.

**Options**

**number**—Specify a valid 802.11a/b/g channel number or **auto**.

**bandwidth** —Channel bandwidth to be used. Specify **20** for the 2.4 GHz band or **40** for the 5 GHz band.

**primary**—In the 40 MHz channel, the relative location of the primary channel. Specify **lower** or **upper**.

**Required Privilege Level**
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

## console (WLAN)

**Syntax**

```
console {
  baud-rate ( 9600 | 19200 | 38400 | 57600 | 115200 );
}
```

**Hierarchy Level** [edit wlan access-point *name* external system]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure serial access on the access point's console port.

**Options**

**console**—Enable serial access on access point's console port. Console port access is disabled by default.

Specify the baud rate for the serial connection: **9600**, **19200**, **38400**, **57600**, or **115200**.

**Required Privilege Level**
wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## country

**Syntax** country *country-code*;

**Hierarchy Level** [edit wlan access-point *name* access-point-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure country of operation for the access point.

**Options** **country**—Two-character code that represents the country of operation for the access point. The following lists supported countries and their country codes:

- Australia—AU
- Austria—AT
- Belgium—BE
- Brazil—BR
- Canada—CA
- China—CN
- Czech Republic—CZ
- Denmark—DK
- Finland—FI
- France—FR
- Germany—DE
- Greece—GR
- Hong Kong—HK
- Hungary—HU
- Iceland—IS
- India—IN
- Ireland—IE
- Israel—IL
- Italy—IT
- Japan—JP
- Liechtenstein—LI
- Luxembourg—LU
- Malaysia—MY
- Mexico—MX

Copyright © 2013, Juniper Networks, Inc.

- Netherlands—NL
- New Zealand—NZ
- Norway—NO
- Poland—PL
- Portugal—PT
- Saudi Arabia—SA
- Singapore—SG
- Slovakia—SK
- Slovenia—SI
- South Africa—ZA
- South Korea—KR
- Spain—ES
- Sweden—SE
- Switzerland—CH
- Taiwan—TW
- Thailand—TH
- United Arab Emirates—AE
- United Kingdom—GB
- United States—US

**Required Privilege Level**

wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## disable-dot11d

**Syntax** disable-dot11d;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) radio-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** (Optional) For radios operating in the 2.4 GHz band, suppress the country code setting from being broadcast in beacons.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

## dot1x (WLAN)

**Syntax**
```
dot1x {
  radius-server ip-address;
  radius-key secret-key;
  broadcast-key-refresh-rate minutes;
  session-key-refresh-rate minutes;
}
```

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id* security]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure 802.1x (also known as dynamic WEP) for generation and distribution of keys.

**Options**

**radius-server**—IP address of the RADIUS server. The default IP address is **192.168.1.10**.

**radius-key**—Key used by the RADIUS server, in the form of a string of up to 64 bytes. The default key is **secret**.

**broadcast-key-refresh-rate**—Interval, in minutes, between key rotations. Specify a value from 1 to 86400. The default is 0 (disabled).

**session-key-refresh-rate**—Interval, in minutes, between session key rotations. Specify a value from 1 to 86400. The default is 0 (disabled).

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## dot1x-supplicant

**Syntax**

```
dot1x-supplicant {
  username username;
  password password;
}
```

**Hierarchy Level** [edit wlan access-point *name* external]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure 802.1x supplicant information for access point.

**Options** **dot1x-supplicant**—Configure username and password for 802.1x supplicant authentication:

- **username**—User identification. Specify a string of up to 64 bytes. ASCII printable characters are allowed, which includes upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.
- **password**—Password. Specify a string of up to 64 bytes. ASCII printable characters are allowed, which includes upper and lower case alphabetic letters, numeric digits, and special symbols such as @ and #.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

## dtim-period

**Syntax** dtim-period *beacons*;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) radio-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure interval, in number of radio beacons transmitted, at which clients in power-save mode check for buffered data from the radio.

**Options** **dtim-period**—Specify a value from 1 to 255. The default is 2 beacons.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## ethernet (WLAN)

**Syntax**

```
ethernet {
  management-vlan vlan-id;
  name-server {
    ip-address1 ip-address2;
  }
  static {
    address ip-address/mask;
    default-gateway ip-address;
  }
  untagged-vlan vlan-id;
}
```

**Hierarchy Level** [edit wlan access-point *name* external system ports]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure Ethernet port on the access point.

**Options** The remaining statements are explained separately.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## external

**Syntax**

```
external {
  dot1x-supplicant {
    username username;
    password password;
  }
  system {
    console {
      baud-rate ( 9600 | 19200 | 38400 | 57600 | 115200 );
    }
    ntp-server name;
    ports {
      ethernet {
        management-vlan vlan-id;
        name-server {
          ip-address1 ip-address2;
        }
        static {
          address ip-address/mask;
          default-gateway ip-address;
        }
        untagged-vlan vlan-id;
      }
    }
  }
}
```

**Hierarchy Level** [edit wlan access-point *name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure access point network options.

**Options** The remaining statements are explained separately.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## fixed-multicast-rate

**Syntax** fixed-multicast-rate ( auto | *rate* );

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) radio-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure multicast/broadcast transmission rate.

**Options** **fixed-multicast-rate**—Specify either a specified speed or **auto**. The default is **auto**.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

## fragmentation-threshold

**Syntax** fragmentation-threshold *size*;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) radio-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure size at which a frame is divided into multiple 802.11 frames.

**Options** **fragmentation-threshold**—Specify an even number from **256** to **2346**. The default is **2346**.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## http-redirect

**Syntax**

```
http-redirect {
  redirect-url url;
}
```

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure HTTP redirection for a virtual access point.

**Options** **redirect-url *url***—Redirect the user's first HTTP access to a specified webpage. This option is commonly used for Wi-Fi hotspots.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## logging-options

**Syntax**

```
logging-options {
  enable-persistent;
  enable-remote;
  log-server-address <ip-address>;
  log-server-port <port-number>;
}
```

**Hierarchy Level** [edit wlan access-point *name*]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Configure access point logging options.

**Options**

- ***enable-persistent***—Specifies that an Access Point stores all persistent log events to internal flash memory and remote server or services gateway periodically fetches these system log messages files from all the Access Points.
- ***enable-persistent***—Specifies that system log messages files are not stored on internal flash and will be sent to remote log server directly.
- ***log-server-address***—Specifies the IP address of the remote log server.
- ***log-server-port***—Specifies the port of the remote log server.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## mac-authentication-type

**Syntax** mac-authentication-type ( disabled | local | radius );

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id* security]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Enable or disable client authentication using the client's MAC address.

**Options**

**disable**—No MAC authentication is performed. This is the default.

**local**—The client's MAC address is looked up on a list of configured MAC addresses. Use the **station-mac-filter** configuration statement to configure the MAC addresses that are allowed or denied access.

**radius**—The client's MAC address is authenticated with a RADIUS server.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

## management-vlan

**Syntax** management-vlan *vlan-id*;

**Hierarchy Level** [edit wlan access-point *name* external system ports ethernet]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure VLAN for management traffic for access point.

**Options**

**management-vlan**—Identifier for VLAN for management traffic. Specify a value from 1 to 4094. The default is 1.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## maximum-stations

**Syntax** maximum-stations *number*;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) radio-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure maximum number of associations the radio can support.

**Options** **maximum-stations**—Specify a value from 0 to 200. The default is 200.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

## maximum-burst

**Syntax** maximum-burst *microseconds*;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) quality-of-service access-point-queues *queue*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure maximum length, in microseconds, allowed for packet bursts on the wireless network. (A packet burst is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance.)

**Options** **maximum-burst**—Specify a value from 0 to 999900. The defaults are 1500 microseconds for **voice-queue**, 3000 microseconds for **video-queue**, and 0 microseconds for **best-effort-queue** and **background-queue**.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## maximum-contention-window

**Syntax** maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) quality-of-service (access-point-queues | station-queues) *queue*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure upper limit, in slots, for the doubling of the random back-off time; doubling of the random back-off time continues until either the data frame is sent or this value is reached.

**Options** **maximum-contention-window**—Specify one of the following values: 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. The defaults are 7 slots for **voice-queue**, 15 slots for **video-queue**, 63 slots for **best-effort-queue**, and 1023 slots for **background-queue**.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

## minimum-contention-window

**Syntax** minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) quality-of-service (access-point-queues | station-queues) *queue*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure upper limit, in slots, of a range from which the initial random back-off wait time is determined. The first random number generated will be a number between 0 and the value specified. If the first random back-off wait time expires before the data frame is sent, a retry counter is incremented and the random back-off value is doubled. Doubling continues until the size of the random back-off values reaches the value defined in **maximum-contention-window**.

**Options** **minimum-contention-window**—Specify one of the following values: 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. The defaults are 3 slots for **voice-queue**, 7 slots for **video-queue**, and 15 slots for **best-effort-queue** and **background-queue**.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## mode (WLAN)

**Syntax** mode (2.4GHz | 5GHz | a | an | bg | bgn);

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) radio-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Set Physical Layer (PHY) standard mode of the radio.

**Options** **mode**—Default for radio 1 is 802.11b/g/n; default for radio 2 is 802.11a/n. Select one of the following values:

- **2.4GHz**—2.4 GHz 802.11n
- **5GHz**—5 GHz 802.11n
- **a**—802.11a
- **an**—802.11a/n
- **bg**—802.11b/g
- **bgn**—802.11b/g/n

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

## name-server (WLAN)

**Syntax**
```
name-server {
  ip-address;
}
```

**Hierarchy Level** [edit wlan access-point *name* external system ports ethernet]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure DNS server for access point.

**Options** **name-server**— IP address of Domain Name System (DNS) server.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## no-acknowledgement

**Syntax** no-acknowledgement;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) quality-of-service]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Suppress sending of acknowledgments (acks) by the access point when a frame is correctly received, per IEEE 802.11e standard.

NOTE: This configuration statement has no effect if Wi-Fi Multimedia (WMM) is disabled.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

## no-auto-power-save

**Syntax** no-auto-power-save;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) quality-of-service]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Disable Automatic Power Save Delivery (APSD), per IEEE 802.11e standard. APSD is recommended if VoIP phones access the network through the access point.

NOTE: Disabling or enabling APSD has no effect if Wi-Fi Multimedia (WMM) is disabled.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## no-broadcast-ssid

**Syntax** no-broadcast-ssid;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Disable access point responses to client broadcast probes.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

## no-short-guard-interval-supported

**Syntax** no-short-guard-interval-supported;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) radio-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Disable 802.11n Short Inter-Symbol Guard Interval.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

## no-wifi-multimedia

**Syntax** no-wifi-multimedia;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) quality-of-service]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Disable Wi-Fi MultiMedia (WMM). Disabling WMM deactivates QoS control of parameters on traffic from the client to the access point. With WMM disabled, you can still set some parameters on traffic from the access point to the client.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## ntp-server

**Syntax** ntp-server *name*;

**Hierarchy Level** [edit wlan access-point *name* external system]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure Network Time Protocol (NTP) server for access point.

**Options** **ntp-server**—NTP server name.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

## protection

**Syntax** protection ( auto | off );

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) radio-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Enable or disable protection mechanisms to prevent interference with legacy client and access points from 802.11n or 802.11g transmissions.

**Options** **protection** —Specify **auto** or **off**. The default is **auto**.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## quality-of-service

**Syntax**

```
quality-of-service {
  access-point-queues {
    background-queue {
      arbitration-inter-frame-space slots;
      maximum-burst microseconds;
      maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    }
    best-effort-queue {
      arbitration-inter-frame-space slots;
      maximum-burst microseconds;
      maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    }
    video-queue {
      arbitration-inter-frame-space slots;
      maximum-burst microseconds;
      maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    }
    voice-queue {
      arbitration-inter-frame-space slots;
      maximum-burst microseconds;
      maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    }
  }
  no-acknowledgement;
  no-auto-power-save;
  no-wifi-multimedia;
  station-queues {
    background-queue {
      arbitration-inter-frame-space slots;
      maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      transmit-opportunity-limit ms;
    }
    best-effort-queue {
      arbitration-inter-frame-space slots;
      maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      transmit-opportunity-limit ms;
    }
    video-queue {
      arbitration-inter-frame-space slots;
      maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      transmit-opportunity-limit ms;
    }
    voice-queue {
      arbitration-inter-frame-space slots;
      maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
```

Copyright © 2013, Juniper Networks, Inc.

```
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
        }
    }
}
```

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) ]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure quality of service (QoS) for the radio.

**Options** The remaining statements are explained separately.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## radio (WLAN)

**Syntax**

```
radio ( 1 | 2 ){
  quality-of-service {
    access-point-queues {
      background-queue {
        arbitration-inter-frame-space slots;
        maximum-burst microseconds;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      }
      best-effort-queue {
        arbitration-inter-frame-space slots;
        maximum-burst microseconds;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      }
      video-queue {
        arbitration-inter-frame-space slots;
        maximum-burst microseconds;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      }
      voice-queue {
        arbitration-inter-frame-space slots;
        maximum-burst microseconds;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
      }
    }
    no-acknowledgement;
    no-auto-power-save;
    no-wifi-multimedia;
    station-queues {
      background-queue {
        arbitration-inter-frame-space slots;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
      best-effort-queue {
        arbitration-inter-frame-space slots;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
      video-queue {
        arbitration-inter-frame-space slots;
        maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
        transmit-opportunity-limit ms;
      }
      voice-queue {
        arbitration-inter-frame-space slots;
```

Copyright © 2013, Juniper Networks, Inc.

```
            maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
            transmit-opportunity-limit ms;
        }
    }
}
radio-options {
    beacon-interval ms;
    broadcast-multicast-rate-limit {
        rate-limit packets-per-second;
        rate-limit-bursts packets-per-second;
    }
    channel {
        number ( auto | channel-number );
        bandwidth (20 | 40 );
        primary ( lower | upper );
    }
    disable-dot11d;
    dtim-period beacons;
    fixed-multicast-rate ( auto | rate );
    fragmentation-threshold size;
    maximum-stations number;
    mode (2.4GHz | 5GHz | a | an | bg | bgn);
    no-short-guard-interval-supported;
    protection ( auto | off );
    radio-off;
    rts-threshold size;
    space-time-block-coding;
    transmit-power percent;
    transmit-rate-sets {
        supported-rates rate1 rate2 ... rate-n;
        supported-basic-rates rate1 rate2 ... rate-n;
    }
}
station-isolation;
virtual-access-point id {
    description description;
    http-redirect {
        redirect-url url;
    }
    no-broadcast-ssid;
    security {
        dot1x {
            radius-server ip-address;
            radius-key secret-key;
            broadcast-key-refresh-rate minutes;
            session-key-refresh-rate minutes;
        }
        mac-authentication-type ( disabled | local | radius );
        none;
        static-wep {
            authentication-type (open | shared | both);
            key-length (64bits | 128bits);
            key-type ( ascii | hex );
            transfer-key-index id;
            wep-key-1 key-1;
```


Copyright © 2013, Juniper Networks, Inc.

```
        wep-key-2 key-2;
        wep-key-3 key-3;
        wep-key-4 key-4;
      }
      wpa-enterprise {
        cipher-suites (tkip | ccmp | both);
        pre-authenticate;
        radius {
          radius-server ip-address;
          radius-key secret-key;
          broadcast-key-refresh-rate minutes;
          session-key-refresh-rate minutes;
        }
        wpa-version (v1 | v2 | both);
      }
      wpa-personal {
        broadcast-key-refresh-rate minutes;
        cipher-suites (tkip | ccmp | both);
        key key;
        wpa-version (v1 | v2 | both);
      }
    }
    ssid ssid;
    vlan vlan-id;
  }
}
```

**Hierarchy Level** [edit wlan access-point *name*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure radio 1 or radio 2 on the access point.

**Options** The remaining statements are explained separately.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## radio-off

**Syntax** radio-off;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) radio-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Set operational state of radio to off.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## radio-options

**Syntax**

```
radio-options {
  beacon-interval ms;
  broadcast-multicast-rate-limit {
    rate-limit packets-per-second;
    rate-limit-bursts packets-per-second;
  }
  channel {
    number ( auto | channel-number );
    bandwidth (20 | 40 );
    primary ( lower | upper );
  }
  disable-dot11d;
  dtim-period beacons;
  fixed-multicast-rate ( auto | rate );
  fragmentation-threshold size;
  maximum-stations number;
  mode (2.4GHz | 5GHz | a | an | bg | bgn);
  no-short-guard-interval-supported;
  protection ( auto | off );
  radio-off;
  rts-threshold size;
  space-time-block-coding;
  transmit-power percent;
  transmit-rate-sets {
    supported-rates rate1 rate2 ... rate-n;
    supported-basic-rates rate1 rate2 ... rate-n;
  }
}
```

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) ]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure access point radio.

**Options** The remaining statements are explained separately.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## rts-threshold

**Syntax** rts-threshold *size*;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) radio-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure size of a request to send (RTS) transmission packet.

**Options** **rts-threshold**—Specify a value from 0 to 2347. The default is 2347.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## security (WLAN)

**Syntax**

```
security {
  dot1x {
    radius-server ip-address;
    radius-key secret-key;
    broadcast-key-refresh-rate minutes;
    session-key-refresh-rate minutes;
  }
  mac-authentication-type ( disabled | local | radius );
  none;
  static-wep {
    authentication-type (open | shared | both);
    key-length (64bits | 128bits);
    key-type ( ascii | hex );
    transfer-key-index id;
    wep-key-1 key-1;
    wep-key-2 key-2;
    wep-key-3 key-3;
    wep-key-4 key-4;
  }
  wpa-enterprise {
    cipher-suites (tkip | ccmp | both);
    pre-authenticate;
    radius {
      radius-server ip-address;
      radius-key secret-key;
      broadcast-key-refresh-rate minutes;
      session-key-refresh-rate minutes;
    }
    wpa-version (v1 | v2 | both);
  }
  wpa-personal {
    broadcast-key-refresh-rate minutes;
    cipher-suites (tkip | ccmp | both);
    key key;
    wpa-version (v1 | v2 | both);
  }
}
```

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure security for the virtual access point.

**Options** The remaining statements are explained separately.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## space-time-block-coding

**Syntax** space-time-block-coding;

**Hierarchy Level** [edit wlan access-point *name* radio-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Enable 802.11n Space Time Block Coding (STBC).

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

## ssid

**Syntax** ssid *ssid*;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure Service Set Identifier (SSID) broadcast by the access point.

**Options** ssid *id*—String of up to 32 characters.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## static (WLAN)

**Syntax**

```
static {
  address ip-address/mask;
  default-gateway ip-address;
}
```

**Hierarchy Level** [edit wlan access-point *name* external system ports ethernet]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure static IP address information for the access point.

**Options**

**address**—IP address and netmask for the access point.

**default-gateway**—IP address of the default gateway.

**Required Privilege Level**

wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## static-wep

**Syntax**

```
static-wep {
  authentication-type (open | shared | both);
  key-length (64bits | 128bits);
  key-type ( ascii | hex );
  transfer-key-index id;
  wep-key-1 key-1;
  wep-key-2 key-2;
  wep-key-3 key-3;
  wep-key-4 key-4;
}
```

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id* security]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure a preshared Wired Equivalent Privacy (WEP) key.

**Options**

**authentication-type**—Specify **open** to allow any client to associate with the access point; clients must have the correct WEP key to transmit and received encrypted data. Specify **shared** to permit only clients with the correct WEP key to associate with the access point. Specify **both** to allow both open and shared authentication.

**static wep**—Configure a preshared Wired Equivalent Privacy (WEP) key.

**key-length**—Length, in bits, of WEP key. Specify **64bits** for 64 bits or **128bits** for 128 bits. The default is 64 bits.

**key-type**—Format of the WEP key. Specify either **ascii** for ASCII format or **hex** for hexadecimal format. The default is ASCII.

**transfer-key-index**—Allow configuration of up to four preshared keys. Specify a value from 1 to 4.

**wep-key-1** through **wep-key-4**—Preshared key string that corresponds to the **transfer-key-index** value.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## station-isolation

**Syntax** station-isolation;

**Hierarchy Level** [edit wlan access-point *access-point-name* radio (1|2)]

**Release Information** Statement introduced in Release 10.3 of Junos OS.

**Description** Isolate the clients connected to the same virtual access point within a radio.

**Required Privilege Level** security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

## station-mac-filter

**Syntax**
```
station-mac-filter {
   ( allow-list | deny-list );
   mac-address addr1 addr2 ... addrn;
}
```

**Hierarchy Level** [edit wlan access-point *name* access-point-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure list of client MAC addresses for local authentication.

**Options** **allow-list**—List of allowed MAC addresses.

**deny-list**—List of denied MAC addresses.

**mac-address**—Client MAC address.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## station-queues

**Syntax**

```
station-queues {
  background-queue {
    arbitration-inter-frame-space slots;
    maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    transmit-opportunity-limit ms;
  }
  best-effort-queue {
    arbitration-inter-frame-space slots;
    maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    transmit-opportunity-limit ms;
  }
  video-queue {
    arbitration-inter-frame-space slots;
    maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    transmit-opportunity-limit ms;
  }
  voice-queue {
    arbitration-inter-frame-space slots;
    maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
    transmit-opportunity-limit ms;
  }
}
```

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) quality-of-service]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure enhanced distributed channel access (EDCA) parameters for upstream traffic from the client to the access point.

**Options** Options can be configured for the following queues:

- **voice-queue**—Highest priority queue with minimum delay.
- **video-queue**—High priority queue with minimum delay.
- **best-effort-queue**—Medium priority queue with medium throughput and delay.
- **background-queue**—Lowest priority queue with high throughput.

The remaining statements are explained separately.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## syslog-options

**Syntax**

```
syslog-options {
  log-size <number>;
  period <number>;
}
```

**Hierarchy Level** [edit wlan access-point *name*]

**Release Information** Statement introduced in Release 11.1 of Junos OS.

**Description** Configure access point logging options.

**Options**

- ***log-size***—Maximum size of each system log file that can be stored on an access point. Range: 4 to 1024 kilobytes.
- ***period***—Specifies the interval, in seconds, between retrieving and storing syslog messages on SRX Series device. Range: 60 through 86,400 seconds.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

## transmit-opportunity-limit

**Syntax** transmit-opportunity-limit *ms*;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) quality-of-service station-queues *queue*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure interval, in milliseconds, when a WMM client can initiate transmissions onto the wireless network.

**Options** **transmit-opportunity-limit**—Specify a value from 0 through 65,535. The defaults are 47 ms for **voice-queue**, 94 ms for **video-queue**, and 0 ms for **best-effort-queue** and **background-queue**.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## transmit-power

**Syntax** transmit-power *percent*;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) radio-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure percent of radio transmit power.

**Options** Specify a value from 0 to 100. The default is 100.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

## transmit-rate-sets

**Syntax**
```
transmit-rate-sets {
  supported-rates rate1 rate2 ... rate-n;
  supported-basic-rates rate1 rate2 ... rate-n;
}
```

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) radio-options]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Specify the transmission rates supported by and advertised by the radio. Valid rates are determined by the radio's **mode** setting.

**Options** **supported-rates**—Transmission rates supported by the radio.

**supported-basic-rates**—Transmission rates advertised by the radio.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## untagged-vlan

**Syntax** untagged-vlan *vlan-id*;

**Hierarchy Level** [edit wlan access-point *name* external system ports ethernet]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure VLAN for untagged traffic for the access point.

**Options** **untagged-vlan**—Identifier for VLAN to which untagged traffic is assigned. Specify a value from 1 to 4094. The default is 1.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## video-queue

**Syntax**

For access-point-queues:

```
video-queue {
  arbitration-inter-frame-space slots;
  maximum-burst microseconds;
  maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
}
```

For station-queues:

```
video-queue {
  arbitration-inter-frame-space slots;
  maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  transmit-opportunity-limit ms;
}
```

**Hierarchy Level**

[edit wlan access-point *name* radio (1 | 2) quality-of-service (access-point-queues | station-queues)]

**Release Information**

Statement introduced in Release 10.0 of Junos OS.

**Description**

Configure high priority queue with minimum delay.

**Options**

The remaining statements are explained separately.

**Required Privilege Level**

wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## virtual-access-point

**Syntax**

```
virtual-access-point id {
  description description;
  http-redirect {
    redirect-url url;
  }
  no-broadcast-ssid;
  security {
    dot1x {
      radius-server ip-address;
      radius-key secret-key;
      broadcast-key-refresh-rate minutes;
      session-key-refresh-rate minutes;
    }
    mac-authentication-type ( disabled | local | radius );
    none;
    static-wep {
      authentication-type (open | shared | both);
      key-length (64bits | 128bits);
      key-type ( ascii | hex );
      transfer-key-index id;
      wep-key-1 key-1;
      wep-key-2 key-2;
      wep-key-3 key-3;
      wep-key-4 key-4;
    }
    wpa-enterprise {
      cipher-suites (tkip | ccmp | both);
      pre-authenticate;
      radius {
        radius-server ip-address;
        radius-key secret-key;
        broadcast-key-refresh-rate minutes;
        session-key-refresh-rate minutes;
      }
      wpa-version (v1 | v2 | both);
    }
    wpa-personal {
      broadcast-key-refresh-rate minutes;
      cipher-suites (tkip | ccmp | both);
      key key;
      wpa-version (v1 | v2 | both);
    }
  }
  ssid ssid;
  vlan vlan-id;
}
```

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) ]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure virtual access point for an access point radio.

Copyright © 2013, Juniper Networks, Inc.

**Options** **virtual-access-point *id***—Virtual access point identifier. Specify an identifier from 0 through 15.



NOTE: VAP 0 is the physical radio interface. VAP 0 is assigned to the BSSID of the physical radio interface.



NOTE: VAP 0 is always enabled. To disable VAP 0, the radio itself must be disabled.

**description**—Description of the virtual access point.

The remaining statements are explained separately.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration

## vlan (WLAN)

**Syntax** vlan *vlan-id*;

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id*]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure the VLAN associated with the virtual access point.

**Options** **vlan *vlan-id***—Specify a VLAN ID from 1 to 4094; however, for SRX240 and SRX650 devices, only VLANs up to 3967 are allowed. The default is 1.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**
- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## voice-queue

**Syntax**

For access-point-queues:

```
voice-queue {
  arbitration-inter-frame-space slots;
  maximum-burst microseconds;
  maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
}
```

For station-queues:

```
voice-queue {
  arbitration-inter-frame-space slots;
  maximum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  minimum-contention-window (1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023);
  transmit-opportunity-limit ms;
}
```

**Hierarchy Level**

[edit wlan access-point *name* radio (1 | 2) quality-of-service (access-point-queues | station-queues)]

**Release Information**

Statement introduced in Release 10.0 of Junos OS.

**Description**

Configure highest priority queue with minimum delay.

**Options**

The remaining statements are explained separately.

**Required Privilege Level**

wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

## wpa-enterprise

**Syntax**

```
wpa-enterprise {
  cipher-suites (tkip | ccmp | both);
  pre-authenticate;
  radius {
    radius-server ip-address;
    radius-key secret-key;
    broadcast-key-refresh-rate minutes;
    session-key-refresh-rate minutes;
  }
  wpa-version (v1 | v2 | both);
}
```

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id* security]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure RADIUS authentication with TKIP and/or CCMP encryption.

**Options**

**cipher-suites**—Encryption type. Specify **tkip**, **ccmp**, or **both**.

**pre-authenticate**—Enable 802.11i pre-authentication.

**radius-server**—IP address of the RADIUS server. The default IP address is **192.168.1.10**.

**radius-key**—Key used by the RADIUS server, in the form of a string of up to 64 bytes. The default key is **secret**.

**broadcast-key-refresh-rate**—Interval, in minutes, between key rotations. Specify a value from 1 to 86400. The default is 0 (disabled).

**session-key-refresh-rate**—Interval, in minutes between session key rotations. Specify a value from 1 to 86400. The default is 0 (disabled).

**wpa-version**—WPA version. Specify **v1**, **v2**, or **both**.

**Required Privilege Level** wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration


Copyright © 2013, Juniper Networks, Inc.

## wpa-personal

**Syntax**

```
wpa-personal {
  broadcast-key-refresh-rate minutes;
  cipher-suites ( tkip | ccmp | both );
  key key;
  wpa-version (v1 | v2 | both);
}
```

**Hierarchy Level** [edit wlan access-point *name* radio (1 | 2) virtual-access-point *id* security]

**Release Information** Statement introduced in Release 10.0 of Junos OS.

**Description** Configure preshared key with Wi-Fi Protected Access (WPA) with Temporal Key Integrity Protocol (TKIP) and/or Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption.

**Options**

**broadcast-key-refresh-rate**—Interval, in minutes, between key rotations. Specify a value from 1 to 86400. The default is 0 (disabled).

**cipher-suites**—Encryption type. Specify **tkip**, **ccmp**, or **both**.

**key**—Preshared key.

**wpa-version**—WPA version. Specify **v1**, **v2**, or **both**.

**Required Privilege Level**

wlan—To view this statement in the configuration.
wlan-control—To add this statement to the configuration.

**Related Documentation**

- WLAN Configuration and Administration

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

PART 2

# Operational Commands


- Clear Commands on page 1357
- Request Commands on page 1487
- Restart Commands on page 1563
- Show Commands on page 1567


Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 25

# Clear Commands

This section contains the following topics:


- Clear Commands Overview on page 1357


## Clear Commands Overview

Use the **clear** configuration commands to clear information about the following features and protocols: Address Resolution Protocol(ARP), auto-configuration, Bidirectional Forwarding Detection (BFD), Border Gateway Protocol (BGP), chassis, 802.1X, End System-to-Intermediate System (ES-IS), Ethernet switching, firewall counters, Generic VLAN Registration Protocol (gvrp), port-forwarding helper, Internet Group Management Protocol (IGMP), IGMP snooping, interfaces, IP version 6 (IPv6), Integrated Services Digital Network (ISDN), Intermediate System-to-Intermediate System (IS-IS), Link Aggregation Control Protocol (LACP), Label Distribution Protocol (LDP), Link Layer Discovery Protocol (LLDP), log file contents, Multicast Listener Discovery, mobile IP, Multiprotocol Label Switching (MPLS), Multicast Source Discovery Protocol (MSDP), multicast, network access, Open Shortest Path First (OSPF), Open Shortest Path First version 3 (OSPFv3), passive monitoring statistics, Packet Forwarding Engine (PFE), Pragmatic Generalized Multicast (PGM), Protocol Independent Multicast (PIM), Point-to-Point Protocol (PPP), Point-to-Point Protocol over Ethernet (PPPoE), Routing Information Protocol (RIP), Routing Information Protocol for IPv6 (RIPng), Resource Reservation Protocol (RSVP), security, services, Simple Network Management Protocol (SNMP), Spanning Tree Protocol, system, Virtual Private LAN Service (VPLS), and Virtual Router Redundancy Protocol.

**Related Documentation**

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*.
- Junos OS Operational Mode Commands.

Copyright © 2013, Juniper Networks, Inc.

## clear chassis cluster control-plane statistics

**Syntax** **clear chassis cluster control-plane statistics**

**Release Information** Command introduced in Release 9.3 of Junos OS.

**Description** Clear the control plane statistics of a chassis cluster.

**Required Privilege Level** clear

**Related Documentation**
- Chassis Cluster for Security Devices
- show chassis cluster control-plane statistics on page 1578

**List of Sample Output** clear chassis cluster control-plane statistics on page 1358

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear chassis cluster control-plane statistics

```
user@host> clear chassis cluster control-plane statistics
Cleared control-plane statistics
```


Copyright © 2013, Juniper Networks, Inc.

## clear chassis cluster data-plane statistics

**Syntax** **clear chassis cluster data-plane statistics**

**Release Information** Command introduced in Release 9.3 of Junos OS.

**Description** Clear the data plane statistics of a chassis cluster.

**Required Privilege Level** clear

**Related Documentation**
- Chassis Cluster for Security Devices
- show chassis cluster data-plane statistics on page 1581

**List of Sample Output** clear chassis cluster data-plane statistics on page 1359

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear chassis cluster data-plane statistics

```
user@host> clear chassis cluster data-plane statistics
Cleared data-plane statistics
```

## clear chassis cluster failover-count

**Syntax** **clear chassis cluster failover-count**

**Release Information** Command introduced in Release 9.3 of Junos OS.

**Description** Clear the failover count of all redundancy-groups.

**Required Privilege Level** clear

**Related Documentation**

- Chassis Cluster for Security Devices
- request chassis cluster failover node on page 1488
- request chassis cluster failover reset on page 1489
- show chassis cluster status on page 1598

**List of Sample Output**

show chassis cluster status on page 1361
clear chassis cluster failover-count on page 1361
show chassis cluster status on page 1361

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

The following example displays the redundancy groups before and after the failover-counts are cleared.


Copyright © 2013, Juniper Networks, Inc.

show chassis cluster status

```
user@host> show chassis cluster status

Cluster ID: 3
Node name         Priority     Status     Preempt  Manual failover

Redundancy group: 0 , Failover count: 1
   node0            200        secondary   no        no
   node1            100        primary     no        no

Redundancy group: 1 , Failover count: 2
   node0            100        primary     no        no
   node1            10         secondary   no        no
```

clear chassis cluster failover-count

```
user@host> clear chassis cluster failover-count
Cleared failover-count for all redundancy-groups
```

show chassis cluster status

```
user@host> show chassis cluster status

Cluster ID: 3
Node name        Priority   Status     Preempt  Manual failover

Redundancy group: 0 , Failover count: 0
  node0           200       secondary    no       no
  node1           100       primary      no       no

Redundancy group: 1 , Failover count: 0
  node0           100       primary      no       no
  node1           10        secondary    no       no
```

Copyright © 2013, Juniper Networks, Inc.

## clear chassis cluster ip-monitoring failure-count

**Syntax** clear chassis cluster ip-monitoring failure-count

**Release Information** Command introduced in Release 10.1 of Junos OS.

**Description** Clear the failure count for all IP addresses.

**Required Privilege Level** clear

**Related Documentation**
- IP Monitoring
- Chassis Cluster for Security Devices
- clear chassis cluster failover-count on page 1360

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

```
user@host> clear chassis cluster ip-monitoring failure-count
node0:
--------------------------------------------------------------------------
Cleared failure count for all IPs

node1:
--------------------------------------------------------------------------
Cleared failure count for all IPs
```


Copyright © 2013, Juniper Networks, Inc.

## clear chassis cluster ip-monitoring failure-count ip-address

**Syntax** clear chassis cluster ip-monitoring failure-count ip-address 1.1.1.1

**Release Information** Command introduced in Release 10.1 of Junos OS.

**Description** Clear the failure count for a specified IP address.



NOTE: Entering an IP address at the end of this command is optional. If you do not specify an IP address, the failure count for all monitored IP addresses is cleared.

**Required Privilege Level** clear

**Related Documentation**

- IP Monitoring
- Chassis Cluster for Security Devices
- clear chassis cluster failover-count on page 1360

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

```
user@host> clear chassis cluster ip-monitoring failure-count ip-address 1.1.1.1
node0:
--------------------------------------------------------------------------
Cleared failure count for IP: 1.1.1.1

node1:
--------------------------------------------------------------------------
Cleared failure count for IP: 1.1.1.1
```

Copyright © 2013, Juniper Networks, Inc.

## clear chassis cluster statistics

**Syntax** **clear chassis cluster statistics**

**Release Information** Command introduced in Release 9.3 of Junos OS.

**Description** Clear the control plane and data plane statistics of a chassis cluster.

**Required Privilege Level** clear

**Related Documentation**
- Chassis Cluster for Security Devices
- show chassis cluster statistics on page 1593

**List of Sample Output** clear chassis cluster statistics on page 1364

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear chassis cluster statistics

```
user@host> clear chassis cluster statistics
Cleared control-plane statistics
Cleared data-plane statistics
```


Copyright © 2013, Juniper Networks, Inc.

## clear dhcp client binding

**Syntax**

clear dhcp client binding
[all|interface <interface-name>]
[routing-instance <routing-instance-name>]

**Release Information**

Statement introduced in Junos OS Release 12.1X44-D10.

**Description**

Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the DHCP client table.

**Options**

**all**—(Optional) Clear the binding state for all DHCP clients.

**interface <interface-name>**—(Optional) Clear the binding state for DHCP clients on the specified interface.

**routing-instance <routing-instance-name>**—(Optional) Clear the binding state for DHCP clients on the specified routing instance. If you do not specify a routing instance, binding state is cleared for DHCP clients on the default routing instance.

**Required Privilege Level**

clear

**Related Documentation**

- show dhcp client binding on page 1628
- Device Configuration

**Output Fields**

This command produces no output.

Copyright © 2013, Juniper Networks, Inc.

## clear dhcp client statistics

**Syntax**

clear dhcp client statistics
<all>
<interface>
<routing-instance>

**Release Information**

Statement introduced in Junos OS Release 12.1X44-D10.

**Description**

Clear all Dynamic Host Configuration Protocol (DHCP) client statistics.

**Options**

**all**—(Optional) Clear all the DHCP client statistics.

**interface**—(Optional) Clear the statistics for DHCP clients on the specified interface.

**routing-instance**—(Optional) Clear the statistics for DHCP clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

**Required Privilege Level**

clear

**Related Documentation**

- show dhcp client statistics on page 1631
- Device Configuration

**Output Fields**

This command produces no output.


Copyright © 2013, Juniper Networks, Inc.

## clear dhcp relay binding

**Syntax**

clear dhcp relay binding
<all | ip-address | mac-address>
<interface interface-name>
<routing-instance routing-instance-name>

**Release Information**

Statement introduced in Junos OS Release 12.1X44-D10.

**Description**

Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table.

**Options**

**all**—(Optional) Clear the binding state for all DHCP clients.

**ip-address**— (Optional) Clear the binding state for the DHCP client, using the specified IP address.

**mac-address**—(Optional) Clear the binding state for the DHCP client, using the specified MAC address.

**interface interface-name**—(Optional) Clear the binding state for DHCP clients on the specified interface

**routing-instance routing-instance-name**—(Optional) Clear the binding state for DHCP clients on the specified routing instance. If you do not specify a routing instance, the binding state is cleared for the default routing instance.

**Required Privilege Level**

clear

**Related Documentation**

- show dhcp relay binding on page 1633
- Device Configuration

**Output Fields**

This command produces no output.

Copyright © 2013, Juniper Networks, Inc.

## clear dhcp relay statistics

**Syntax** clear dhcp relay statistics
<routing-instance routing-instance-name>

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Clear all Dynamic Host Configuration Protocol (DHCP) relay statistics.

**Options** **routing-instance routing-instance-name**—(Optional) Clear the DHCP relay statistics on the specified routing instance. If you do not specify a routing instance name, statistics are cleared for the default routing instance.

**Required Privilege Level** clear

**Related Documentation**
- show dhcp relay statistics on page 1635
- Device Configuration

**Output Fields** This command produces no output.


Copyright © 2013, Juniper Networks, Inc.

## clear dhcp server binding

**Syntax**

clear dhcp server binding
<all | ip-address | mac-address>
<interface interface-name>
<routing-instance routing-instance-name>

**Release Information**

Statement introduced in Junos OS Release 12.1X44-D10.

**Description**

Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table on the DHCP local server.

**Options**

**all**—(Optional) Clear the binding state for all DHCP clients.

**ip-address**— (Optional) Clear the binding state for the DHCP client, using the specified IP address.

**mac-address**—(Optional) Clear the binding state for the DHCP client, using the specified MAC address.

**interface interface-name**—(Optional) Clear the binding state for DHCP clients on the specified interface.

**routing-instance routing-instance-name**—(Optional) Clear the binding state for DHCP clients on the specified routing instance.

**Required Privilege Level**

clear

**Related Documentation**

- show dhcp server binding on page 1637
- Device Configuration

**Output Fields**

This command produces no output.

Copyright © 2013, Juniper Networks, Inc.

## clear dhcp server statistics

**Syntax** clear dhcp server statistics
<routing-instance routing-instance-name>

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Clear all Dynamic Host Configuration Protocol (DHCP) local server statistics.

**Options** **routing-instance routing-instance-name**—(Optional) Clear the statistics for DHCP clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

**Required Privilege Level** clear

**Related Documentation**
- show dhcp server statistics on page 1639
- Device Configuration

**Output Fields** This command produces no output.


Copyright © 2013, Juniper Networks, Inc.

## clear dhcpv6 server binding (Local Server)

**Syntax**

clear dhcpv6 server binding
<all | *client-id* | *ip-address* | *session-id*>
<interface *interface-name*>
<routing-instance *routing-instance-name*>

**Release Information**

Command introduced in Junos Release 10.4.

**Description**

Clear the binding state of a DHCPv6 client from the client table on the DHCPv6 local server.

**Options**

- all—(Optional) Clear the binding state for all DHCPv6 clients.
- *client-id*—(Optional) Clear the binding state for the DHCPv6 client with the specified client ID (option 1).
- *ip-address*—(Optional) Clear the binding state for the DHCPv6 client with the specified address.
- *session-id*—(Optional) Clear the binding state for the DHCPv6 client with the specified session ID.
- interface *interface-name*—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.
- routing-instance *routing-instance-name*—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.

**Required Privilege Level**

clear

**Related Documentation**

- show dhcpv6 server binding (View) on page 1641
- Interfaces for Security Devices
- Device Configuration

Copyright © 2013, Juniper Networks, Inc.

## clear dhcpv6 server statistics (Local Server)

**Syntax**

**clear dhcpv6 server statistics**
**<logical-system** ***logical-system-name*****>**
**<routing-instance** ***routing-instance-name*****>**

**Release Information**

Command introduced in Junos Release 10.4.

**Description**

Clear all DHCPv6 local server statistics.

**Options**

**logical-system** ***logical-system-name***—(Optional) Clear the statistics for DHCPv6 clients on the specified logical system. If you do not specify a logical system, statistics are cleared for the default logical system.

**routing-instance** ***routing-instance-name***—(Optional) Clear the statistics for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

**Required Privilege Level**

clear

**Related Documentation**

- show dhcpv6 server statistics (View) on page 1645
- Device Configuration


Copyright © 2013, Juniper Networks, Inc.

## clear ethernet-switching statistics mac-learning

**Syntax** clear ethernet-switching statistics mac-learning

**Release Information** Command introduced in Release 10.1 of Junos OS.

**Description** Clear the media access control (MAC) learning statistics.

**Options**
- **none**—Clear MAC learning statistics on all interfaces.
- **interface *interface-name***—(Optional) Clear MAC learning statistics on the specified interface.

**Required Privilege Level** view

**Related Documentation**
- show ethernet-switching table
- show ethernet-switching mac-learning-log
- Ethernet Interfaces
- Interfaces for Security Devices

**List of Sample Output**
clear ethernet-switching statistics mac-learning on page 1373
clear ethernet-switching statistics mac-learning interface interface-name on page 1373

### Sample Output

This command produces no output.

clear ethernet-switching statistics mac-learning

```
user@host> clear ethernet-switching statistics mac-learning
```

clear ethernet-switching statistics mac-learning interface interface-name

```
user@host> clear ethernet-switching statistics mac-learning interface interface-name
```

Copyright © 2013, Juniper Networks, Inc.

## clear firewall

**Syntax**

clear firewall
<all>
<counter *counter-name*>
<filter *filter-name*>

**Release Information**

Command introduced in Junos Release 10.0.

**Description**

Clear statistics about configured firewall filters.



NOTE: The clear firewall command cannot be used to clear the Routing Engine filter counters on a backup Routing Engine that is enabled for GRES.

If you clear statistics for firewall filters that are applied to Trio-based DPCs and that also use the **prefix-action** action on matched packets, wait at least 5 seconds before you enter the **show firewall prefix-action-stats** command. A 5-second pause between issuing the **clear firewall** and **show firewall prefix-action-stats** commands avoids a possible timeout of the **show firewall prefix-action-stats** command.

**Options**

**all**—Clear the packet and byte counts for all filters.

**counter** ***counter-name***—Clear the packet and byte counts for a filter counter that has been configured with the counter firewall filter action.

**filter** ***filter-name***—Clear the packet and byte counts for the specified firewall filter.

**Required Privilege Level**

clear

**Related Documentation**

- show firewall (View) on page 1656

**List of Sample Output**

clear firewall all on page 1374

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear firewall all

```
user@host> clear firewall all
```


Copyright © 2013, Juniper Networks, Inc.

## clear gtp tunnels

**Syntax** **clear security gprs gtp tunnel <all | *identifier*>**

**Release Information** Command introduced in Release 10.0 of Junos OS. Support for GTPv2 added in Release 11.4 of Junos OS.

**Description** Clear all or specified GTP tunnels on the device.

**Options**
- *identifier*—Clear a single tunnel by entering the tunnel ID. To view current tunnel IDs, type **show security gprs gtp tunnels**.
- all—Clear all existing tunnels.

**Required Privilege Level** clear

**Related Documentation**
- General Packet Radio Service for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## clear interfaces statistics swfabx

**Syntax** clear interfaces statistics <swfab0 | swfab1>

**Release Information** Command introduced in Release 11.1 of Junos OS.

**Description** Clears interface statistics for the specified swfab interface.

**Required Privilege Level** clear

**Related Documentation**
- show interfaces swfabx on page 1698
- Interfaces Overview

**List of Sample Output** clear interfaces statistics <swfab0 | swfab1> on page 1376

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear interfaces statistics <swfab0 | swfab1>

```
user@host> clear interfaces statistics <swfab0 | swfab1>
```


Copyright © 2013, Juniper Networks, Inc.

## clear lacp statistics interfaces

**Syntax** **clear lacp statistics interfaces** <*interface-name*>

**Release Information** Command modified in Release 10.2 of Junos OS.

**Description** Clear the LACP statistics. If you do not specify an interface name, LACP statistics for all interfaces are cleared.

**Options** ***interface-name***—(Optional) Name of an interface.

**Required Privilege Level** clear

**Related Documentation**

- show lacp statistics interfaces (View) on page 1705
- Ethernet Interfaces
- Interfaces for Security Devices

**Output Fields** This command produces no output.

Copyright © 2013, Juniper Networks, Inc.

## clear network-access requests pending

**Syntax** clear network-access requests pending
<index *index-number* >

**Release Information** Command introduced in Release 8.5 of Junos OS.

**Description** Clear or cancel all pending authentication requests.

**Options**
- none—Clear all network access requests pending.
- **index** ***index-number*** —Clear the specified authentication request. To display index numbers, use the **show network-access requests pending** command.

**Required Privilege Level** clear

**Related Documentation**
- show network-access requests pending on page 1715

**List of Sample Output** clear network-access requests pending on page 1378

**Output Fields** This command produces no output.

### Sample Output

The following example displays the network access requests that are pending, clears the requests, and displays the results of the clear operation:

clear network-access requests pending

```
user@host> show network-access requests pending
Information about pending authentication entries
  Total pending authentication requests: 2
Index User                  Status
1     Sun                   Processing
2     Sam                   Processed

user@host> clear network-access requests pending
user@host> show network-access requests pending
Information about pending authentication entries
  Total pending authentication requests: 2
Index User                  Status
1     Sun                   Cancelled by Admin
2     Sam                   Cancelled by Admin
```


Copyright © 2013, Juniper Networks, Inc.

## clear network-access requests statistics

**Syntax** clear network-access requests statistics

**Release Information** Command introduced in Release 8.5 of Junos OS.

**Description** Clear general authentication statistics for the configured authentication type.

**Required Privilege Level** clear

**Related Documentation**
- authentication-order (Access Profile) on page 12
- show network-access requests statistics on page 1717

**List of Sample Output** clear network-access requests statistics on page 1379

**Output Fields** This command produces no output.

### Sample Output

clear network-access requests statistics

```
user@host> clear network-access requests statistics
```

## clear network-access securid-node-secret-file

**Syntax** clear network-access securid-node-secret-file

**Release Information** Command introduced in Release 9.1 of Junos OS.

**Description** Delete the node secret file for the SecurID authentication type.

**Required Privilege Level** clear

**Related Documentation**
- configuration-file on page 17
- securid-server on page 44
- show network-access securid-node-secret-file on page 1718

**List of Sample Output** clear network-access securid-node-secret-file on page 1380

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear network-access securid-node-secret-file

```
user@host> clear network-access securid-node-secret-file
```


Copyright © 2013, Juniper Networks, Inc.

## clear oam ethernet connectivity-fault-management path-database

**Syntax** clear oam ethernet connectivity-fault-management path-database maintenance-domain *md-name* maintenance-association *ma-name* host <*mac-addr*>

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Clear the relevant path information from the database for the specified remote host.

**Options** **host**—(Optional) MAC address of remote host in xx:xx:xx:xx:xx:xx format.

**maintenance-association** —Name of the maintenance association.

**maintenance-domain** —Name of the maintenance domain.

**Required Privilege Level** clear

**Related Documentation**
- Ethernet Port Switching for Security Devices
- show oam ethernet connectivity-fault-management path-database on page 1731

**List of Sample Output** clear oam ethernet connectivity-fault- management path-database on page 1381

### Sample Output

clear oam ethernet connectivity-fault-management path-database

```
user@host> clear oam ethernet connectivity-fault-management path-database
maintenance-domain private maintenance-association private-ma
Path database entries cleared for the remote-host
```

Copyright © 2013, Juniper Networks, Inc.

## clear oam ethernet connectivity-fault-management statistics

**Syntax**
clear oam ethernet connectivity-fault-management statistics
interface
level

**Release Information**
Statement introduced in Junos OS Release 12.1X44-D10.

**Description**
Clear connectivity-fault-management statistics.

**Options**
**Interface**—Clear the statistics on an interface.

**Level**—The maintenance-domain level (0 through 7).

**Required Privilege Level**
View

**Related Documentation**
- Ethernet Port Switching for Security Devices
- show oam ethernet connectivity-fault-management mep-statistics on page 1727

**List of Sample Output**
clear oam ethernet connectivity-fault- management statistics on page 1382

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear oam ethernet connectivity-fault-management statistics

```
user@host> clear oam ethernet connectivity-fault-management statistics
Cleared statistics of all CFM sessions
```


Copyright © 2013, Juniper Networks, Inc.

## clear security alarms

**Syntax** clear security alarms
<all>
<alarm-id *id-number*>
<alarm-type [ *types* ]>
<newer-than *YYYY-MM-DD.HH:MM:SS*>
<older-than *YYYY-MM-DD.HH:MM:SS*>
<process *process*>
<severity *severity*>

**Release Information** Command introduced in Junos OS Release 11.2.

**Description** Clear (acknowledge) the alarms that are active on the device.

**Options** **all**—(Optional) Clear all active alarms.

**alarm-id *id-number***—(Optional) Clear the specified alarm.

**alarm-type [ *types* ]**—(Optional) Clear the specified alarm type or a set of types.
You can specify one or more of the following alarm types:

- **authentication**
- **cryptographic-self-test**
- **decryption-failures**
- **encryption-failures**
- **ike-phase1-failures**
- **ike-phase2-failures**
- **key-generation-self-test**
- **non-cryptographic-self-test**
- **policy**
- **replay-attacks**

**newer-than *YYYY-MM-DD.HH:MM:SS***—(Optional) Clear active alarms that were raised after the specified date and time.

**older-than *YYYY-MM-DD.HH:MM:SS***—(Optional) Clear active alarms that were raised before the specified date and time.

**process *process***—(Optional) Clear active alarms that were raised by the specified system process.

**severity *severity***—(Optional) Clear active alarms of the specified severity.

Copyright © 2013, Juniper Networks, Inc.

You can specify the following severity levels:

- **alert**
- **crit**
- **debug**
- **emerg**
- **err**
- **info**
- **notice**
- **warning**

**Required Privilege Level** security—To view this statement in the configuration.

**Related Documentation**
- show security alarms on page 1753
- Security Policies for Security Devices

**List of Sample Output**
clear security alarms all on page 1385
clear security alarms alarm-id <alarm-id> on page 1385
clear security alarms alarm-type authentication on page 1385
clear security alarms newer-than <time> on page 1385
show security alarms older-than <time> on page 1385
show security alarms process <process> on page 1385
show security alarms severity <severity> on page 1385

**Output Fields** This command produces no output, except a statement about the number of security alarms cleared.


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

clear security alarms all

```
[3 SECURITY ALARMS] user@router> clear security alarms all

3 security alarms cleared
```

clear security alarms alarm-id <alarm-id>

```
[3 SECURITY ALARMS] user@router> clear security alarms alarm-id 1

1 security alarm cleared
```

clear security alarms alarm-type authentication

```
[3 SECURITY ALARMS] user@router> clear security alarms alarm-type authentication

3 security alarms cleared
```

clear security alarms newer-than <time>

```
[3 SECURITY ALARMS] user@router> clear security alarms newer-than 2010-01-19.13:41:59

1 security alarm cleared
```

show security alarms older-than <time>

```
[3 SECURITY ALARMS] user@router> clear security alarms older-than 2010-01-19.13:41:59

2 security alarms cleared
```

show security alarms process <process>

```
[3 SECURITY ALARMS] user@router> clear security alarms process sshd

3 security alarms cleared
```

show security alarms severity <severity>

```
[3 SECURITY ALARMS] user@router> clear security alarms severity notice

3 security alarms cleared
```

Copyright © 2013, Juniper Networks, Inc.

## clear security alg h323 counters

**Syntax** clear security alg h323 counters
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Clear information about H.323 Application Layer Gateway (ALG) counters.

**Options**

- none—Clear H.323 ALG counters.
- **node**—(Optional) For chassis cluster configurations, clear H.323 counters on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level** clear

**Related Documentation**

- h323 on page 631
- show security alg h323 counters on page 1758
- H.323 ALGs for Security Devices

**List of Sample Output** clear security alg h323 counters on page 1386

**Output Fields** This command produces no output.

### Sample Output

clear security alg h323 counters

```
user@host> clear security alg h323 counters
```


Copyright © 2013, Juniper Networks, Inc.

## clear security alg ike-esp-nat

**Syntax** clear security alg ike-esp-nat

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Clear state information about Application Layer Gateway (ALG) for IKE and ESP.

**Required Privilege Level** clear

**Related Documentation**
- show security alg ike-esp-nat summary on page 1760

**List of Sample Output** clear security alg ike-esp-nat on page 1387

**Output Fields** This command produces no output.

### Sample Output

clear security alg ike-esp-nat

```
user@host> clear security alg ike-esp-nat
10 active IKE-ESP alg state cleared
```

Copyright © 2013, Juniper Networks, Inc.

## clear security alg mgcp calls

**Syntax**
clear security alg mgcp calls
<node ( *node-id* | all | local | primary)>

**Release Information**
Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description**
Clear information about Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG) calls.

**Options**
- none—Clear all MGCP ALG calls.
- **node**—(Optional) For chassis cluster configurations, clear MGCP calls on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level**
clear

**Related Documentation**
- mgcp on page 757
- show security alg mgcp calls on page 1761
- MGCP ALGs for Security Devices

**List of Sample Output**
clear security alg mgcp calls on page 1388

**Output Fields**
This command produces no output.

### Sample Output

clear security alg mgcp calls

```
user@host> clear security alg mgcp calls
```


Copyright © 2013, Juniper Networks, Inc.

## clear security alg mgcp counters

**Syntax**
clear security alg mgcp counters
<node ( *node-id* | all | local | primary)>

**Release Information**
Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description**
Clear Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG) counter information.

**Options**
- none—Clear all MGCP ALG counters.
- **node**—(Optional) For chassis cluster configurations, clear MGCP counters on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level**
clear

**Related Documentation**
- mgcp on page 757
- show security alg mgcp counters on page 1763
- MGCP ALGs for Security Devices

**List of Sample Output**
clear security alg mgcp counters on page 1389

**Output Fields**
This command produces no output.

### Sample Output

**clear security alg mgcp counters**

```
user@host> clear security alg mgcp counters
```

Copyright © 2013, Juniper Networks, Inc.

## clear security alg sccp calls

**Syntax** clear security alg sccp calls
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Clear Skinny Client Protocol (SCCP) Application Layer Gateway (ALG) call information.

**Options**

- none—Clear all SCCP ALG calls.
- **node**—(Optional) For chassis cluster configurations, clear SCCP calls on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level** clear

**Related Documentation**

- sccp on page 914
- show security alg sccp calls on page 1770
- SCCP ALGs for Security Devices

**List of Sample Output** clear security alg sccp calls on page 1390

**Output Fields** This command produces no output.

### Sample Output

clear security alg sccp calls

```
user@host> clear security alg sccp calls
```


Copyright © 2013, Juniper Networks, Inc.

## clear security alg sccp counters

**Syntax** clear security alg sccp counters
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Clear Skinny Client Control Protocol (SCCP) Application Layer Gateway (ALG) counters.

**Options**

- none—Clear all SCCP ALG counters.
- **node**—(Optional) For chassis cluster configurations, clear SCCP counters on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level** clear

**Related Documentation**

- sccp on page 914
- show security alg sccp counters on page 1772
- SCCP ALGs for Security Devices

**List of Sample Output** clear security alg sccp counters on page 1391

**Output Fields** This command produces no output.

### Sample Output

clear security alg sccp counters

```
user@host> clear security alg sccp counters
```

## clear security alg sip calls

**Syntax**

clear security alg sip calls
<node ( *node-id* | all | local | primary)>

**Release Information**

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description**

Clear Session Initiation Protocol (SIP) Application Layer Gateway (ALG) call information.

**Options**

- none—Clear all SIP ALG calls.
- **node**—(Optional) For chassis cluster configuration, clear SIP calls on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level**

clear

**Related Documentation**

- sip (Security) on page 949
- show security alg sip calls on page 1774
- SIP ALGs for Security Devices

**List of Sample Output**

clear security alg sip calls on page 1392

**Output Fields**

This command produces no output.

### Sample Output

clear security alg sip calls

```
user@host> clear security alg sip calls
```


Copyright © 2013, Juniper Networks, Inc.

## clear security alg sip counters

**Syntax**
clear security alg sip counters
<node ( *node-id* | all | local | primary)>

**Release Information**
Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description**
Clear Session Initiation Protocol (SIP) Application Layer Gateway (ALG) counters.

**Options**
- none—Clear all SIP ALG counters.
- **node**—(Optional) For chassis cluster configurations, clear SIP counters on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level**
clear

**Related Documentation**
- sip (Security) on page 949
- show security alg sip counters on page 1776
- SIP ALGs for Security Devices

**List of Sample Output**
clear security alg sip counters on page 1393

**Output Fields**
This command produces no output.

### Sample Output

clear security alg sip counters

```
user@host> clear security alg sip counters
```

## clear security application-firewall rule-set statistics

**Syntax** **clear security application-firewall rule-set statistics**

**Release Information** Command introduced in Release 11.1 of Junos OS.

**Description** Clear all the security application firewall rule set statistics information.

**Required Privilege Level** clear

**Related Documentation**
- Application Firewall
- show security application-firewall rule-set on page 1787

**Output Fields** This command produces no output.


Copyright © 2013, Juniper Networks, Inc.

## clear security application-firewall rule-set statistics logical-system

**Syntax** The master, or root, administrator can issue the following statements:

clear security application-firewall rule-set statistics [logical-system *logical-system-name* | all | root-logical-system]

The user logical system administrator can issue the following statement:

clear security application-firewall rule-set statistics all

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Clear all security application firewall rule set statistics.



NOTE: User logical system administrators can clear statistics only for the logical systems they can access. For information about master and user administrator roles in logical systems, see the *Junos OS Logical Systems Configuration Guide for Security Devices*.

**Options** ***logical-system-name***—Name of a specific logical system.

**all**—(default) Clear all rule set statistics for a specific logical system or all logical systems.

**root-logical-system**—Clear application firewall rule set statistics on the root logical system (master administrator only).

**Required Privilege Level** clear

**Related Documentation**

- Application Firewall
- show security application-firewall rule-set logical-system on page 1789

**Output Fields** This command produces no output.

Copyright © 2013, Juniper Networks, Inc.

## clear security datapath-debug counters

**Syntax** clear security datapath-debug counters

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Clear all data path-debugging counters.

**Required Privilege Level** clear

**Related Documentation**
- show security datapath-debug capture on page 1793
- show security datapath-debug counter on page 1794

**List of Sample Output** clear security datapath-debug counters on page 1396

**Output Fields** This command produces no output.

### Sample Output

clear security datapath-debug counters

```
user@host> clear security datapath-debug counters
```


Copyright © 2013, Juniper Networks, Inc.

## clear security dns-cache

**Syntax** clear security dns-cache <dns-name *dns-name*>

**Release Information** Command introduced in Junos OS Release 12.1X44-D10.

**Description** Reset DNS cache information.



NOTE: This command is only available to the master administrator on devices that are configured for logical systems. This command is not available in user logical systems or on devices that are not configured for logical systems.

**Options**

- **dns-name**—Clear DNS cache information for the specified name.

**Required Privilege Level** clear

**Related Documentation**

- show security dns-cache on page 1795
- Master Administrator for Logical Systems on Security Devices

Copyright © 2013, Juniper Networks, Inc.

## clear security dynamic-vpn all

**Syntax** clear security dynamic-vpn all

**Release Information** Command introduced in Junos Release 10.4.

**Description** Clear all dynamic VPN user connections.

**Required Privilege Level** clear

**Related Documentation**
- show security dynamic-vpn users on page 1803
- show security dynamic-vpn users terse on page 1804

**List of Sample Output** clear security dynamic-vpn all on page 1398

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security dynamic-vpn all

```
user@host> clear security dynamic-vpn all
2 user connection entries cleared
```


Copyright © 2013, Juniper Networks, Inc.

## clear security dynamic-vpn user

**Syntax** clear security dynamic-vpn user *username* ike-id *id*

**Release Information** Command introduced in Junos OS Release 10.4.

**Description** Clear the dynamic VPN user connection for the specified username.

**Required Privilege Level** clear

**Related Documentation**
- show security dynamic-vpn users on page 1803
- show security dynamic-vpn users terse on page 1804

**List of Sample Output** clear security dynamic-vpn user on page 1399

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security dynamic-vpn user

```
user@host> clear security dynamic-vpn user guang ike-id bob.juniper.net
Connection entry for user guang has been cleared
```

Copyright © 2013, Juniper Networks, Inc.

## clear security firewall-authentication history

**Syntax** clear security firewall-authentication history
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Clear all firewall authentication history information.

**Options**

- **node**—(Optional) For chassis cluster configurations, clear all firewall authentication history on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level** clear

**Related Documentation**

- firewall-authentication (Security) on page 590
- show security firewall-authentication history on page 1805

**List of Sample Output**

clear security firewall-authentication history on page 1400
clear security firewall-authentication history node 1 on page 1400

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security firewall-authentication history

```
user@host> clear security firewall-authentication history
node0:
--------------------------------------------------------------------------
node1:
--------------------------------------------------------------------------
```

### Sample Output

clear security firewall-authentication history node 1

```
user@host> clear security firewall-authentication history node 1
node1:
--------------------------------------------------------------------------
```


Copyright © 2013, Juniper Networks, Inc.

## clear security firewall-authentication history address

**Syntax** clear security firewall-authentication history address *address*
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Clear firewall authentication history for this source IP address.

**Options**

- **address** *address* —Source IP address for which to clear firewall authentication history.
- none—Clear all firewall authentication history for this address.
- **node**—(Optional) For chassis cluster configurations, clear firewall authentication history for this address on a specific node.
  - *node-id* —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level** clear

**Related Documentation**

- firewall-authentication (Security) on page 590
- show security firewall-authentication history address on page 1807

**List of Sample Output**

clear security firewall-authentication history address 100.0.0.1 on page 1401
clear security firewall-authentication history address 100.0.0.1 node 1 on page 1401

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security firewall-authentication history address 100.0.0.1

```
user@host> clear security firewall-authentication history address 100.0.0.1
node0:
--------------------------------------------------------------------------
node1:
--------------------------------------------------------------------------
```

### Sample Output

clear security firewall-authentication history address 100.0.0.1 node 1

```
user@host> clear security firewall-authentication history address 100.0.0.1 node 1
node1:
--------------------------------------------------------------------------
```

Copyright © 2013, Juniper Networks, Inc.

## clear security firewall-authentication history identifier

**Syntax** clear security firewall-authentication history identifier *identifier*
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; node options added in Release 9.0 of Junos OS.

**Description** Clear firewall authentication history information for the authentication with this identifier.

**Options**

- **identifier** *identifier* —Identification number of the authentication for which to clear authentication history.
- none—Clear all firewall authentication history information for the authentication with this identifier.
- **node**—(Optional) For chassis cluster configurations, clear firewall authentication history on a specific node for the authentication with this identifier.
  - *node-id* —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level** clear

**Related Documentation**

- firewall-authentication (Security) on page 590
- show security firewall-authentication history identifier on page 1810

**List of Sample Output**

clear security firewall-authentication history identifier 2 on page 1402
clear security firewall-authentication history identifier 2 node 1 on page 1402

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security firewall-authentication history identifier 2

```
user@host> clear security firewall-authentication history identifier 2
node0:
--------------------------------------------------------------------------
node1:
--------------------------------------------------------------------------
```

### Sample Output

clear security firewall-authentication history identifier 2 node 1

```
user@host> clear security firewall-authentication history identifier 2 node 1
node1:
--------------------------------------------------------------------------
```


Copyright © 2013, Juniper Networks, Inc.

## clear security firewall-authentication users

**Syntax** clear security firewall-authentication users
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Clear firewall authentication tables for all users.

**Options**

- **node**—(Optional) For chassis cluster configurations, clear firewall authentication details for all users on a specific node.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level** clear

**Related Documentation**

- show security firewall-authentication users on page 1813

**List of Sample Output**

clear security firewall-authentication users on page 1403
clear security firewall-authentication users node 1 on page 1403

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security firewall-authentication users

```
user@host> clear security firewall-authentication users node 1
node0:
--------------------------------------------------------------------------
node1:
--------------------------------------------------------------------------
```

### Sample Output

clear security firewall-authentication users node 1

```
user@host> clear security firewall-authentication users node 1
node1:
--------------------------------------------------------------------------
```

Copyright © 2013, Juniper Networks, Inc.

## clear security firewall-authentication users address

**Syntax** clear security firewall-authentication users address *address*
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Clear information about the users at the specified IP address that are currently authenticated.

**Options**

- **address** *address* —IP address for which to clear user firewall authentication information.
- none—Clear all the firewall authentication information for users at this IP address.
- **node**—(Optional) For chassis cluster configurations, clear user firewall authentication entries on a specific node.
  - *node-id* —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level** clear

**Related Documentation**

- show security firewall-authentication users address on page 1815

**List of Sample Output**

clear security firewall-authentication users address 100.0.0.1 on page 1404
clear security firewall-authentication users address 100.0.0.1 node 1 on page 1404

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security firewall-authentication users address 100.0.0.1

```
user@host> clear security firewall-authentication users address 100.0.0.1
node0:
--------------------------------------------------------------------------
node1:
--------------------------------------------------------------------------
```

### Sample Output

clear security firewall-authentication users address 100.0.0.1 node 1

```
user@host> clear security firewall-authentication users address 100.0.0.1 node 1
node1:
--------------------------------------------------------------------------
```


Copyright © 2013, Juniper Networks, Inc.

## clear security firewall-authentication users identifier

**Syntax** clear security firewall-authentication users identifier *identifier*
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Clear firewall authentication details about the user with this identification number.

**Options**

- none—Identification number of the user for which to clear authentication details.
- **node**—(Optional) For chassis cluster configurations, clear the firewall authentication details on a specific node (device) in the cluster for the user with this identification number.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level** clear

**Related Documentation**

- show security firewall-authentication users identifier on page 1818

**List of Sample Output**

clear security firewall-authentication users identifier 2 on page 1405
clear security firewall-authentication users identifier 2 node 1 on page 1405

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security firewall-authentication users identifier 2

```
user@host> clear security firewall-authentication users identifier 2
node0:
--------------------------------------------------------------------------
node1:
--------------------------------------------------------------------------
```

### Sample Output

clear security firewall-authentication users identifier 2 node 1

```
user@host> clear security firewall-authentication users identifier 2 node 1
node1:
--------------------------------------------------------------------------
```

Copyright © 2013, Juniper Networks, Inc.

## clear security flow ip-action

**Syntax** **clear security flow ip-action** [*filter*]

**Release Information** Command introduced in Release 10.4 of Junos OS. Logical systems option introduced in Release 11.2 of Junos OS.

**Description** Clear IP-action entries, based on filtered options, for IP sessions running on the device.

**Options** *filter*—Filter the display based on the specified criteria.

The following filters display those sessions that match the criteria specified by the filter. Refer to the sample output for filtered output examples.

**all |** [*filter*]—All active sessions on the device.

**destination-port** ***destination-port***—Destination port number of the traffic. Range is 1 through 65,535.

**destination-prefix** ***destination-prefix***—Destination IP prefix or address.

**family (inet | inet6)** [*filter*]—IPv4 traffic or IPv6-NATPT traffic and filtered options.

**logical-system** ***logical-system-name*** **| all** [*filter*]—Specified logical system or all logical systems.

**protocol** ***protocol-name*** **|** ***protocol-number*** [*filter*]—Protocol name or number and filtered options.

- **ah** or **51**
- **egp** or **8**
- **esp** or **50**
- **gre** or **47**
- **icmp** or **1**
- **icmp6** or **58**
- **igmp** or **2**
- **ipip** or **4**
- **ospf** or **89**
- **pim** or **103**
- **rsvp** or **46**
- **sctp** or **132**
- **tcp** or **6**
- **udp** or **17**


Copyright © 2013, Juniper Networks, Inc.

**root-logical-system** [*filter*]—Default logical system information and filtered options.

**source-port** ***source-port***—Source port number of the traffic. Range is 1 through 65,535.

**source-prefix** ***source-prefix***—Source IP prefix or address of the traffic.

**Required Privilege Level** clear

**Related Documentation**
- show security flow ip-action on page 1874

**List of Sample Output**
clear security flow ip-action all on page 1407
clear security flow ip-action destination-prefix on page 1407
clear security flow ip-action family inet on page 1407
clear security flow ip-action protocol udp on page 1407

**Output Fields** When you enter this command, the system responds with the status of your request.

## Sample Output

clear security flow ip-action all

```
user@host>clear security flow ip-action all
1008 ip-action entries cleared
```

clear security flow ip-action destination-prefix

```
user@host>clear security flow ip-action destination-prefix 5.0.0.0/8
87 ip-action entries cleared
```

clear security flow ip-action family inet

```
user@host>clear security flow ip-action family inet
2479 ip-action entries cleared
```

clear security flow ip-action protocol udp

```
user@host>clear security flow ip-action protocol udp
270 ip-action entries cleared
```

Copyright © 2013, Juniper Networks, Inc.

## clear security flow session all

**Syntax** clear security flow session all
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Clear all currently active security sessions on the device.

**Options**

- all—Clear information about all active sessions.
- **node**—(Optional) For chassis cluster configurations, clear all security sessions on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level** clear

**Related Documentation**

- show security flow session on page 1879

**List of Sample Output**

clear security flow session all on page 1408
clear security flow session all node 0 on page 1408

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security flow session all

```
user@host> clear security flow session all
node0:
--------------------------------------------------------------------------
1 active sessions cleared
node1:
-------- ------------------------------------------------------------------
0 active sessions cleared
```

### Sample Output

clear security flow session all node 0

```
user@host> clear security flow session all node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```


Copyright © 2013, Juniper Networks, Inc.

## clear security flow session application

**Syntax** clear security flow session application
*application-name*
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS. The **node** options added in Junos OS Release 9.0.

**Description** Clear currently active sessions for application types or application sets.

**Options**

- *application-name* —Name of the specified application type or application set.
  - **dns**—Domain Name System
  - **ftp**—File Transfer Protocol
  - **ignore**—Ignore application type
  - **mgcp-ca**—Media Gateway Control Protocol with Call Agent
  - **mgcp-ua**—MGCP with User Agent
  - **ms-rpc**—Microsoft RPC
  - **pptp**—Point-to-Point Tunneling Protocol
  - **q931**—ISDN connection control protocol
  - **ras**—RAS
  - **realaudio**—RealAudio
  - **rsh**—UNIX remote shell services
  - **rtsp**—Real-Time Streaming Protocol
  - **sccp**—Skinny Client Control Protocol
  - **sip**—Session Initiation Protocol
  - **sqlnet-v2**—Oracle SQLNET
  - **sun-rpc**—Sun Microsystems RPC
  - **talk**—TALK program
  - **tftp**—Trivial File Transfer Protocol
- **node**—(Optional) For chassis cluster configurations, clear sessions for applications on a specific node (device) in the cluster.
  - *node-id* —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.

Copyright © 2013, Juniper Networks, Inc.

- **local** —Clear the local node.
- **primary**—Clear the primary node.

**Required Privilege Level** clear

**Related Documentation**
- show security flow session application on page 1884
- Security Policy Applications for Security Devices

**List of Sample Output**
clear security flow session application dns on page 1410
clear security flow session application dns node 0 on page 1410

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

## Sample Output

clear security flow session application dns

```
user@host> clear security flow session application dns
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

## Sample Output

clear security flow session application dns node 0

```
user@host> clear security flow session application dns node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```


Copyright © 2013, Juniper Networks, Inc.

## clear security flow session destination-port

**Syntax** clear security flow session destination-port
*destination-port-number*
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Clear each session that uses the specified destination port

**Options**

- ***destination-port-number*** —Number of the destination port.
- **node**—(Optional) For chassis cluster configurations, clear security sessions on the port on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level** clear

**Related Documentation**

- show security flow session destination-port on page 1900

**List of Sample Output**

clear security flow session destination-port 1 on page 1411
clear security flow session destination-port 1 node 0 on page 1411

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security flow session destination-port 1

```
user@host> clear security flow session destination-port 1
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

### Sample Output

clear security flow session destination-port 1 node 0

```
user@host> clear security flow session destination-port 1 node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```

Copyright © 2013, Juniper Networks, Inc.

## clear security flow session destination-prefix

**Syntax**

clear security flow session destination-prefix
*destination-IP-prefix*
<node ( *node-id* | all | local | primary)>

**Release Information**

Command introduced in Release 8.5 of Junos OS.
The **node** options added in Release 9.0 of Junos OS.
Support for IPv6 addresses added in Release 10.2 of Junos OS.

**Description**

Clear sessions that match this destination IP prefix or address.

**Options**

- ***destination-IP-prefix***—Destination IP prefix or address.
- **node**—(Optional) For chassis cluster configurations, clear sessions that match the IP prefix or address on a specific node (device) in the cluster.
  - ***node-id***—Identification number of the node. It can be 0 or 1.
  - **all**—Clear all nodes.
  - **local**—Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level**

clear

**Related Documentation**

- show security flow session destination-prefix on page 1904

**List of Sample Output**

clear security flow session destination-prefix 100.0.0.1 on page 1412
clear security flow session destination-prefix 10::10 on page 1412
Clear security flow session destination-prefix 100.0.0.1 node 0 on page 1413

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security flow session destination-prefix 100.0.0.1

```
clear security flow session destination-prefix 100.0.0.1
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

clear security flow session

```
user@host> clear security flow session destination-prefix 10::10
1 active sessions cleared
```


Copyright © 2013, Juniper Networks, Inc.

destination-prefix
10::10

## Sample Output

Clear security flow session destination-prefix 100.0.0.1 node 0

```
user@host> clear security flow session destination-prefix 100.0.0.1 node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```

## clear security flow session family

**Syntax** clear security flow session family (inet | inet6)

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Clear sessions that match the specified protocol family.

**Options**
- **inet**—Clear IPv4 sessions.
- **inet6**—Clear IPv6 sessions.

**Required Privilege Level** clear

**Related Documentation**
- show security flow session family on page 1915

**List of Sample Output**
clear security flow session family inet on page 1414
clear security flow session family inet6 on page 1414

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security flow session family inet

```
user@host> clear security flow session family inet
1 active sessions cleared
```

clear security flow session family inet6

```
user@host> clear security flow session family inet6
1 active sessions cleared
```


Copyright © 2013, Juniper Networks, Inc.

## clear security flow session interface

**Syntax**

clear security flow session interface
*interface-name*
<node ( *node-id* | all | local | primary)>

**Release Information**

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description**

Clear sessions that use the specified interface.

**Options**

- *interface-name* —Name of a specific incoming or outgoing interface.
- **node**—(Optional) For chassis cluster configurations, clear security sessions on the interface on a specific node (device) in the cluster.
  - *node-id* —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level**

clear

**Related Documentation**

- show security flow session interface on page 1922

**List of Sample Output**

clear security flow session interface ge-0/0/0.0 on page 1415
clear security flow session interface ge/0/0.0 node 0 on page 1415

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security flow session interface ge-0/0/0.0

```
user@host> clear security flow session interface ge-0/0/0.0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

### Sample Output

clear security flow session interface ge/0/0.0 node 0

```
user@host> clear security flow session interface ge-0/0/0.0 node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```

Copyright © 2013, Juniper Networks, Inc.

## clear security flow session protocol

**Syntax** clear security flow session protocol *protocol-name* | *protocol-number*
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Clear each session that uses the specified IP protocol.

**Options**

- ***protocol-name*** — (Optional) Networking protocol name. The following text values are supported.
  - **ah**—IP Security Authentication Header
  - **egp**—Exterior gateway protocol
  - **esp**—IPsec Encapsulating Security Payload
  - **gre**—Generic routing encapsulation
  - **icmp**—Internet Control Message Protocol
  - **igmp**—Internet Group Management Protocol
  - **ipip**—IP over IP
  - **ospf**—Open Shortest Path First
  - **pim**—Protocol Independent Multicast
  - **rsvp**—Resource Reservation Protocol
  - **sctp**—Stream Control Transmission Protocol
  - **tcp**—Transmission Control Protocol
  - **udp**—User Datagram Protocol
- ***protocol-number*** —(Optional) Numeric protocol value. For a complete list of possible numeric values, see RFC 1700, *Assigned Numbers (for the Internet Protocol Suite)*.

  **Range:** 0 through 255
- **node**—(Optional) For chassis cluster configurations, clear security on a specific node (device) in the cluster for the user with this identification number.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level** clear


Copyright © 2013, Juniper Networks, Inc.

**Related Documentation**
- show security flow session protocol on page 1931

**List of Sample Output**
clear security flow session protocol pim on page 1417
clear security flow session protocol 0 on page 1417

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

## Sample Output

clear security flow session protocol pim

```
user@host> clear security flow session protocol pim
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

## Sample Output

clear security flow session protocol 0

```
user@host> clear security flow session protocol 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

Copyright © 2013, Juniper Networks, Inc.

## clear security flow session resource-manager

**Syntax** clear security flow session resource-manager
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Clear resource-manager sessions.

**Options**

- **node**—(Optional) For chassis cluster configurations, clear the resource manager sessions on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level** clear

**Related Documentation**

- show security flow session resource-manager on page 1937

**List of Sample Output**

clear security flow session resource-manager on page 1418
clear security flow session resource-manager node 0 on page 1418

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security flow session resource-manager

```
user@host> clear security flow session resource-manager
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

### Sample Output

clear security flow session resource-manager node 0

```
user@host> clear security flow session resource-manager node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```


Copyright © 2013, Juniper Networks, Inc.

## clear security flow session services-offload

**Syntax** **clear security flow session services-offload** [*filter*]

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Clear services-offload security sessions, based on filtered options, on the device. This command also clears a services-offload security session from both the network processor and the Services Processing Unit (SPU) on which the specified session was installed.

**Options** *filter*—Filter the display based on the specified criteria.

The following filters clear those sessions that match the criteria specified by the filter. Refer to the sample output for filtered output examples.

**application** ***application-name***—Application name.

**destination-port** ***destination-port***—Destination port number. Range is from 1 through 65,535.

**destination-prefix** ***destination-prefix***—Destination IP prefix or address.

**family (inet | inet6)**—IPv4 traffic or IPv6-NAT-PT traffic.

**interface** ***interface-name***—Incoming or outgoing interface name.

**logical-system** ***logical-system-name*** **| all**—Specified logical system name or all logical systems.

**protocol** ***protocol-name*** **|** ***protocol-number*** —Protocol name or number.

- **ah** or **51**
- **egp** or **8**
- **esp** or **50**
- **gre** or **47**
- **icmp** or **1**
- **icmp6** or **58**
- **igmp** or **2**
- **ipip** or **4**
- **ospf** or **89**
- **pim** or **103**
- **rsvp** or **46**
- **sctp** or **132**

Copyright © 2013, Juniper Networks, Inc.

- **tcp** or **6**
- **udp** or **17**

**root-logical-system** [*filter*]—Root logical system information and filtered options.

**source-port** ***source-port***—Source port number of the traffic. Range is from 1 through 65,535.

**source-prefix** ***source-prefix***—Source IP prefix or address of the traffic.

**Required Privilege Level** clear

**Related Documentation**
- show security flow session services-offload on page 1942

**List of Sample Output**
clear security flow session services-offload on page 1420
clear security flow session services-offload application on page 1420
clear security flow session services-offload destination-port on page 1420
clear security flow session services-offload destination-prefix on page 1420
clear security flow session services-offload family on page 1421
clear security flow session services-offload interface on page 1421
clear security flow session services-offload logical-system on page 1421
clear security flow session services-offload protocol on page 1421
clear security flow session services-offload root-logical-system on page 1421
clear security flow session services-offload source-port on page 1421
clear security flow session services-offload source-prefix on page 1421

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

## Sample Output

clear security flow session services-offload

```
user@host>clear security flow session services-offload
0 active sessions cleared
```

clear security flow session services-offload application

```
user@host>clear security flow session services-offload dns
0 active sessions cleared
```

clear security flow session services-offload destination-port

```
user@host>clear security flow session services-offload destination-port 1
0 active sessions cleared
```

clear security flow session

```
user@host>clear security flow session services-offload destination-prefix 100.0.0.1
0 active sessions cleared
```


Copyright © 2013, Juniper Networks, Inc.

services-offload destination-prefix

clear security flow session services-offload family

```
user@host>clear security flow session services-offload family inet
1 active sessions cleared
```

clear security flow session services-offload interface

```
user@host>clear security flow session services-offload interface ge-0/0/0.0
0 active sessions cleared
```

clear security flow session services-offload logical-system

```
user@host>clear security flow session services-offload logical-system all
0 active sessions cleared
```

clear security flow session services-offload protocol

```
user@host>clear security flow session services-offload protocol pim
0 active sessions cleared
```

clear security flow session services-offload root-logical-system

```
user@host>clear security flow session services-offload root-logical-system application dns
0 active sessions cleared
```

clear security flow session services-offload source-port

```
user@host>clear security flow session services-offload source-port 1
0 active sessions cleared
```

clear security flow session services-offload source-prefix

```
user@host>clear security flow session services-offload source-prefix 100.0.0.1
0 active sessions cleared
```

Copyright © 2013, Juniper Networks, Inc.

## clear security flow session session-identifier

**Syntax**

clear security flow session session-identifier
*session-identifier*
<node ( *node-id* | all | local | primary)>

**Release Information**

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description**

Clear the session with the specific identifier.

**Options**

- ***session-identifier*** —Number from 1 through 4,294,967,295 that identifies the security session.
- **node**—(Optional) For chassis cluster configurations, clear the specified session on a specific node (device) in the cluster.
  - ***node-id***—Identification number of the node. It can be 0 or 1.
  - **all**—Clear all nodes.
  - **local**—Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level**

clear

**Related Documentation**

- show security flow session session-identifier on page 1947

**List of Sample Output**

clear security flow session session-identifier 1 on page 1422
clear security flow session session-identifier 1 node 0 on page 1422

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security flow session session-identifier 1

```
user@host> clear security flow session session-identifier 1
0 active sessions cleared
```

### Sample Output

clear security flow session session-identifier 1 node 0

```
user@host> clear security flow session session-identifier 1 node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```


Copyright © 2013, Juniper Networks, Inc.

## clear security flow session source-port

**Syntax**

clear security flow session source-port
*source-port-number*
<node ( *node-id* | all | local | primary)>

**Release Information**

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description**

Clear each session that uses the specified source port.

**Options**

- *source-port-number* —Number that identifies the source port.

  **Range:** 1 through 65,535

- **node**—(Optional) For chassis cluster configurations, clear sessions on the specified source port on a specific node (device) in the cluster.
  - *node-id* —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level**

clear

**Related Documentation**

- show security flow session source-port on page 1951

**List of Sample Output**

clear security flow session source-port 1 on page 1423
clear security flow session source-port 1 node 0 on page 1423

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security flow session source-port 1

```
user@host> clear security flow session source-port 1
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

### Sample Output

clear security flow session source-port 1 node 0

```
user@host> clear security flow session source-port 1 node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```

Copyright © 2013, Juniper Networks, Inc.

## clear security flow session source-prefix

**Syntax**

clear security flow session source-prefix
*source-prefix-number*
<node ( *node-id* | all | local | primary)>

**Release Information**

Command introduced in Release 8.5 of Junos OS.
The **node** options added in Release 9.0 of Junos OS.
Support for IPv6 addresses added in Release 10.2 of Junos OS.

**Description**

Clear sessions that match the source prefix.

**Options**

- *source-prefix-number*—Source IP prefix or address.
- **node**—(Optional) For chassis cluster configurations, clear security sessions matching the source prefix on a specific node (device) in the cluster.
  - *node-id*—Identification number of the node. It can be 0 or 1.
  - **all**—Clear all nodes.
  - **local**—Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level**

clear

**Related Documentation**

- show security flow session source-prefix on page 1955

**List of Sample Output**

clear security flow session source-prefix 100.0.0.1 on page 1425
clear security flow session source-prefix 10::10 on page 1425
clear security flow session source-prefix 100.0.0.1 node 0 on page 1425

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

clear security flow session source-prefix 100.0.0.1

```
user@host> clear security flow session source-prefix 100.0.0.1
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

clear security flow session source-prefix 10::10

```
user@host> clear security flow session source-prefix 10::10
1 active sessions cleared
```

## Sample Output

clear security flow session source-prefix 100.0.0.1 node 0

```
user@host> clear security flow session source-prefix 100.0.0.1 node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```

Copyright © 2013, Juniper Networks, Inc.

## clear security flow statistics

**Syntax** clear security flow statistics

**Release Information** Command introduced in Junos Release 11.4

**Description** Clear the flow-related system statistics.

**Required Privilege Level** clear

**Related Documentation**
- show security flow statistics on page 1976

**Output Fields** This command produces no output.


Copyright © 2013, Juniper Networks, Inc.

## clear security gprs sctp counters

**Syntax** clear security gprs sctp counters

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Clear the statistics of the dropped Stream Control Transmission Protocol (SCTP) counters.

**Options** none—Clear all dropped SCTP counters.

**Required Privilege Level** clear

**Related Documentation**
- General Packet Radio Service for Security Devices
- show security gprs sctp counters on page 1981

**List of Sample Output** clear security gprs sctp counters on page 1427

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security gprs sctp counters

```
user@host> clear security gprs sctp counters
```

## clear security gprs gtp counters

**Syntax** clear security gprs gtp counters *<all | error | ha | message <message-name> | packet | request | tunnel>*

**Release Information** Command introduced in Junos OS Release 12.1X44-D2.

**Description** Clear all GTP counters on the device.

**Options**

- **all**—Clear all GTP counters.
- **error**—Clear GTP error counters.
- **ha**—Clear GTP HA counters.
- **message *message-name***—Clear GTP message counters.
- **packet**—Clear GTP packet counters.
- **request**—Clear GTP request counters.
- **tunnel**—Clear GTP tunnel counters.

**Required Privilege Level** clear

**Related Documentation**

- show security gprs gtp counters on page 1659

**List of Sample Output**

clear security gprs gtp counters all on page 1429
clear security gprs gtp counters error on page 1429
clear security gprs gtp counters ha on page 1429
clear security gprs gtp counters message v0-create-aa-pdp-req on page 1429
clear security gprs gtp counters packet on page 1429
clear security gprs gtp counters request on page 1429
clear security gprs gtp counters tunnel on page 1429

**Output Fields** When you enter this command, you are provided feedback on the status of your request.


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

clear security gprs gtp counters all

```
user@host> clear security gprs gtp counters all
All GTP counters have been cleared
```

clear security gprs gtp counters error

```
user@host> clear security gprs gtp counters error
GTP error counter has been cleared
```

clear security gprs gtp counters ha

```
user@host> clear security gprs gtp counters ha
GTP HA counter has been cleared
```

clear security gprs gtp counters message v0-create-aa-pdp-req

```
user@host> clear security gprs gtp counters message v0-create-aa-pdp-req
GTPv0 create AA PDP request message counter has been cleared
```

clear security gprs gtp counters packet

```
user@host> clear security gprs gtp counters packet
GTP packet counter has been cleared
```

clear security gprs gtp counters request

```
user@host> clear security gprs gtp counters request
GTP request counter has been cleared
```

clear security gprs gtp counters tunnel

```
user@host> clear security gprs gtp counters tunnel
GTP tunnel counter has been cleared
```

Copyright © 2013, Juniper Networks, Inc.

## clear security group-vpn member ike security-associations

**Syntax** clear security group-vpn member ike security-associations [index *SA-index*] [*peer-ipaddress*]

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Clear IKE security association (SA) for a group member.

**Options**
- none—Clear all IKE SAs for the group member.
- **index**—(Optional) Clear the IKE SA with this index number.
- *peer-ipaddress*—(Optional) Clear the IKE SA with this peer.

**Required Privilege Level** clear

**Related Documentation**
- show security group-vpn member ike security-associations on page 1983

**List of Sample Output** clear security group-vpn member ike security-associations on page 1430

**Output Fields** This command produces no output.

### Sample Output

clear security group-vpn member ike security-associations

```
user@host> clear security group-vpn member ike security-associations
```


Copyright © 2013, Juniper Networks, Inc.

## clear security group-vpn member ipsec security-associations

**Syntax** clear security group-vpn member ipsec security-associations [index *SA-index*]

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Clear group VPN SA for a group member.

**Options**
- none—Clear all group VPN SAs for the group member.
- **index**—(Optional) Clear the group VPN SA with this index number.

**Required Privilege Level** clear

**Related Documentation**
- show security group-vpn member ipsec security-associations on page 1987

**List of Sample Output** clear security group-vpn member ipsec security-associations on page 1431

**Output Fields** This command produces no output.

### Sample Output

clear security group-vpn member ipsec security-associations

```
user@host> clear security group-vpn member ipsec security-associations
```

## clear security group-vpn member kek security-associations

**Syntax** clear security group-vpn member kek security-assocations [index *SA-index*]

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Clear key encryption key (KEK) SAs for a group member.

**Options**
- none—Clear all KEK SAs for the group member.
- **index**—(Optional) Clear the KEK SA with this index number.

**Required Privilege Level** clear

**Related Documentation**
- show security group-vpn member kek security-associations on page 1990

**List of Sample Output** clear security group-vpn member kek security-associations on page 1432

**Output Fields** This command produces no output.

### Sample Output

clear security group-vpn member kek security-associations

```
user@host> clear security group-vpn member kek security-associations
```


Copyright © 2013, Juniper Networks, Inc.

## clear security group-vpn server

**Syntax** clear security group-vpn server [group *group-name* | group-id *group-id*] [now]

**Description** Remove active members for a specified group. If no options are specified, members are removed from all groups. After this command is issued, members will need to reregister.



NOTE: An IKE SA can be used by a group member to register to multiple groups. When you remove members for a specified group, all existing IKE SAs that could be used to register to the group are also removed.

**Options**

- none—All members are removed from all groups.
- **group**—(Optional) Remove members for the specified group name.
- **group-id**—(Optional) Remove members for the specified group identifier.
- **now**—(Optional) Immediatly remove all group-related information.

**Required Privilege Level** clear

**Related Documentation**

- show security group-vpn server registered-members on page 2005

**List of Sample Output** clear security group-vpn server on page 1433

**Output Fields** If there is a problem with the command, one of the following messages appears:

- Group does not exist
- Group is in the process of deletion
- Error in clear members
- Warning Message; Fail to push delete to members as server-member-communication is not configured.

## Sample Output

clear security group-vpn server

```
user@host> clear security group-vpn server
```

Copyright © 2013, Juniper Networks, Inc.

## clear security idp

**Syntax** clear security idp
(application-identification | application-statistics | attack | counters | status)

**Release Information** Command introduced in Release 10.1 of Junos OS.

**Description** Clear the following IDP information:

- **application-identification**—Clear IDP application identification data.
- **application-statistics**—Clear IDP application statistics.
- **attack**—Clear IDP attack data
- **counters**—Clear IDP counters
- **status**—Clear IDP Status

**Required Privilege Level** clear

**Related Documentation**
- IDP Policies for Security Devices

**List of Sample Output** clear security idp status on page 1434

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security idp status

```
user@host> clear security idp status
State of IDP: 2-default, Up since: 2010-02-04 13:37:16 UTC (17:13:45 ago)

Packets/second: 0 Peak: 0 @ 2010-02-05 06:49:51 UTC
KBits/second: 0 Peak: 0 @ 2010-02-05 06:49:51 UTC
Latency (microseconds): [min: 0] [max: 0] [avg: 0]

Packet Statistics:
 [ICMP: 0] [TCP: 0] [UDP: 0] [Other: 0]

Flow Statistics:
  ICMP: [Current: 0] [Max: 0 @ 2010-02-05 06:49:51 UTC]
  TCP: [Current: 0] [Max: 0 @ 2010-02-05 06:49:51 UTC]
  UDP: [Current: 0] [Max: 0 @ 2010-02-05 06:49:51 UTC]
  Other: [Current: 0] [Max: 0 @ 2010-02-05 06:49:51 UTC]

Session Statistics:
 [ICMP: 0] [TCP: 0] [UDP: 0] [Other: 0]
  Policy Name: sample
  Running Detector Version: 10.4.160091104
```


Copyright © 2013, Juniper Networks, Inc.

## clear security idp application-ddos cache

**Syntax** **clear security idp application-ddos cache**

**Release Information** Command introduced in Release 10.1 of Junos OS.

**Description** Clear application-level distributed denial-of-service (DDOS) state including context, context value, and client classification.

**Required Privilege Level** clear

**Related Documentation**

- show security idp application-ddos application on page 2008
- Application-Level Distributed Denial of Service
- IDP Policies for Security Devices

**Output Fields** This command produces no output.

Copyright © 2013, Juniper Networks, Inc.

## clear security idp attack table

**Syntax** clear security idp attack table

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Clear details of the IDP attack table.

**Required Privilege Level** clear

**Related Documentation**
- show security idp attack table on page 2013
- IDP Policies for Security Devices

**Output Fields** This command produces no output.


Copyright © 2013, Juniper Networks, Inc.

## clear security idp counters application-identification

**Syntax** clear security idp counters application-identification

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Reset all the application identification counter values.

**Required Privilege Level** clear

**Related Documentation**
- application-identification on page 413
- show security idp counters application-identification on page 2017
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

**List of Sample Output** clear security idp counters application-identification on page 1437

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security idp counters application-identification

```
user@host> clear security idp counters application-identification
clear_counter_class: counters cleared, status = 0
```

## clear security idp counters dfa

**Syntax** clear security idp counters dfa

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Reset all the DFA counter values.

**Required Privilege Level** clear

**Related Documentation**
- show security idp counters dfa on page 2019
- IDP Policies for Security Devices

**List of Sample Output** clear security idp counters dfa on page 1438

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security idp counters dfa

```
user@host> clear security idp counters dfa
clear_counter_class: counters cleared, status = 0
```


Copyright © 2013, Juniper Networks, Inc.

## clear security idp counters flow

**Syntax** clear security idp counters flow

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Reset all the IDP flow-related counter values.

**Required Privilege Level** clear

**Related Documentation**
- flow (Security IDP) on page 597
- show security idp counters flow on page 2020
- IDP Policies for Security Devices

**List of Sample Output** clear security idp counters flow on page 1439

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security idp counters flow

```
user@host> clear security idp counters dfa
clear_counter_class: counters cleared, status = 0
```

## clear security idp counters http-decoder

**Syntax** clear security idp counters http-decoder

**Release Information** Command introduced in Release 11.2 of Junos OS.

**Description** Reset all the HTTP decoder counter values.

**Required Privilege Level** clear

**Related Documentation**
- show security idp counters http-decoder on page 2023
- IDP Policies for Security Devices

**List of Sample Output** clear security idp counters http-decoder on page 1440

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security idp counters http-decoder

```
user@host> clear security idp counters http
```


Copyright © 2013, Juniper Networks, Inc.

## clear security idp counters ips

**Syntax** clear security idp counters ips

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Reset all the ips counter values.

**Required Privilege Level** clear

**Related Documentation**
- ips on page 698
- show security idp counters ips on page 2024
- IDP Policies for Security Devices

**List of Sample Output** clear security idp counters ips on page 1441

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security idp counters ips

```
user@host> clear security idp counters ips
clear_counter_class: counters cleared, status = 0
```

# clear security idp counters log

**Syntax** clear security idp counters log

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Reset all the IDP log counter values.

**Required Privilege Level** clear

**Related Documentation**
- event-rate on page 566
- show security idp counters log on page 2027
- IDP Policies for Security Devices

**List of Sample Output** clear security idp counters log on page 1442

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

## Sample Output

clear security idp counters log

```
user@host> clear security idp counters log
clear_counter_class: counters cleared, status = 0
```


Copyright © 2013, Juniper Networks, Inc.

## clear security idp counters packet

**Syntax** clear security idp counters packet

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Reset all the IDP packet counter values.

**Required Privilege Level** clear

**Related Documentation**
- show security idp counters packet on page 2030
- IDP Policies for Security Devices

**List of Sample Output** clear security idp counters packet on page 1443

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security idp counters packet

```
user@host> clear security idp counters packet
clear_counter_class: counters cleared, status = 0
```

Copyright © 2013, Juniper Networks, Inc.

## clear security idp counters policy-manager

**Syntax** clear security idp counters policy-manager

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Reset all the IDP policies counter values.

**Required Privilege Level** clear

**Related Documentation**
- show security idp counters policy-manager on page 2035
- IDP Policies for Security Devices

**List of Sample Output** clear security idp counters policy-manager on page 1444

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security idp counters policy-manager

```
user@host> clear security idp counters policy-manager
clear_counter_class: counters cleared, status = 0
```


Copyright © 2013, Juniper Networks, Inc.

## clear security idp counters tcp-reassembler

**Syntax** clear security idp counters tcp-reassembler

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Reset all the TCP reassembler counter values.

**Required Privilege Level** clear

**Related Documentation**
- re-assembler on page 873
- show security idp counters tcp-reassembler on page 2036
- IDP Policies for Security Devices

**List of Sample Output** clear security idp counters tcp-reassembler on page 1445

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security idp counters tcp-reassembler

```
user@host> clear security idp counters tcp-reassembler
clear_counter_class: counters cleared, status = 0
```

Copyright © 2013, Juniper Networks, Inc.

## clear security idp ssl-inspection session-id-cache

**Syntax** clear security idp ssl-inspection session-id-cache

**Release Information** Command introduced in Release 9.3 of Junos OS.

**Description** Clear all the entries stored in the SSL session ID cache.

**Required Privilege Level** clear

**Related Documentation**
- show security idp ssl-inspection session-id-cache on page 2050
- IDP Policies for Security Devices

**List of Sample Output** clear security idp ssl-inspection session-id-cache on page 1446

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security idp ssl-inspection session-id-cache

```
user@host> clear security idp ssl-inspection session-id-cache
Total SSL session cache entries cleared : 2
```


Copyright © 2013, Juniper Networks, Inc.

## clear security ike respond-bad-spi-count

**Syntax** clear security ike respond-bad-spi-count
< *gateway-name* >

**Release Information** Command introduced in Release 8.5 of Junos OS.

**Description** Clear information about invalid Internet Key Exchange (IKE) security parameter index (SPI) counters.

**Options**
- none—Clear all invalid SPI counters.
- ***gateway-name*** —(Optional) Clear the invalid SPI counters for the given gateway.

**Required Privilege Level** clear

**Related Documentation**
- respond-bad-spi on page 885

**List of Sample Output**
clear security ike respond-bad-spi-count on page 1447
clear security ike respond-bad-spi-count gateway-name1 on page 1447

**Output Fields** This command produces no output.

### Sample Output

clear security ike respond-bad-spi-count

```
user@host> clear security ike respond-bad-spi-count
```

### Sample Output

clear security ike respond-bad-spi-count gateway-name1

```
user@host> clear security ike respond-bad-spi-count gateway-name1
```

Copyright © 2013, Juniper Networks, Inc.

## clear security ike security-associations

**Syntax**

clear security ike security-associations
< *peer-address* >
< **port** >
<fpc *slot-number*>
<index *SA-index-number*>
<kmd-instance (all | *kmd-instance-name*)>
<pic *slot-number*>
port
<family (inet | inet6)>

**Release Information**

Command introduced in Release 8.5 of Junos OS. The **fpc, pic,** and **kmd-instance** options added in Release 9.3 of Junos OS. The **port** option added in Release 10.0 of Junos OS. The **family** option added in Release 11.1 of Junos OS.

**Description**

Clear information about the current Internet Key Exchange security associations (IKE SAs). For IKEv2, the device clears the information about the IKE SAs and the associated IPSec SA.

**Options**

- none—Clear all IKE SAs.
- ***peer-address*** —(Optional) Clear IKE SAs for the destination peer at this IP address.
- **fpc** ***slot-number*** —Specific to SRX Series devices. Clear information about existing IKE SAs in this Flexible PIC Concentrator (FPC) slot.
- **index** ***SA-index-number*** —(Optional) Clear the IKE SA with this index number.
- **port**—(Optional) Port number of SA (1 through 65,535).
- **kmd-instance**—Specific to SRX Series devices. Clear information about existing IKE SAs in the key management process (the daemon, which in this case is KMD) identified by FPC ***slot-number*** and PIC ***slot-number***.
  - **all**—All KMD instances running on the Services Processing Unit (SPU).
  - ***kmd-instance-name***—Name of the KMD instance running on the SPU.
- **pic** ***slot-number*** —Specific to SRX Series devices. Clear information about existing IKE SAs in this PIC slot.
- **family**—(Optional) Clear IKE SAs by family.
  - **inet**—IPv4 address family.
  - **inet6**—IPv6 address family.

**Required Privilege Level**

clear

**Related Documentation**

- show security ike security-associations on page 2059


Copyright © 2013, Juniper Networks, Inc.

List of Sample Output
clear security ike security-associations on page 1449
clear security ike security-associations 1.1.1.2 port 19405 on page 1449
clear security ike security-associations index 8 on page 1449
clear security ike security-associations family inet6 on page 1449
clear security ike security-associations fpc 5 pic 0 kmd-instance all (SRX Series Devices) on page 1449

Output Fields
This command produces no output.

## Sample Output

clear security ike security-associations

```
user@host> clear security ike security-associations
```

## Sample Output

clear security ike security-associations 1.1.1.2 port 19405

```
user@host> clear security ike security-associations 1.1.1.2 port 19405
```

## Sample Output

clear security ike security-associations index 8

```
user@host> clear security ike security-associations index 8
```

## Sample Output

clear security ike security-associations family inet6

```
user@host> clear security ike security-associations family inet6
```

## Sample Output

clear security ike security-associations fpc 5 pic 0 kmd-instance all (SRX Series Devices)

```
user@host> clear security ike security-associations fpc 5 pic 0 kmd-instance all
```

Copyright © 2013, Juniper Networks, Inc.

## clear security ipsec security-associations

**Syntax**

clear security ipsec security-associations
fpc *slot-number*
<index *SA-index-number*>
kmd-instance (all | *kmd-instance-name* )
pic *slot-number*
<family (inet | inet6)>

**Release Information**

Command introduced in Release 8.5 of Junos OS. The **fpc**, **pic,** and **kmd-instance** options added in Release 9.3 of Junos OS. The **family** option added in Release 11.1 of Junos OS.

**Description**

Clear information about IPsec security associations (SAs).

**Options**

- none—Clear all IPsec SAs.
- **fpc** *slot-number* —Specific to SRX Series devices. Clear information about existing IPsec SAs in this Flexible PIC Concentrator (FPC) slot.
- **index** *SA-index-number* —(Optional) Clear the IPsec SA with this index number.
- **kmd-instance**—Specific to SRX Series devices. Clear information about existing IPsec SAs in the key management process (the daemon, which in this case is KMD) identified by FPC *slot-number* and PIC *slot-number* .
  - **all**—All KMD instances running on the Services Processing Unit (SPU).
  - ***kmd-instance-name***—Name of the KMD instance running on the SPU.

**pic** *slot-number* —Specific to SRX Series devices. Clear information about existing IPsec SAs in this PIC slot.

**family**—(Optional) Clear SAs by family.

- **inet**—IPv4 address family.
- **inet6**—IPv6 address family.

**Required Privilege Level**

clear

**Related Documentation**

- show security ipsec security-associations on page 2071

**List of Sample Output**

clear security ipsec security-associations on page 1451
clear security ipsec security-associations index 8 on page 1451
clear security ipsec security-associations family inet6 on page 1451

**Output Fields**

This command produces no output.


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

clear security ipsec security-associations

```
user@host> clear security ipsec security-associations
```

## Sample Output

clear security ipsec security-associations index 8

```
user@host> clear security ipsec security-associations index 8
```

## Sample Output

clear security ipsec security-associations family inet6

```
user@host> clear security ipsec security-associations family inet6
```

Copyright © 2013, Juniper Networks, Inc.

## clear security ipsec statistics

**Syntax**

clear security ike statistics
<fpc *slot-number*>
<index *SA-index-number*>
<kmd-instance (all | *kmd-instance-name* )>
<pic *slot-number*>

**Release Information**

Command introduced in Release 8.5 of Junos OS; **fpc and pic** options added in Release 9.3 of Junos OS ;**kmd-instance** option added in Release 10.4 of Junos OS.

**Description**

Clear IPsec statistics on the device.

**Options**

- none—Clear all IPsec statistics.
- **fpc** *slot-number* —Specific to SRX Series devices. Clear statistics about existing IPsec security associations (SAs) in this Flexible PIC Concentrator (FPC) slot.
- **index** *SA-index-number* —(Optional) Clear the IPsec statistics for the SA with this index number.
- **kmd-instance**—Specific to SRX Series devices. Clear information about existing IKE SAs in the key management process (the daemon, which in this case is KMD) identified by FPC *slot-number* and PIC *slot-number* .
  - **all**—All KMD instances running on the Services Processing Unit (SPU).
  - ***kmd-instance-name***—Name of the KMD instance running on the SPU.
- **pic** *slot-number* —Specific to SRX Series devices. Clear statistics about existing IPsec SAs in this PIC slot.

**Required Privilege Level**

clear

**Related Documentation**

- show security ipsec statistics on page 2079

**List of Sample Output**

clear security ipsec statistics on page 1453
clear security ipsec statistics index 1 on page 1453
clear security ipsec statistics fpc 5 pic 0 (SRX Series devices) on page 1453

**Output Fields**

This command produces no output.


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

clear security ipsec statistics

```
user@host> clear security ipsec statistics
```

## Sample Output

clear security ipsec statistics index 1

```
user@host> clear security ipsec statistics index 1
```

## Sample Output

clear security ipsec statistics fpc 5 pic 0 (SRX Series devices)

```
user@host> clear security ipsec statistics fpc 5 pic 0
```

Copyright © 2013, Juniper Networks, Inc.

## clear security log

**Syntax** clear security log
<*all*>
<*destination-address*>
<*destination-port*>
<*event-id*>
<*failure*>
<*interface-name*>
<*newer-than*>
<*older--than*>
<*process*>
<*protocol*>
<*severity*>
<*source-address*>
<*source-port*>
<*success*>
<*username*>

**Release Information** Command introduced in Release 11.2 of Junos OS.

**Description** Deletes the event log.

**Options** **all**—Clears all audit event logs stored in the device memory.

**destination-address**—Clears audit event logs with the specified destination address.

**destination-port**—Clears audit event logs with the specified destination port.

**event-id**—Clears audit event logs with the specified event identification number.

**failure**—Clears failed audit event logs.

**interface-name**—Clears audit event logs with the specified interface.

**newer-than**—Clears audit event logs newer than the specified date and time.

**older-than**—Clears audit event logs older than the specified date and time

**process**—Clears audit event logs with the specified process that generated the event.

**protocol**—Clears audit event logs generated through the specified protocol.

**severity**—Clears audit event logs generated with the specified severity.

**source-address**—Clears audit event logs with the specified source address.

**source-port**—Clears audit event logs with the specified source port.

**success**—Clears successful audit event logs.

**username**—Clears audit event logs generated for the specified user.


Copyright © 2013, Juniper Networks, Inc.

**Required Privilege Level** clear

**Related Documentation**

- exclude (Security Log) on page 568
- show security log on page 2082
- System Log Messages
- Security Logs
- CLI Statements and Commands

## Sample Output

clear security log all

```
user@host> clear security log all
7905 security log events cleared
```

## clear security log file

**Syntax** clear security log file

**Release Information** Command introduced in Release 12.1 of Junos OS.

**Description** Deletes the content of an event mode security log file stored on the device in binary format.

**Required Privilege Level** clear

**Related Documentation**

- show security log file on page 2086
- System Log Messages
- Security Logs
- CLI Statements and Commands

### Sample Output

clear security log file

```
user@host> clear security log file
7905 security log events cleared
```


Copyright © 2013, Juniper Networks, Inc.

## clear security nat incoming-table

**Syntax** clear security nat incoming-table
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Junos OS Release 8.5. The **node** options added in Junos OS Release 9.0.

**Description** Clear Network Address Translation (NAT) incoming table information.

**Options**

- none—Clear all information NAT incoming table.
- **node**—(Optional) For chassis cluster configurations, clear incoming table information on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level** clear

**Related Documentation**

- show security nat incoming-table on page 2107
- Network Address Translation for Security Devices

**List of Sample Output** clear security nat incoming-table on page 1457

**Output Fields** This command produces no output.

### Sample Output

clear security nat incoming-table

```
user@host> clear security nat incoming-table
```

## clear security nat source persistent-nat-table

**Syntax** clear security nat source persistent-nat-table
( all | interface | internal-ip *ip-address* <internal-port *port*> | pool *poolname* )

**Release Information** Command introduced in Junos OS Release 10.0.

**Description** Clear Network Address Translation (NAT) persistent NAT bindings that are in query mode, where all sessions of the binding are gone.

**Options**

- **all**—Clear all persistent NAT bindings that are in query mode.
- **interface**—Clear persistent NAT bindings that are in query mode for the specified interface.
- **internal-ip *ip-address***—Clear persistent NAT bindings for the specified internal IP address.
- **internal-ip *ip-address* internal-port *port***—Clear persistent NAT bindings that are in query mode for the specified internal IP address and port.
- **pool**—Clear persistent NAT bindings that are in query mode for the specified source NAT pool.

**Required Privilege Level** clear

**Related Documentation**

- show security nat source persistent-nat-table on page 2111
- Network Address Translation for Security Devices

**List of Sample Output** clear security nat source persistent-nat-table all on page 1458

**Output Fields** This command produces no output.

### Sample Output

clear security nat source persistent-nat-table all

```
user@host> clear security nat source persistent-nat-table all
```


Copyright © 2013, Juniper Networks, Inc.

## clear security nat statistics destination pool

**Syntax**

clear security nat statistics destination pool
<*pool-name*>
all

**Release Information**

Command introduced in Junos OS Release 11.1.

**Description**

Clear the destination NAT pool information.

**Options**

*pool-name*—Clear specified destination nat pool information.

*all*—Clear all destination nat pool information.

**Required Privilege Level**

clear

**Related Documentation**

- show security nat destination pool on page 2100
- show security nat destination summary on page 2105
- Network Address Translation for Security Devices

**List of Sample Output**

clear security nat statistics destination pool on page 1459

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security nat statistics destination pool

```
user@host>clear security nat statistics destination pool all
This command produces no output.
```

Copyright © 2013, Juniper Networks, Inc.

## clear security nat statistics destination rule

**Syntax**

clear security nat statistics destination rule
<rule-name>
alll

**Release Information**

Command introduced in Junos OS Release 11.1.

**Description**

Clear the destination NAT rule information.

**Options**

*rule-name*—Clear specified destination nat rule-set information.

*all*—Clear all destination nat rule-set information.

**Required Privilege Level**

clear

**Related Documentation**

- show security nat destination rule on page 2102
- show security nat destination summary on page 2105
- Network Address Translation for Security Devices

**List of Sample Output**

clear security nat statistics destination rule on page 1460

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security nat statistics destination rule

```
user@host> clear security nat statistics destination rule all
This command produces no output.
```


Copyright © 2013, Juniper Networks, Inc.

## clear security nat statistics source pool

**Syntax**
clear security nat statistics source pool
<*pool-name*>
all

**Release Information**
Command introduced in Junos OS Release 11.1.

**Description**
Clear the source NAT statistic pool information.

**Options**
*pool-name*—Clear the specified source nat pool information.

*all*—Clear all source pool information.

**Required Privilege Level**
clear

**Related Documentation**
- show security nat source pool on page 2114
- show security nat source summary on page 2121
- Network Address Translation for Security Devices

**List of Sample Output**
clear security nat statistics source pool on page 1461

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security nat statistics source pool

```
user@host>clear security nat statistics source pool all
This command produces no output.
```

Copyright © 2013, Juniper Networks, Inc.

## clear security nat statistics source rule

**Syntax**

clear security nat statistics source rule
<*rule-name*>
all

**Release Information**

Command introduced in Junos OS Release 11.1.

**Description**

Clear the source NAT statistic rule-set information.

**Options**

*rule-name*—Clear the specified source rule-set information.

*all*—Clear all source nat rule-set information.

**Required Privilege Level**

clear

**Related Documentation**

- show security nat source summary on page 2121
- show security nat source rule on page 2118
- Network Address Translation for Security Devices

**List of Sample Output**

clear security nat statistics source rule on page 1462

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security nat statistics source rule

```
user@host>clear security nat statistics source rule all
This command produces no output.
```


Copyright © 2013, Juniper Networks, Inc.

## clear security nat statistics static rule

**Syntax**
clear security nat statistics static rule
<*rule-name*>
all

**Release Information**
Command introduced in Junos OS Release 11.1.

**Description**
Clear the static NAT rule-set information.

**Options**
*rule-name*—Clear specified static nat rule-set information.

*all*—Clear all static nat rule-set information.

**Required Privilege Level**
clear

**Related Documentation**
- show security nat static rule on page 2123
- Network Address Translation for Security Devices

**List of Sample Output**
clear security nat statistics static rule on page 1463

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security nat statistics static rule

```
user@host>clear security nat statistics static rule all
This command produces no output.
```

Copyright © 2013, Juniper Networks, Inc.

## clear security pki key-pair (Local Certificate)

**Syntax** clear security pki key-pair (all | certificate-id *certificate-id* )

**Release Information** Command introduced in Release 8.5 of Junos OS.

**Description** Clear public key infrastructure (PKI) key pair information for local digital certificates on the device.

**Options**

- **all**—Clear key pair information for all local certificates.
- **certificate-id** *certificate-id* —Clear key pair information for the local certificate with this certificate ID.

**Required Privilege Level** clear and security

**Related Documentation**

- show security pki certificate-request (View) on page 2129

**List of Sample Output** clear security pki key-pair all on page 1464

**Output Fields** This command produces no output.

### Sample Output

clear security pki key-pair all

```
user@host> clear security pki key-pair all
```


Copyright © 2013, Juniper Networks, Inc.

## clear security pki local-certificate (Device)

**Syntax** clear security pki local-certificate (all | certificate-id *certificate-id* | system-generated)

**Release Information** Command modified in Release 9.1 of Junos OS.

**Description** Clear public key infrastructure (PKI) information for local digital certificates on the device.

**Options**

- **all**—Clear information for all the local digital certificates on the device.

  NOTE: You cannot clear the automatically generated self-signed certificate using **clear security pki local-certificate all** command. To clear the self-signed certificate you need to use **system-generated** as an option.

- **certificate-id** *certificate-id* —Clear the specified local digital certificate with this certificate ID.
- **system-generated**—Clear the existing automatically generated self-signed certificate and generate a new self-signed certificate.

**Required Privilege Level** clear and security

**Related Documentation**

- show security pki local-certificate (View) on page 2134
- request security pki local-certificate generate-self-signed (Security) on page 1514

**List of Sample Output**

clear security pki local-certificate all on page 1465
clear security pki local-certificate system-generated on page 1465

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security pki local-certificate all

```
user@host> clear security pki local-certificate all
```

### Sample Output

clear security pki local-certificate system-generated

```
user@host> clear security pki local-certificate system-generated
```

Copyright © 2013, Juniper Networks, Inc.

## clear security policies hit-count

**Syntax**

clear security policies hit-count
<from-zone *zone-name*>
<to-zone *zone-name*>

**Release Information**

Command introduced in Junos Release 12.1.

**Description**

Clear the hit-count values for security policies.

**Options**

- **from-zone** ***zone-name***—(Optional) Clear the number of hits for security policies associated with the named source zone.
- **to-zone** ***zone-name***—(Optional) Clear the number of hits for security policies associated with the named destination zone.

**Required Privilege Level**

clear

**Related Documentation**

- show security policies hit-count on page 2145
- Security Policies for Security Devices

**Output Fields**

This command produces no output.


Copyright © 2013, Juniper Networks, Inc.

## clear security policies statistics

**Syntax** clear security policies statistics

**Release Information** Command introduced in Junos OS Release 8.5.

**Description** Clear statistics for security policies configured on the device.

**Required Privilege Level** clear

**Related Documentation**
- show security policies on page 2139
- Security Policies for Security Devices

**List of Sample Output** clear security policies statistics on page 1467

**Output Fields** This command produces no output.

### Sample Output

clear security policies statistics

```
user@host> clear security policies statistics
```

## clear security screen statistics

**Syntax**
clear security screen statistics
<node ( *node-id* | all | local | primary)>

**Release Information**
Command introduced in Release 9.0 of Junos OS.

**Description**
Clear intrusion detection service (IDS) security screen statistics on the device.

**Options**
**node**—(Optional) For chassis cluster configurations, clear security screen statistics on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all** —Clear all nodes.
- **local** —Clear the local node.
- **primary**—Clear the primary node.

**Required Privilege Level**
clear

**Related Documentation**
- show security screen statistics on page 2159

**List of Sample Output**
clear security screen statistics node 0 on page 1468

**Output Fields**
This command produces no output.

### Sample Output

clear security screen statistics node 0

```
user@host> clear security screen statistics node 0
```


Copyright © 2013, Juniper Networks, Inc.

## clear security screen statistics interface

**Syntax** clear security screen statistics interface *interface-name*

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Clear intrusion detection service (IDS) security screen statistics for an interface.

**Options**

- **interface** ***interface-name*** —Name of the interface on which to clear security screen statistics.
- **node**—(Optional) For chassis cluster configurations, clear security screen statistics on a specific node.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level** clear

**Related Documentation**

- show security screen statistics on page 2159

**List of Sample Output**

clear security screen statistics interface fab0 on page 1469
clear security screen statistics interface fab0 node 0 on page 1469

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security screen statistics interface fab0

```
user@host> clear security screen statistics interface fab0
node0:
--------------------------------------------------------------------------
  IDS statistics has been cleared.
node1:
--------------------------------------------------------------------------
  IDS statistics has been cleared.
```

### Sample Output

clear security screen statistics interface fab0 node 0

```
user@host> clear security screen statistics interface fab0 node 0
node0:
--------------------------------------------------------------------------
  IDS statistics has been cleared.
```

Copyright © 2013, Juniper Networks, Inc.

## clear security screen statistics zone

**Syntax** clear security screen statistics zone *zone-name*
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Clear IDS security screen statistics for a security zone.

**Options**

- **zone** *zone-name* —Name of the security zone for which to clear security screen statistics.
- **node**—(Optional) For chassis cluster configurations, clear security screen statistics for a security zone on a specific node.
  - *node-id* —Identification number of the node. It can be 0 or 1.
  - **all** —Clear all nodes.
  - **local** —Clear the local node.
  - **primary**—Clear the primary node.

**Required Privilege Level** clear

**Related Documentation**

- show security screen statistics on page 2159

**List of Sample Output**

clear security screen statistics zone abc node all on page 1470
clear security screen statistics node 0 zone my-zone on page 1470

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear security screen statistics zone abc node all

```
user@host> clear security screen statistics zone abc node all
node0:
--------------------------------------------------------------------------
  IDS statistics has been cleared.
node1:
--------------------------------------------------------------------------
  IDS statistics has been cleared.
```

### Sample Output

clear security screen statistics node 0 zone my-zone

```
user@host> clear security screen statistics node 0 zone my-zone
node0:
--------------------------------------------------------------------------
  IDS statistics has been cleared.
```


Copyright © 2013, Juniper Networks, Inc.

## clear security user-identification local-authentication-table

**Syntax** clear security user-identification local-authentication-table

**Release Information** Command introduced in release 12.1 of Junos OS.

**Description** This command removes all entries from the local authentication table.

**Required Privilege Level** clear

**Related Documentation**
- request security user-identification local-authorization-table add on page 1519
- request security user-identification local-authentication-table delete on page 1521
- Understanding the User Identification Table

**List of Sample Output** clear security user-identification local-authentication-table on page 1471

**Output Fields** When you enter this command, all entries are cleared from the local authentication table.

### Sample Output

clear security user-identification local-authentication-table

```
user@host> clear security user-identification local-authentication-table
user@host> show security user-identification local-authentication-table all
Total entries: 0
```

Copyright © 2013, Juniper Networks, Inc.

## clear security utm anti-spam statistics

**Syntax** clear security utm anti-spam statistics

**Release Information** Command introduced in Release 9.5 of Junos OS. Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Clear antispam statistics information. With chassis cluster support for UTM, statistics from both the nodes is cleared.

**Required Privilege Level** clear

**Related Documentation**

- show security utm anti-spam statistics on page 2174
- show security utm anti-spam status on page 2175
- UTM for Security Devices

**Output Fields** This command produces no output.

### Sample Output

clear security utm anti-spam statistics

```
user@host> clear security utm anti-spam statistics
```


Copyright © 2013, Juniper Networks, Inc.

## clear security utm antivirus statistics

**Syntax** clear security utm anti-virus statistics

**Release Information** Command introduced in Release 9.5 of Junos OS. Support for Sophos Antivirus added in Release 11.1 of Junos OS.
Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Clear antivirus statistics information. With chassis cluster support for UTM, statistics from both the nodes is cleared.

**Required Privilege Level** clear

**Related Documentation**

- show security utm anti-virus statistics on page 2176
- show security utm anti-virus status on page 2178
- request security utm anti-virus juniper-express-engine on page 1522
- request security utm anti-virus kaspersky-lab-engine on page 1523
- UTM for Security Devices
- Unified Threat Management
- UTM Express Antivirus Protection for Security Devices

**Output Fields** This command produces no output.

### Sample Output

clear security utm antivirus statistics

```
user@host> clear security utm anti-virus statistics
```

## clear security utm content-filtering statistics

**Syntax** clear security utm content-filtering statistics

**Release Information** Command introduced in Release 9.5 of Junos OS.
Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Clear content-filtering statistics information. With chassis cluster support for UTM, statistics from both the nodes is cleared.

**Required Privilege Level** clear

**Related Documentation**
- show security utm content-filtering statistics on page 2180

**Output Fields** This command produces no output.

### Sample Output

clear security utm content-filtering statistics

```
user@host> clear security utm content-filtering statistics
```


Copyright © 2013, Juniper Networks, Inc.

## clear security utm session

**Syntax** clear security utm session

**Release Information** Command introduced in Release 9.5 of Junos OS.
Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Clears UTM session information. With chassis cluster support for UTM, sessions on both the nodes is cleared.

**Required Privilege Level** clear

**Related Documentation**

- show security utm session on page 2181
- show security utm status on page 2182
- UTM for Security Devices
- Unified Threat Management

**Output Fields** This command produces no output.

### Sample Output

clear security utm session

```
user@host> clear security utm session
```

Copyright © 2013, Juniper Networks, Inc.

## clear security utm web-filtering statistics

**Syntax** clear security utm web-filtering statistics

**Release Information** Command introduced in Release 9.5 of Junos OS.
Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Clear web filtering statistics information. With chassis cluster support for UTM, statistics from both the nodes is cleared.

**Required Privilege Level** clear

**Related Documentation**

- show security utm web-filtering statistics on page 2183
- show security utm web-filtering status on page 2185
- Unified Threat Management
- UTM for Security Devices

**Output Fields** This command produces no output.

### Sample Output

clear security utm web-filtering statistics

```
user@host> clear security utm web-filtering statistics
```


Copyright © 2013, Juniper Networks, Inc.

## clear services application-identification application-statistics

**Syntax** clear services application-identification application-statistics

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Clears all Junos OS application statistics such as cumulative, interval, applications, and application groups.

**Required Privilege Level** clear

**Related Documentation**

- Application Identification for Security Devices
- show services application-identification statistics applications on page 2210
- show services application-identification statistics application-groups on page 2212
- clear services application-identification application-statistics interval on page 1479
- clear services application-identification application-statistics cumulative on page 1478

**Output Fields** This command produces no output.

Copyright © 2013, Juniper Networks, Inc.

## clear services application-identification application-statistics cumulative

**Syntax** clear services application-identification application-statistics cumulative

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Clear all Junos OS application cumulative statistics.

**Required Privilege Level** clear

**Related Documentation**

- Application Identification for Security Devices
- show services application-identification statistics applications on page 2210
- show services application-identification statistics application-groups on page 2212
- clear services application-identification application-statistics on page 1477
- clear services application-identification application-statistics interval on page 1479

**Output Fields** This command produces no output.


Copyright © 2013, Juniper Networks, Inc.

## clear services application-identification application-statistics interval

**Syntax** clear services application-identification application-statistics interval

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Clear all Junos OS application interval statistics.

**Required Privilege Level** clear

**Related Documentation**

- Application Identification for Security Devices
- show services application-identification statistics applications on page 2210
- show services application-identification statistics application-groups on page 2212
- clear services application-identification application-statistics on page 1477
- clear services application-identification application-statistics cumulative on page 1478

**Output Fields** This command produces no output.

Copyright © 2013, Juniper Networks, Inc.

## clear services application-identification application-system-cache (Junos OS)

**Syntax** clear services application-identification application-system-cache
<node ( *node-id* | all | local | primary ) >

**Release Information** Command introduced in Release 10.2 of Junos OS. Command syntax updated in Release 12.1 of Junos OS.

**Description** Clear Junos OS application identification application system cache.

**Options**

- none—Clear the application system cache on the device.
- **node**—(Optional) For chassis cluster configurations, clear application system cache on the specified nodes.
  - ***node-id***—Specific node number
  - **all**—All nodes
  - **local**—Local node
  - **primary**—Primary node

**Required Privilege Level** clear

**Related Documentation**

- Application Identification for Security Devices
- show services application-identification application-system-cache (View) on page 2202

**List of Sample Output**

clear services application-identification application-system-cache on page 1480
clear services application-identification application-system-cache node primary on page 1480

**Output Fields** This command produces no output.

### Sample Output

clear services application-identification application-system-cache

```
user@host> clear services application-identification application-system-cache
```

clear services application-identification application-system-cache node primary

```
user@host> clear services application-identification application-system-cache node primary
```


Copyright © 2013, Juniper Networks, Inc.

## clear services application-identification counter (Values)

**Syntax** clear services application-identification counter

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Reset all the Junos OS application identification counter values.

**Required Privilege Level** clear

**Related Documentation**
- Application Identification for Security Devices
- show services application-identification counter (AppSecure) on page 2204

**List of Sample Output** clear services application-identification counter on page 1481

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

clear services application-identification counter

```
user@host> clear services application-identification counter
clear_counter_class: counters cleared, status = 0
```

## clear services application-identification counter ssl-encrypted-sessions

**Syntax** clear services application-identification counter ssl-encrypted-sessions

**Release Information** Command introduced in Release 12.1 of Junos OS

**Description** Reset all counter values for application identification SSL-encrypted counters.

**Required Privilege Level** clear

**Related Documentation**
- Application Identification for Security Devices

**Output Fields** This command produces no output.


Copyright © 2013, Juniper Networks, Inc.

## clear services ssl proxy statistics

**Syntax** **clear services ssl proxy statistics**

**Release Information** Command introduced in Release 12.1 of Junos OS.

**Description** Clear services SSL proxy statistics.

**Options** **none**—Clear the ssl proxy statistics.

**Required Privilege Level** clear

**Related Documentation**
- show services ssl proxy statistics on page 2223

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

**clear services ssl proxy statistics**

```
user@host> clear services ssl proxy statistics
```

Copyright © 2013, Juniper Networks, Inc.

## clear system login lockout

**Syntax**
clear system login lockout
<*all*>
<*username*>

**Release Information**
Command introduced in Release 11.2 of Junos OS.

**Description**
Unlock the user account locked as a result of invalid login attempts.

**Options**
**<*all*>**—Clear all locked user accounts.

**<*username*>**—Clear the specified locked user account.

**Required Privilege Level**
clear

**Related Documentation**
- lockout-period
- show system login lockout on page 2262
- Device Configuration

**Output Fields**
This command produces no output.


Copyright © 2013, Juniper Networks, Inc.

## clear system services dns dns-proxy

**Syntax** clear system services dns dns-proxy

**Release Information** Command introduced in Junos OS Release 12.1X44-D10.

**Description** Clear DNS proxy cache information.

**Options**

- **cache**—Clear DNS proxy cache information.
- **statistics**—Clear DNS proxy statistics.
- **none**—Clear all DNS proxy cache information.
- **hostname**—(Optional) Clear DNS proxy cache information from the specified host.

**Required Privilege Level** clear

**Related Documentation**

- show system services dns dns-proxy

**List of Sample Output** clear system services dns-proxy on page 1485

**Output Fields** When you enter this command no output is produced.

### Sample Output

clear system services dns-proxy

```
user@host> clear system services dns dns-proxy cache
user@host> clear system services dns dns-proxy statistics
```

Copyright © 2013, Juniper Networks, Inc.

## clear wlan access-point neighbors

**Syntax** clear wlan access-point neighbors *ap-name*

**Release Information** Command introduced in Release 10.3 of Junos OS.

**Description** Clear all entries (stale and current) from the list of access-point neighbors on a specified wireless LAN access point.

**Required Privilege Level** clear

**Related Documentation**
- show wlan access-points on page 2273
- WLAN Configuration and Administration

**Output Fields** This command produces no output.


Copyright © 2013, Juniper Networks, Inc.

CHAPTER 26

# Request Commands

This section contains the following topics:


- Request Commands Overview on page 1487


## Request Commands Overview

Use the **request** operational commands to stop or reboot device components, switch between primary and backup components, display messages, and display system information. Operational commands are organized alphabetically.

**Related Documentation**

- Junos OS Operational Mode Commands.
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

Copyright © 2013, Juniper Networks, Inc.

## request chassis cluster failover node

**Syntax** request chassis cluster failover node *node-number*
redundancy-group *group-number*

**Release Information** Command introduced in Release 9.0 of Junos OS.

**Description** For chassis cluster configurations, initiate manual failover in a redundancy group from one node to the other, which becomes the primary node, and automatically reset the priority of the group to 255. The failover stays in effect until the new primary node becomes unavailable, the threshold of the redundancy group reaches 0, or you use the **request chassis cluster failover reset** command.

After a manual failover, you must use the **request chassis cluster failover reset** command before initiating another failover.

**Options**

- **node** *node-number*-Number of the chassis cluster node to which the redundancy group fails over.
- **Range:** 0 through 1
- **redundancy-group** *group-number* —Number of the redundancy group on which to initiate manual failover. Redundancy group 0 is a special group consisting of the two Routing Engines in the chassis cluster.

  **Range:** 0 through 255

**Required Privilege Level** maintenance

**Related Documentation**

- Chassis Cluster for Security Devices
- clear chassis cluster failover-count on page 1360
- request chassis cluster failover reset on page 1489
- show chassis cluster status on page 1598

**List of Sample Output** request chassis cluster failover node 0 redundancy-group 1 on page 1488

**Output Fields** This command produces no output.

### Sample Output

request chassis cluster failover node 0 redundancy-group 1

```
user@host> request chassis cluster failover node 0 redundancy-group 1
```


Copyright © 2013, Juniper Networks, Inc.

## request chassis cluster failover reset

**Syntax** request chassis cluster failover reset
redundancy-group *group-number*

**Release Information** Command introduced in Release 9.0 of Junos OS.

**Description** In chassis cluster configurations, undo the previous manual failover and return the redundancy group to its original settings.

**Options** **redundancy-group** ***group-number*** —Number of the redundancy group on which to reset manual failover. Redundancy group 0 is a special group consisting of the two Routing Engines in the chassis cluster.

**Range:** 0 through 255

**Required Privilege Level** maintenance

**Related Documentation**

- Chassis Cluster for Security Devices
- clear chassis cluster failover-count on page 1360
- request chassis cluster failover node on page 1488
- show chassis cluster status on page 1598

**List of Sample Output** request chassis cluster failover reset redundancy-group 0 on page 1489

**Output Fields** This command produces no output.

### Sample Output

request chassis cluster failover reset redundancy-group 0

```
user@host> request chassis cluster failover reset redundancy-group 0
```

## request chassis cluster in-service-upgrade abort (ISSU)

**Syntax** request chassis cluster in-service-upgrade abort

**Release Information** Command introduced in Junos OS Release 11.2.

**Description** Abort an upgrade in a chassis cluster during an in-service software upgrade (ISSU). Use this command to end the ISSU on any nodes in a chassis cluster followed by **reboot** to abort the ISSU on that device.

**Options** This command has no options.

**Required Privilege Level** view

**Related Documentation**
- request system software in-service-upgrade (Maintenance) on page 1551

**List of Sample Output** request chassis cluster in-service-upgrade abort on page 1490

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request chassis cluster in-service-upgrade abort

```
user@host> request chassis cluster in-service-upgrade abort
Exiting in-service-upgrade window
Chassis ISSU Aborted
```


Copyright © 2013, Juniper Networks, Inc.

## request dhcp client renew

**Syntax**
request dhcp client renew
[all|interface <interface-name>]
routing-instance <routing-instance-name>

**Release Information**
Statement introduced in Junos OS Release 12.1X44-D10.

**Description**
Initiates a renew request for the specified clients if they are in the bound state.

**Options**
**all**—Initiate renew requests for all DHCP clients. If you specify a routing instance, renew requests are initiated for all DHCP clients within that routing instance.

**interface <interface-name>**—Initiate renew requests for DHCP clients on the specified interface.

**routing-instance <routing-instance-name>**—Initiate renew requests for DHCP clients in the specified routing instance. If you do not specify a routing instance, renew requests are initiated on the default routing instance.

**Required Privilege Level**
view

**Related Documentation**
- Device Configuration

**Output Fields**
This command produces no output.

Copyright © 2013, Juniper Networks, Inc.

## request modem wireless activate iota

**Syntax** request modem wireless activate iota *interface-name*

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** For CDMA EV-DO 3G wireless modem interfaces, enable modem card to connect to service provider's cellular network using Internet-based over the air (IOTA) provisioning.

**Options** ***interface-name***—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.

**Required Privilege Level** maintenance

**Related Documentation**
- Modem Interfaces
- Interfaces for Security Devices

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request modem wireless activate iota cl-0/0/8

```
user@host> request modem wireless activate iota cl-0/0/8
Beginning IOTA Activation. It can take up to 5 minutes
Please check the trace logs for details.
```


Copyright © 2013, Juniper Networks, Inc.

## request modem wireless activate manual

**Syntax** request modem wireless activate manual *interface-name* msl *msl-number* mdn *mdn-number* imsi *imsi-number* sid *sid-number* nid *nid-number* sip-user-id *sip-id* sip-password *sip-password*

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** For CDMA EV-DO 3G wireless modem interfaces, enable modem card to connect to service provider's cellular network.

**Options**

- *interface-name*—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.
- **msl** *msl-number*—Master subsidy lock (MSL) number required to unlock the modem card. Obtain the number from the service provider.
- **mdn** *mdn-number*—Mobile directory number (MDN) 10–digit phone number. Obtain the number from the service provider.
- **imsi** *imsi-number*—International mobile station identity (IMSI) subscriber identification number. Obtain the number from the service provider.
- **sid** *sid-number*—System identification (SID) number. Use the **show modem wireless interface network** command to display the SID.
- **nid** *nid-number*—Network identification (NID) number. Use the **show modem wireless interface network** command to display the NID.
- **sip-user-id** *sip-id*—Simple IP user identification. Obtain the username from the service provider.
- **sip-password** *sip-password*—Simple IP password. Obtain the password from the service provider.

**Required Privilege Level** maintenance

**Related Documentation**

- show modem wireless interface network on page 1711
- Modem Interfaces
- Interfaces for Security Devices

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request modem wireless activate manual cl-0/0/8 msl 43210 mdn 0123456789 imsi 0123456789 sid 12345

```
user@host> request modem wireless activate manual cl-0/0/8 msl 43210 mdn 0123456789
imsi 0123456789 sid 12345 nid 12345 sip-usr-id jnpr sip-password jn9r1
Checking status...
 Modem current activation status: Not Activated
Starting activation...
 Performing account activation step 1/6 : [Unlock] Done
 Performing account activation step 2/6 : [Set MDN] Done
 Performing account activation step 3/6 : [Set SIP Info] Done
```

Copyright © 2013, Juniper Networks, Inc.

nid 12345 sip-usr-id jnpr sip-password jn9r1

```
 Performing account activation step 4/6 : [Set IMSI] Done
 Performing account activation step 5/6 : [Set SID/NID] Done
 Performing account activation step 6/6 : [Commit/Lock] Done
Configuration Commit Result: PASS
Resetting the modem ... Done
Account activation in progress. It can take up to 5 minutes
Please check the trace logs for details.
```


Copyright © 2013, Juniper Networks, Inc.

## request modem wireless activate otasp

**Syntax** request modem wireless activate otasp *interface-name* dial-string *calling-number*

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** For CDMA EV-DO 3G wireless modem interfaces, enable the modem card to connect to service provider's cellular network using over-the-air service provisioning (OTASP).

**Options**

- ***interface-name***—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.
- **dial-string *calling-number***—Dial number that the modem uses to contact the network. Obtain the number from the service provider.

**Required Privilege Level** maintenance

**Related Documentation**

- Modem Interfaces
- Interfaces for Security Devices

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request modem wireless activate otasp cl-0/0/8 dial-string *22864

```
user@host> request modem wireless activate otasp cl-0/0/8 dial-string *22864
OTASP number *22286*, Selecting NAM 0
Beginning OTASP Activation. It can take up to 5 minutes
Please check the trace logs for details.
```

Copyright © 2013, Juniper Networks, Inc.

## request modem wireless gsm sim-unblock

**Syntax** request modem wireless gsm sim-unblock *interface-name* puk *unblock-code*

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** Unblock a blocked subscriber identity module (SIM) in the GSM 3G wireless modem card.

**Options**

- ***interface-name***—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.
- **puk *unblock-code***—Eight-digit PIN unblocking key (PUK). Obtain the PUK from the service provider.



NOTE: If the PUK is entered incorrectly ten times, the SIM must be returned to the service provider for reactivation.

**Required Privilege Level** maintenance

**Related Documentation**

- request modem wireless gsm sim-unlock on page 1497
- Modem Interfaces
- Interfaces for Security Devices

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request modem wireless gsm sim-unblock cl-0/0/8 puk 76543210

```
user@host> request modem wireless gsm sim-unblock cl-0/0/8 puk 76543210
Issued SIM unblock request successfully.
Please verify SIM lock status under firmware stats
```


Copyright © 2013, Juniper Networks, Inc.

## request modem wireless gsm sim-unlock

**Syntax** request modem wireless gsm sim-unlock *interface-name* pin *unlock-code*

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** Unlock the subscriber identity module (SIM) in the GSM 3G wireless modem card.

**Options**

- ***interface-name***—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.
- **pin *unlock-code***—Four-digit personal identification number (PIN). Obtain the PIN from the service provider.



NOTE: If the PIN is entered incorrectly three consecutive times, the SIM is blocked. Obtain a PIN unblocking key (PUK) from the service provider.

**Required Privilege Level** maintenance

**Related Documentation**

- request modem wireless gsm sim-unblock on page 1496
- Modem Interfaces
- Interfaces for Security Devices

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request modem wireless gsm sim-unlock cl-0/0/8 pin 3210

```
user@host> request modem wireless gsm sim-unlock cl-0/0/8 pin 3210
Issued SIM unlock request successfully.
Please verify SIM lock status under firmware stats
```

Copyright © 2013, Juniper Networks, Inc.

## request pppoe connect

**Syntax** request pppoe connect

**Release Information** Statement supported on SRX100, SRX110, SRX210, SRX220, SRX240, and SRX650 is introduced in Release 11.2 and 11.4 of Junos OS.

**Description** Connect all sessions that are down.

**Options** **pppoe interface name**— (Optional) Connect to a specified session.

**Required Privilege Level** maintenance

**Related Documentation**
- Device and Routing Operations Monitoring

**List of Sample Output** request pppoe connect on page 1498

**Output Fields** When you enter this command, this command returns no output.

### Sample Output

request pppoe connect

```
user@host> request pppoe connect
```


Copyright © 2013, Juniper Networks, Inc.

## request pppoe disconnect

**Syntax** request pppoe disconnect

**Release Information** Statement supported on SRX100, SRX110, SRX210, SRX220, SRX240, and SRX650 is introduced in Release 11.2 and 11.4 of Junos OS.

**Description** Connect all sessions that are down.

**Options** **session id** — (Optional) Disconnect the session for which the session ID is specified.

**pppoe interface name**— (Optional) Disconnect the session for a specific pppoe interface name.

**Required Privilege Level** maintenance

**Related Documentation**
- Device and Routing Operations Monitoring

**List of Sample Output** request pppoe disconnect on page 1499

**Output Fields** When you enter this command, this command returns no output.

### Sample Output

request pppoe disconnect

```
user@host> request pppoe disconnect
```

Copyright © 2013, Juniper Networks, Inc.

## request security datapath-debug capture start

**Syntax** request security datapath-debug capture start

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Start the data path debugging capture.

**Required Privilege Level** maintenance

**Related Documentation**
- Master Administrator for Logical Systems on Security Devices

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request security datapath-debug capture start

```
user@host> request security datapath-debug capture start
datapath-debug capture started on file
```


Copyright © 2013, Juniper Networks, Inc.

## request security datapath-debug capture stop

**Syntax** request security datapath-debug capture stop

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Stop the data path debugging capture.

**Required Privilege Level** maintenance

**Related Documentation**
- Master Administrator for Logical Systems on Security Devices

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request security datapath-debug capture stop

```
user@host> request security datapath-debug capture stop
datapath-debug capture successfully stopped, use show security datapath-debug
capture to view
```

Copyright © 2013, Juniper Networks, Inc.

## request security idp security-package download

**Syntax**

request security idp security-package download
<check-server>
<full-update>
<policy-templates>
<version *version-number* >
<status>

**Release Information**

Command introduced in Release 9.2 of Junos OS. Detailed status added in Release 10.1 of Junos OS. Description modified in Release 11.1 of Junos OS. Application package support added in Release 11.4 of Junos OS.

**Description**

Manually download the individual components of the security package from the Juniper Security Engineering portal. The components are downloaded into a staging folder inside the device.

By default, this command tries to download the delta set attack signature table. It also downloads IDP, IPS, and application package signatures.

**Options**

- **check-server**—(Optional) Retrieve the version information of the latest security package from the security portal server.
- **full-update**—(Optional) Download the latest security package with the full set of attack signature tables from the portal.
- **policy-templates**—(Optional) Download the latest policy templates from the portal.
- **version** *version-number* —(Optional) Download the security package of a specific version from the portal.
- **status**—(Optional) Provide detailed status of security package download operation.

**Additional Information**

The **request security idp security-package download** command does not download security package files if the installed version on the device is same as the security package version on the server (https://services.netscreen.com/cgi-bin/index.cgi always). The **request security idp security-package download full-update** command downloads the latest security package files on the device from the server, irrespective of the version on the device and the server.

**Required Privilege Level**

maintenance

**Related Documentation**

- IDP Policies for Security Devices
- IDP Signature Database for Security Devices
- show security idp active-policy on page 2007
- show security idp security-package-version on page 2047

**List of Sample Output**

request security idp security-package download on page 1503


Copyright © 2013, Juniper Networks, Inc.

request security idp security-package download policy-templates on page 1503
request security idp security-package download version 1151 full-update on page 1503
request security idp security-package download status on page 1503

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

## Sample Output

request security idp security-package download

```
user@host> request security idp security-package download
Successfully downloaded from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:1152(Thu Apr 24 14:37:44 2008, Detector=9.1.140080400)
```

## Sample Output

request security idp security-package download policy-templates

```
user@host> request security idp security-package download policy-templates
Successfully downloaded from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:35
```

## Sample Output

request security idp security-package download version 1151 full-update

```
user@host> request security idp security-package download version 1151 full-update
Successfully downloaded from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:1151(Wed Apr 23 14:39:15 2008, Detector=9.1.140080400)
```

request security idp security-package download status

To request status for a package download:

```
user@host> request security idp security-package download status
Done;Successfully downloaded
from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:2014(Thu Oct 20 12:07:01 2011, Detector=11.6.140110920)
```

To request status for a template download:

```
user@host> request security idp security-package download status
Done; Successfully downloaded from
(https://services.netscreen.com/cgi-bin/index.cgi).
```

When devices are operating in chassis cluster mode, when you check the security package download status, a message is displayed confirming that the downloaded security package is being synchronized to the primary and secondary nodes.

```
user@host> request security idp security-package download status
node0:
--------------------------------------------------------------------------
Done;Successfully downloaded from(https://services.netscreen.com/cgi-bin/index.cgi)
and synchronized to backup.
Version info:2011(Mon Oct 17 15:13:06 2011, Detector=11.6.140110920)
```

Copyright © 2013, Juniper Networks, Inc. 

## request security idp security-package install

**Syntax**

request security idp security-package install
<policy-templates>
<status>
<update-attack-database-only>

**Release Information**

Command introduced in Release 9.2 of Junos OS. Description modified in Release 11.1 of Junos OS. Added application package support in Release 11.4 of Junos OS.

**Description**

Updates the attack database inside the device with the newly downloaded one from the staging folder, recompiles the existing running policy, and pushes the recompiled policy to the data plane.

Also, if there is an existing running policy, and the previously installed detector's version is different from the newly downloaded one, the downloaded components are pushed to the data plane. This command installs IDP, IPS, and application package signatures.

**Options**

- **policy-templates**—(Optional) Installs the policy template file into /var/db/scripts/commit/templates.
- **status**—(Optional) The command **security-package install** may take a long time depending on the new Security database size. Hence, **security-package install** command returns immediately and a background process performs the task. User can check the status using **security-package install status** command.
- **update-attack-database-only**—(Optional) Loads the security package into IDP database but does not compile/push the active policy or the new detector to the data plane.

**Required Privilege Level**

maintenance

**Related Documentation**

- IDP Policies for Security Devices
- IDP Signature Database for Security Devices
- show security idp active-policy on page 2007
- show security idp security-package-version on page 2047

**List of Sample Output**

request security idp security-package install on page 1505
request security idp security-package install status on page 1505

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

request security idp security-package install

```
user@host> request security idp security-package install
Will be processed in async mode. Check the status using the status checking CLI
```

## Sample Output

request security idp security-package install status

To request status on a package installation:

```
user@host> request security idp security-package install status
Done;Attack DB update : successful - [UpdateNumber=1152,ExportDate=Thu Apr 24
14:37:44 2008]
     Updating data-plane with new attack or detector : not performed
     due to no existing active policy found.
```

To request status on a template installation:

```
user@host> request security idp security-package install status
Done; policy-template has been successfully updated into internal repository
(=>/var/db/scripts/commit/templates.xsl)!
```

Copyright © 2013, Juniper Networks, Inc.

## request security idp ssl-inspection key add

**Syntax** request security idp ssl-inspection key add *<key-name>* [file *<file-name>*] [password *<password-string>*] [server *<server-ip>*]

**Release Information** Command introduced in Release 9.3 of Junos OS.

**Description** Install a Privacy-Enhanced Mail (PEM) key that is optionally password protection, and associate a server with an installed key. The length of each key name and password string should not exceed 32 alpha-numeric characters long.

**Options**

- ***key-name***—Name of the SSL private key.
- **file *<file-name>***—(Optional) Location of RSA private key (PEM format) file.
- **password *<password-string>***—(Optional) Password used to encrypt specified key.
- **server *<server-ip>*** —(Optional) Server IP address to be added to the specified key.

**Required Privilege Level** maintenance

**Related Documentation**

- show security idp ssl-inspection key on page 2048
- IDP Policies for Security Devices

**List of Sample Output**

request security idp ssl-inspection key add key1 file /var/tmp/enc1.key password encrypted on page 1506
request security idp ssl-inspection key add key2 file /var/tmp/enc2.key password encrypted on page 1506
request security idp ssl-inspection key add key3 file /var/tmp/norm.key on page 1507
request security idp ssl-inspection key add key1 server 1.1.0.1 on page 1507
request security idp ssl-inspection key add key1 server 1.1.0.2 on page 1507

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request security idp ssl-inspection key add key1 file /var/tmp/enc1.key password encrypted

```
user@host> request security idp ssl-inspection key add key1 file /var/tmp/enc1.key password
encrypted
Added key 'key1'
```

### Sample Output

request security idp ssl-inspection key add key2 file

```
user@host> request security idp ssl-inspection key add key2 file /var/tmp/enc2.key password
encrypted
Added key 'key2', server 2.2.0.1
```


Copyright © 2013, Juniper Networks, Inc.

/var/tmp/enc2.key
password encrypted

## Sample Output

request security idp ssl-inspection key add key3 file /var/tmp/norm.key

```
user@host> request security idp ssl-inspection key add key3 file /var/tmp/norm.key
Added key 'key3'
```

## Sample Output

request security idp ssl-inspection key add key1 server 1.1.0.1

```
user@host> request security idp ssl-inspection key add key1 server 1.1.0.1
Added key 'key1', server 1.1.0.1
```

## Sample Output

request security idp ssl-inspection key add key1 server 1.1.0.2

```
user@host> request security idp ssl-inspection key add key1 server 1.1.0.2
Added key 'key1', server 1.1.0.2
```

Copyright © 2013, Juniper Networks, Inc.

## request security idp ssl-inspection key delete

**Syntax** request security idp ssl-inspection key delete [<*key-name*> [server <*server-ip*>]]

**Release Information** Command introduced in Release 9.3 of Junos OS.

**Description** Delete the specified server IP from the given key if the server is specified. If the server IP is not specified, the given key will be deleted along with all the server addresses associated with it.



NOTE: You will get a delete confirmation question before deleting one or more keys or server.

**Options**

- ***key-name***—(Optional) Name of the SSL private key.
- **server** <***server-ip***> —(Optional) Server IP address associated with the specified key to be deleted.

**Required Privilege Level** maintenance

**Related Documentation**

- show security idp ssl-inspection key on page 2048
- IDP Policies for Security Devices

**List of Sample Output**

request security idp ssl-inspection key delete on page 1509
request security idp ssl-inspection key delete key1 on page 1509
request security idp ssl-inspection key delete key2 server 2.2.0.1 on page 1509

**Output Fields** When you enter this command, you are provided feedback on the status of your request.


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

request security idp ssl-inspection key delete

```
user@host> request security idp ssl-inspection key delete

This command will delete one or more ssl keys.
Continue? [yes,no] (no) yes

Number of keys 4, server 3 deleted
```

## Sample Output

request security idp ssl-inspection key delete key1

```
user@host> request security idp ssl-inspection key delete key1

This command will delete one or more ssl keys.
Continue? [yes,no] (no) yes

Number of keys 1, server 2 deleted
```

## Sample Output

request security idp ssl-inspection key delete key2 server 2.2.0.1

```
user@host> request security idp ssl-inspection key delete key2 server 2.2.0.1

This command will delete one or more ssl keys.
Continue? [yes,no] (no) yes

Number of keys 0, server 1 deleted
```

Copyright © 2013, Juniper Networks, Inc.

## request security idp storage-cleanup

**Syntax** request security idp storage-cleanup

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Delete unused files to free up storage space on a device.

**Options** **cache-files**— Delete DFA cache files used for optimizing idp policy compilation.

**downloaded-files**— Delete downloaded security-package files (with out affecting the installed database).

**Required Privilege Level** maintenance

**Related Documentation**
- IDP Policies for Security Devices

**List of Sample Output** request security idp storage-cleanup on page 1510

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request security idp storage-cleanup

```
user@host> request security idp storage-cleanup downloaded-files
Successfully deleted downloaded secdb files
```


Copyright © 2013, Juniper Networks, Inc.

## request security ike debug-disable

**Syntax** request security ike debug-disable

**Release Information** Command introduced in Release 11.4R3 of Junos OS.

**Description** Disable IKE debugging.

**Required Privilege Level** maintenance

**Related Documentation**
- request security ike debug-enable on page 1512
- show security ike debug-status on page 2057

**List of Sample Output** request security ike debug-disable on page 1511

**Output Fields** This command produces no output.

### Sample Output

request security ike debug-disable

```
user@host> request security ike debug-disable
```

## request security ike debug-enable

**Syntax** request security ike debug-enable local *local-ip-address* remote *remote-ip-address*

**Release Information** Command introduced in Release 11.4R3 of Junos OS.

**Description** Enable IKE debugging.

**Options**
- **local** ***local-ip-address***—The address of the local peer.
- **remote** ***remote-ip-address***—The address of the remote peer.

**Required Privilege Level** maintenance

**Related Documentation**
- request security ike debug-disable on page 1511
- show security ike debug-status on page 2057

**List of Sample Output** request security ike debug-enable local 1.1.1.1 remote 2.2.2.2 on page 1512

**Output Fields** This command produces no output.

### Sample Output

request security ike debug-enable local 1.1.1.1 remote 2.2.2.2

```
user@host> request security ike debug-enable local 1.1.1.1 remote 2.2.2.2
```


Copyright © 2013, Juniper Networks, Inc.

## request security pki ca-certificate verify (Security)

**Syntax** **request security pki ca-certificate verify ca-profile** *ca-profile-name*

**Release Information** Command introduced in Release 8.5 of Junos OS.

**Description** Verify the digital certificate installed for the specified certificate authority (CA).

**Options** **ca-profile** *ca-profile-name* —Display the specified CA profile.

**Required Privilege Level** maintenance and security

**Related Documentation**
- ca-profile (Security) on page 448
- show security pki ca-certificate (View) on page 2126

**List of Sample Output**
request security pki ca-certificate verify ca-profile ca1 (CRL downloaded) on page 1513
request security pki ca-certificate verify ca-profile ca1 (CRL not downloaded) on page 1513

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

This user has downloaded the certificate revocation list (CRL).

request security pki ca-certificate verify ca-profile ca1 (CRL downloaded)

```
user@host> request security pki ca-certificate verify ca-profile ca1
CA certificate ca1 verified successfully
```

### Sample Output

This user has not downloaded the certificate revocation list (CRL).

request security pki ca-certificate verify ca-profile ca1 (CRL not downloaded)

```
user@host> request security pki ca-certificate verify ca-profile ca1
CA certificate ca1: CRL verification in progress. Please check the PKId debug
logs for completion status
```

Copyright © 2013, Juniper Networks, Inc.

## request security pki local-certificate generate-self-signed (Security)

**Syntax**

**request security pki local-certificate generate-self-signed**

**certificate-id** ***certificate-id-name***

**domain-name** ***domain-name*** **subject** ***subject-distinguished-name***

**<email** ***email-address>***

**<ip-address** ***ip-address***>

**Release Information**

Command introduced in Release 9.1 of Junos OS.

**Description**

Manually generate a self-signed certificate for the given distinguished name.

**Options**

- **certificate-id** ***certificate-id-name***—Name of the certificate and the public/private key pair.
- domain-name ***domain-name***—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.
- subject ***subject-distinguished-name***—Distinguished name format that contains the common name, department, company name, state, and country in the following format: CN, OU, O, ST, C
  - CN—Common name
  - OU—Organizational unit name
  - O—Organization name
  - ST—State
  - C—Country
- email ***email-address***—E-mail address of the certificate holder.
- ip-address ***ip-address***—IP address of the routing platform.

**Required Privilege Level**

maintenance and security

**Related Documentation**

- clear security pki local-certificate (Device) on page 1465
- show security pki local-certificate (View) on page 2134

**List of Sample Output**

request security pki local-certificate generate-self-signed certificate-id self-cert subject cn=abc domain-name juniper.net email mholmes@juniper.net on page 1515

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

request security pki local-certificate generate-self-signed certificate-id self-cert subject cn=abc domain-name juniper.net email mholmes@juniper.net

```
user@host> request security pki local-certificate generate-self-signed certificate-id self-cert
subject cn=abc domain-name juniper.net email mholmes@juniper.net
Self-signed certificate generated and loaded successfully
```

Copyright © 2013, Juniper Networks, Inc.

## request security pki local-certificate load

**Syntax** request security pki local-certificate load filename *ssl_proxy_ca.crt* key *ssl_proxy_ca.key* certificate-id *certificate id*

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Manually load a local digital certificate from a specified location.

**Options** **filename** — Filename that contains the certificate to load

**key**— File pathname that contains the private key/key-pair to loaded

**certificate-id** —Name of the certificate identifier

**Required Privilege Level** maintenance and security

**List of Sample Output** request security pki local-certificate load on page 1516

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request security pki local-certificate load

```
user@host> request security pki local-certificate load filename cert_name.crt key key_name.key
certificate-id test
Local certificate cert_name.crt loaded successfully
```


Copyright © 2013, Juniper Networks, Inc.

## request security pki local-certificate verify (Security)

**Syntax** request security pki local-certificate verify certificate-id *certificate-id-name*

**Release Information** Command introduced in Release 8.5 of Junos OS.

**Description** Verify the validity of the local digital certificate identifier.

**Options** **certificate-id** *certificate-id-name* — Name of the local digital certificate identifier.

**Required Privilege Level** maintenance and security

**List of Sample Output**
request security pki local-certificate verify certificate-id bme1 (not downloaded) on page 1517
request security pki local-certificate verify certificate bme1 (downloaded) on page 1517

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

You receive the following response before the certificate revocation list (CRL) is downloaded:

request security pki local-certificate verify certificate-id bme1 (not downloaded)

```
user@host> request security pki local-certificate verify certificate-id bme1
Local certificate bme1: CRL verification in progress. Please check the PKId debug
 logs for completion status
```

### Sample Output

You receive the following response after the certificate revocation list (CRL) is downloaded:

request security pki local-certificate verify certificate bme1 (downloaded)

```
user@host> request security pki local-certificate verify certificate-id bme1
Local certificate bme1 verification success
```

Copyright © 2013, Juniper Networks, Inc.

## request security pki verify-integrity-status

**Syntax** request security pki verify-integrity-status

**Release Information** Command introduced in Junos OS Release 11.2.

**Description** Verify the integrity of public key infrastructure (PKI) files.

**Required Privilege Level** maintenance

**Related Documentation**
- [edit security pki] Hierarchy Level on page 349

**List of Sample Output** request security pki verify-integrity-status on page 1518

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request security pki verify-integrity-status

```
user@host> request security pki verify-integrity-status
All PKI objects: verification success
```


Copyright © 2013, Juniper Networks, Inc.

## request security user-identification local-authorization-table add

**Syntax** request security user-identification local-authorization-table add user *user-name* ip-address *ip-address* roles [*role-name*]

**Release Information** Command introduced in Junos OS Release 12.1. Command updated in Junos OS Release 12.1X44-D10.

**Description** This command adds user and role information to the local authentication table. The table is used to retrieve user and role information for traffic from the specified IP address to enforce a user role firewall.

To add an entry, specify the user name, IP address, and up to 40 roles to be associated with this user. Subsequent commands for the same user and IP address aggregates any new roles to the existing list. An authentication entry can contain up to 200 roles.



NOTE: To change the user name of an entry or to remove or change entries in a role list, you must delete the existing entry and create a new one.

An IP address can be associated with only one user. If a second request is made to add a different user using the same IP address, the second authentication entry overwrites the existing entry.

**Options** user *user-name*—Specify the name of the user to be added to the table.

ip-address *ip-address*—Specify the IP address of the user. Either IPv4 or IPv6 addresses are supported.

roles [*role-name*]—(Optional) Specify the role or list of roles to be associated with the specified user. If the specified user and IP address already exist, any roles specified in the command are added to the existing role list.

**Required Privilege Level** maintenance

**Related Documentation**

- request security user-identification local-authentication-table delete on page 1521
- Understanding the User Identification Table

**List of Sample Output** request security user-identification local-authentication-table add on page 1519

**Output Fields** When you enter this command, either an entry is added to the local authentication table, or the roles of an existing entry are aggregated with additional roles.

### Sample Output

request security user-identification

```
user@host> request security user-identification local-authentication-table add user user1
ip-address 1.1.1.1 roles role1
```

Copyright © 2013, Juniper Networks, Inc.

local-authentication-table add

```
user@host> request security user-identification local-authentication-table add user user2
ip-address 2.2.2.2 roles [role2 role3]
user@host> request security user-identification local-authentication-table add user user2
ip-address 2.2.2.2 roles role1
user@host> show security user-identification local-authentication-table all
Total entries: 2
Source IP       Username      Roles
1.1.1.1         user1      role1
2.2.2.2         user2      role2, role3, role1
```


Copyright © 2013, Juniper Networks, Inc.

## request security user-identification local-authentication-table delete

**Syntax** request security user-identification local-authentication-table delete *ip-address* | *user-name*

**Release Information** Command introduced in Junos OS Release 12.1.

**Description** This command removes an entry from the local authentication table. You can identify the entry by IP address or user-name. To change the user name of an entry or to remove or change entries in a role list, you must delete the existing entry and create a new one.

**Options** ***ip-address***—The IP address of the entry to be deleted.

***user-name***—The user name of the entry to be deleted. To change the user name of an entry, you must delete the old entry and create a new one.

**Required Privilege Level** maintenance

**Related Documentation**

- request security user-identification local-authorization-table add on page 1519
- Understanding the User Identification Table

**Output Fields** The specified show command verifies the table content before and after an entry has been deleted from the local authentication table.

### Sample Output

```
user@host> show security user-identification local-authentication-table all
Total entries: 2
    Ip-address: 1.1.1.1
    Username: user1
    Roles: role1

    Ip-address: 2.2.2.2
    Username: user2
    Roles: role2, role3, role1
```

```
user@host> request security user-identification local-authentication-table delete 2.2.2.2
user@host> show security user-identification local-authentication-table all
Total entries: 1
    Ip-address: 1.1.1.1
    Username: user1
    Roles: role1
```

Copyright © 2013, Juniper Networks, Inc.

## request security utm anti-virus juniper-express-engine

**Syntax** request security utm anti-virus juniper-express-engine

**Release Information** Command introduced in Release 9.5 of Junos OS.
Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Manually update the express antivirus pattern database using the command described. You can update the express antivirus pattern database automatically or manually. With full chassis cluster support for UTM this command is operational on both the nodes.

**Options**

- **pattern-delete** — Delete the current express antivirus pattern database.
- **pattern-reload** — Reload the express antivirus pattern database.
- **pattern-update** — Update the express antivirus pattern database with the latest signatures.

**Required Privilege Level** maintenance

**Related Documentation**

- request security utm anti-virus kaspersky-lab-engine on page 1523
- clear security utm antivirus statistics on page 1473
- show security utm anti-virus statistics on page 2176
- show security utm anti-virus status on page 2178
- Unified Threat Management
- UTM Express Antivirus Protection for Security Devices

**List of Sample Output** request security utm anti-virus juniper-express-engine pattern-update on page 1522

**Output Fields** request security utm anti-virus juniper-express-engine pattern-update

When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request security utm anti-virus juniper-express-engine pattern-update

```
user@host> request security utm anti-virus juniper-express-engine pattern-update
```


Copyright © 2013, Juniper Networks, Inc.

## request security utm anti-virus kaspersky-lab-engine

**Syntax** request security utm anti-virus kaspersky-lab-engine

**Release Information** Command introduced in Release 11.1 of Junos OS.
Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Manually update the full file-based antivirus pattern database using the commands described. You can update the full file-based antivirus pattern database automatically or manually. With full chassis cluster support for UTM this command is operational on both the nodes.

**Options**

- **pattern-delete** — Delete the current full file-based antivirus pattern database.
- **pattern-reload** — Reload the full file-based antivirus pattern database.
- **pattern-update** — Update the full file-based antivirus pattern database with the latest signatures.

**Required Privilege Level** maintenance

**Related Documentation**

- request security utm anti-virus juniper-express-engine on page 1522
- clear security utm antivirus statistics on page 1473
- show security utm anti-virus statistics on page 2176
- show security utm anti-virus status on page 2178
- UTM for Security Devices

**List of Sample Output** request security utm anti-virus kaspersky-lab-engine pattern-update on page 1523

**Output Fields** request security utm anti-virus kaspersky-lab-engine pattern-update

When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request security utm anti-virus kaspersky-lab-engine pattern-update

```
user@host> request security anti-virus kaspersky-lab-engine pattern-update
```

Copyright © 2013, Juniper Networks, Inc.

## request security utm anti-virus sophos-engine

**Syntax** request security utm anti-virus sophos-engine

**Release Information** Command introduced in Release 11.1 of Junos OS.
Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Manually update the Sophos antivirus pattern database using the command described. You can update the express antivirus pattern database automatically or manually. To update automatically you use the configuration statement **set security utm feature-profile anti-virus sophos-engine pattern-update interval *seconds***. With full chassis cluster support for UTM this command is operational on both the nodes.

**Options**
- **pattern-delete** — Delete the current Sophos antivirus pattern database.
- **pattern-reload** — Reload the Sophos antivirus pattern database.
- **pattern-update** — Update the Sophos antivirus pattern database with the latest signatures.

**Required Privilege Level** maintenance

**Related Documentation**
- clear security utm antivirus statistics on page 1473
- show security utm anti-virus statistics on page 2176
- show security utm anti-virus status on page 2178
- Unified Threat Management

**List of Sample Output** request security utm anti-virus sophos-engine pattern-update on page 1524

**Output Fields** request security utm anti-virus sophos-engine pattern-update

When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request security utm anti-virus sophos-engine pattern-update

```
user@host> request security utm anti-virus sophos-engine pattern-update
```


Copyright © 2013, Juniper Networks, Inc.

## request services application-identification application

**Syntax**

request services application-identification application copy *predefined-application-name*

request services application-identification application [disable | enable] *predefined-application-name* <no-commit>

**Release Information**

Command introduced in Release 11.4 of Junos OS.

**Description**

Copy, disable, or enable a predefined application signature.

**Options**

**copy** —(Optional) Copy a predefined application signature from the database to the configuration and change the name (for example, my:FTP). The ID and order will be generated automatically. Do not name your custom application signature with the "junos" prefix; this prefix is reserved for predefined application signatures. You can copy the same predefined application signature only once; duplicate custom signatures are not allowed. The **copy** command does not initiate signature recompilation.



NOTE: In configuration mode, if an uncommitted action is pending, the **request services application-identification application copy** command will fail. Uncompiled application signatures are shown as uncommitted in the **show services application-identification application [summary | detail]** command.

**disable**—(Optional) Disable a predefined application signature, initiate signature recompilation, and commit all pending uncompiled signatures to the configuration. Include the <no-commit> keyword to defer signature recompilation.

The following conditions apply:

- You cannot disable a predefined application signature that is referenced by an active security policy or custom application signature. First modify or deactivate the policy or custom application signature.
- If you disable an application signature, for example, junos:HTTP, that has nested applications, the nested applications will not be recognized.

**enable**—(Optional) Enable a predefined application signature, initiate signature recompilation, and commit all pending uncompiled signatures to the configuration. Include the <no-commit> keyword to defer signature recompilation.

**no-commit**—(Optional) Enables you to enter multiple **enable** and **disable** commands before initiating signature recompilation (which takes some time) and committing the configuration. Uncompiled application signatures are shown as uncommitted in the **show services application-identification application [summary | detail]** command.

**Required Privilege Level**

maintenance

Copyright © 2013, Juniper Networks, Inc.

**Related Documentation**

- Application Identification for Security Devices
- show services application-identification application on page 2197

**Output Fields** When you enter this command, the system provides feedback on the status of your request.

## Sample Output

request services application-identification application copy

```
user@host> request services application-identification application junos:FTP copy
application package 63 copied successfully.
```

request services application-identification application disable

```
user@host> request services application-identification application disable junos:163
 Please wait while we are re-compiling signatures ...
 Please wait while we are re-compiling signatures ...
 Please wait while we are re-compiling signatures ...
 Please wait while we are re-compiling signatures ...
 Disable application junos:163 succeed.
```

request services application-identification application disable no-commit

```
user@host> request services application-identification application disable
junos:FACEBOOK-SOCIALRSS no-commit
Disable application junos:FACEBOOK-SOCIALRSS succeed. It is not committed yet.
```


Copyright © 2013, Juniper Networks, Inc.

## request services application-identification download

**Syntax** request services application-identification download <version>;

**Release Information** Statement introduced in Release 10.2 of Junos OS. Statement modified in Release 11.4 of Junos OS.

**Description** Manually download the application package for Junos OS application identification. The application package is extracted from the IDP signature database and contains signature definitions for known applications, such as: DNS, Facebook, FTP, Skype, and SNMP.

**Options** **version**—(Optional) Download a specific version of the application package from the Juniper security website. If you do not enter a version, the most recent version will be downloaded.

**Required Privilege Level** maintenance

**Related Documentation**

- Application Identification for Security Devices
- request services application-identification download status on page 1528
- request services application-identification install on page 1530

**List of Sample Output** request services application-identification download on page 1527

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request services application-identification download

```
user@host> request services application-identifications download
Please use command "request services application-identification download status"
 to check status
```

Copyright © 2013, Juniper Networks, Inc.

## request services application-identification download status

**Syntax** request services application-identification download status

**Release Information** Statement introduced in Release 10.2 of Junos OS. Statement modified in Release 11.4 of Junos OS.

**Description** Check the download status of the application signature package. The downloaded application package is saved under /var/db/appid/sec-download/.

**Required Privilege Level** maintenance

**Related Documentation**
- Application Identification for Security Devices
- request services application-identification download on page 1527

**List of Sample Output** request services application-identification download status on page 1528

**Output Fields** When you enter this command, the system provides feedback on the status of your request.

### Sample Output

request services application-identification download status

```
user@host> request services application-identifications download status
Application package 1608 is downloaded successfully.
```


Copyright © 2013, Juniper Networks, Inc.

## request services application-identification group

**Syntax** request services application-identification group [copy |disable | enable]
*predefined-application-group-name*

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Copy, disable, or enable a predefined application signature group.

**Options** **copy** —(Optional) Copy a predefined application signature group from the database to the configuration and change the name (for example, my:FTP). The ID and order will be generated automatically. Do not name your custom application signature group with the "junos" prefix; this prefix is reserved for predefined application signature groups. You can copy the same predefined application signature group only once; duplicate custom signature groups are not allowed.



NOTE: In configuration mode, if an uncommitted action is pending, the **request services application-identification group copy** command will fail.

**disable**—(Optional) Disable a predefined application signature group.



NOTE: You cannot disable a predefined application signature group that is referenced by an active security policy or custom application signature group. First modify or deactivate the policy or custom application signature group.

**enable**—(Optional) Enable a predefined application signature group.

**Required Privilege Level** maintenance

**Related Documentation**
- Application Identification for Security Devices
- show services application-identification group on page 2208

**Output Fields** When you enter this command, the system provides feedback on the status of your request.

### Sample Output

request services application-identification group

```
user@host> request services application-identification group copy junos:SYBASE
group 1040 copied successfully.
```

Copyright © 2013, Juniper Networks, Inc.

## request services application-identification install

**Syntax** request services application-identification install

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Install the downloaded predefined application signature package. The install operation will fail if any custom application signatures or custom application signature groups have been manually inserted before any predefined application signatures or predefined application signature groups in the Junos OS configuration. Remove any "insert-before" signatures, then retry the install operation.



NOTE: You can also use the **request security idp security-package [download | install]** command to download and install the predefined application signature package along with the IDP security package.

**Required Privilege Level** maintenance

**Related Documentation**

- Application Identification for Security Devices
- request services application-identification install status on page 1531
- request services application-identification download on page 1527

**Output Fields** When you enter this command, the system provides feedback on the status of your request.

### Sample Output

```
user@host> request services application-identification install
Please use command "request services application-identification install status"
 to check status
```


Copyright © 2013, Juniper Networks, Inc.

## request services application-identification install status

**Syntax** request services application-identification install status

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Display the status of the install operation.

**Required Privilege Level** maintenance

**Related Documentation**
- Application Identification for Security Devices
- request services application-identification install on page 1530

**Output Fields** When you enter this command, the system provides feedback on the status of your request.

### Sample Output

```
user@host> request services application-identification install status
Install application package version (1776) succeed.
```

## request services application-identification uninstall

**Syntax** request services application-identification uninstall

**Release Information** Statement introduced in Release 10.2 of Junos OS. Statement modified in Release 10.4 and Release 11.4 of Junos OS.

**Description** Uninstall the predefined application package. The uninstall operation will fail if any active security policies or custom application signatures or custom application signature groups reference predefined application signatures or predefined application signature groups in the Junos OS configuration.

**Required Privilege Level** maintenance

**Related Documentation**

- Application Identification for Security Devices
- request services application-identification install on page 1530

**Output Fields** When you enter this command, the system provides feedback on the status of your request.

### Sample Output

```
user@host> request services application-identification uninstall
Please use command "request services application-identification uninstall status"
 to check status
```


Copyright © 2013, Juniper Networks, Inc.

## request services application-identification uninstall status

**Syntax** request services application-identification uninstall status

**Release Information** Statement introduced in Release 11.4 of Junos OS.

**Description** Display the status of the uninstall operation.

**Required Privilege Level** maintenance

**Related Documentation**
- Application Identification for Security Devices
- request services application-identification uninstall on page 1532

**Output Fields** When you enter this command, the system provides feedback on the status of your request.

### Sample Output

```
user@host> request services application-identification uninstall status
Uninstall application package version (1776) succeed.
```

## request system autorecovery state

**Syntax** request system autorecovery state (save | recover | clear)

**Release Information** Command introduced in Junos Release 11.2.

**Description** Prepares the system for autorecovery of configuration, licenses, and disk information.

**Options** **save**—Save the current state of the disk partitioning, configuration, and licenses for autorecovery.

The active Junos OS configuration is saved as the Junos rescue configuration, after which the rescue configuration, licenses, and disk partitioning information is saved for autorecovery. Autorecovery information must be initially saved using this command for the autorecovery feature to verify integrity of data on every bootup.



NOTE:

- Any recovery performed at a later stage will restore the data to the same state as it was when the save command was executed.
- A fresh rescue configuration is generated when the command is executed. Any existing rescue configuration will be overwritten.

**recover**—Recover the disk partitioning, configuration, and licenses.

After autorecovery data has been saved, the integrity of saved items is always checked automatically on every bootup. The recovery command allows you to forcibly re-run the tests at any time if required.

**clear**—Clear all saved autorecovery information.

Only the autorecovery information is deleted; the original copies of the data used by the router are not affected. Clearing the autorecovery information also disables all autorecovery integrity checks performed during bootup.

**Required Privilege Level** maintenance

**Related Documentation**

- show system autorecovery state on page 2247
- Device Configuration

**List of Sample Output**

request system autorecovery state save on page 1535
request system autorecovery state recover on page 1535
request system autorecovery state clear on page 1535

**Output Fields** When you enter this command, you are provided feedback on the status of your request.


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

request system autorecovery state save

```
user@host> request system autorecovery state save
Saving config recovery information
      Saving license recovery information
      Saving bsdlabel recovery information
```

## Sample Output

request system autorecovery state recover

```
user@host> request system autorecovery state recover

Configuration:
File             Recovery Information    Integrity Check    Action / Status
rescue.conf.gz   Saved                   Passed             None
Licenses:
File             Recovery Information    Integrity Check    Action / Status
JUNOS282736.lic  Saved                   Passed             None
JUNOS282737.lic  Saved                   Failed             Recovered
BSD Labels:
Slice            Recovery Information    Integrity Check    Action / Status
s1               Saved                   Passed             None
s2               Saved                   Passed             None
s3               Saved                   Passed             None
s4               Saved                   Passed             None
```

## Sample Output

request system autorecovery state clear

```
user@host> request system autorecovery state clear
Clearing config recovery information
       Clearing license recovery information
       Clearing bsdlabel recovery information
```

Copyright © 2013, Juniper Networks, Inc.

## request services ip-monitoring preempt-restore policy

**Syntax** **request services ip-monitoring preempt-restore policy** *<policy-name>*

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** If the no–preempt option is specified, the policy will not perform preemptive failback when it is in a failover state, and when the RPM probe test recovers from failure. To manually revert to the failback state, run the **request services ip-monitoring preempt-restore policy** command.



NOTE: The **request services ip-monitoring preempt-restore policy** command takes effect only when the RPM probe is in the pass state, and when the policy is in a failover state.

**Options** **policy name**—Name of the policy.

**Required Privilege Level** maintenance

**Related Documentation**

- IP Monitoring
- show services rpm probe-results (View) on page 2219
- show services ip-monitoring status on page 2215

**List of Sample Output** run request services ip-monitoring preempt-restore policy <policy name> on page 1536

**Output Fields** When you run this command, the policy is restored to the failback state.

### Sample Output

run request services ip-monitoring preempt-restore policy <policy name>

```
user@host> run request services ip-monitoring preempt-restore policy policy1
Restore request succeeded: Policy policy1
```


Copyright © 2013, Juniper Networks, Inc.

## request system download abort

**Syntax** request system download abort <*download-id*>

**Release Information** Command introduced in Release 11.2 of Junos OS.

**Description** Abort a download. The download instance is stopped and cannot be resumed. Any partially downloaded file is automatically deleted to free disk space. Information regarding the download is retained and can be displayed with the **show** command until a Clear operation is performed.



NOTE: Only downloads in the active, paused, and error states can be aborted.

**Options** **download-id**—(Required) The ID number of the download to be paused.

**Required Privilege Level** maintenance

**Related Documentation**

- request system download start on page 1541
- request system download pause on page 1539
- request system download resume on page 1540
- request system download clear on page 1538
- Device Configuration

**List of Sample Output** request system download abort on page 1537

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request system download abort

```
user@host> request system download abort 1
Aborted download #1
```

Copyright © 2013, Juniper Networks, Inc.

## request system download clear

**Syntax** request system download clear

**Release Information** Command introduced in Release 11.2 of Junos OS.

**Description** Delete the history of completed and aborted downloads.

**Required Privilege Level** maintenance

**Related Documentation**

- request system download start on page 1541
- request system download pause on page 1539
- request system download resume on page 1540
- request system download abort on page 1537
- Device Configuration

**List of Sample Output** request system download clear on page 1538

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request system download clear

```
user@host> request system download clear
Cleared information on completed and aborted downloads
```


Copyright © 2013, Juniper Networks, Inc.

## request system download pause

**Syntax** request system download pause <*download-id*>

**Release Information** Command introduced in Release 11.2 of Junos OS.

**Description** Suspend a particular download instance.



NOTE: Only downloads in the active state can be paused.

**Options** **download-id**—(Required) The ID number of the download to be paused.

**Required Privilege Level** maintenance

**Related Documentation**

- request system download start on page 1541
- request system download resume on page 1540
- request system download abort on page 1537
- request system download clear on page 1538
- Device Configuration

**List of Sample Output** request system download pause on page 1539

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request system download pause

```
user@host> request system download pause 1
Paused download #1
```

## request system download resume

**Syntax** request system download resume *download-id* <max-rate>

**Release Information** Command introduced in Release 11.2 of Junos OS.

**Description** Resume a download that has been paused. Download instances that are not in progress because of an error or that have been explicitly paused by the user can be resumed by the user. The file will continue downloading from the point where it paused. By default, the download resumes with the same bandwidth specified with the **request system download start** command. The user can optionally specify a new (maximum) bandwidth with the **request system download resume** command.



NOTE: Only downloads in the paused and error states can be resumed.

**Options** **download-id**—(Required) The ID number of the download to be paused.

**max-rate**—(Optional) The maximum bandwidth for the download.

**Required Privilege Level** maintenance

**Related Documentation**

- request system download start on page 1541
- request system download pause on page 1539
- request system download abort on page 1537
- request system download clear on page 1538
- Device Configuration

**List of Sample Output** request system download resume on page 1540

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request system download resume

```
user@host> request system download resume 1
Resumed download #1
```


Copyright © 2013, Juniper Networks, Inc.

## request system download start

**Syntax** request system download start (*url* | *max-rate* | *save as* | *login* | *delay*)

**Release Information** Command introduced in Release 11.2 of Junos OS.

**Description** Creates a new download instance and identifies it with a unique integer called the download ID.

**Options**

**url**—(Required) The FTP or HTTP URL location of the file to be downloaded.

**max-rate**—(Optional) The maximum average bandwidth for the download. Numbers with the suffix k or K, m or M, and g or G are interpreted as kbps, mbps, or gbps, respectively.

**save-as**—(Optional) The filename to be used for saving the file in the **/var/tmp** location.

**login**—(Optional) The username and password for the server in the format **username:password**.

**delay**—(Optional) The number of hours after which the download should start.

**Required Privilege Level** maintenance

**Related Documentation**

- request system download pause on page 1539
- request system download resume on page 1540
- request system download abort on page 1537
- request system download clear on page 1538
- Device Configuration

**List of Sample Output** request system download start on page 1541

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request system download start

```
user@host> request system download start login user:passwd ftp://ftp-server//tftpboot/1m_file
max-rate 1k
Starting download #1
```

Copyright © 2013, Juniper Networks, Inc.

## request system firmware upgrade

**Syntax** request system firmware upgrade

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Upgrade firmware on a system.

**Options** **fpc**—Upgrade FPC ROM monitor.

**pic**—Upgrade PIC firmware.

**re**—Upgrade baseboard BIOS/FPGA. There is an active BIOS image and a backup BIOS image.

**vcpu**—Upgrade VCPU ROM monitor.

**Required Privilege Level** maintenance

**Related Documentation**
- Device Configuration

**List of Sample Output** request system firmware upgrade on page 1542

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request system firmware upgrade

```
user@host> request system firmware upgrade re bios
Part             Type           Tag Current   Available Status
                                    version   version
Routing Engine 0 RE BIOS        0   1.5       1.9       OK
Routing Engine 0 RE BIOS Backup 1   1.7       1.9       OK
Perform indicated firmware upgrade ? [yes,no] (no) yes

user@host> request system firmware upgrade re bios backup
Part             Type           Tag Current   Available Status
                                    version   version
Routing Engine 0 RE BIOS        0   1.5       1.9       OK
Routing Engine 0 RE BIOS Backup 1   1.7       1.9       OK
Perform indicated firmware upgrade ? [yes,no] (no) yes
```


Copyright © 2013, Juniper Networks, Inc.

## request system fips self-test

**Syntax** request system fips self-test

**Release Information** Command introduced in Junos OS Release 11.1.

**Description** Manually execute known answer test (KAT) self-tests to validate the output of cryptographic algorithms approved for the Federal Information Processing Standard (FIPS) and to test the integrity of some system modules.

This command is available on EX Series switches with Junos OS in FIPS mode and on routers with Junos-FIPS installed.

If a manually executed KAT fails, the system writes a log message to the system log messages file with details of the failure. Then the system enters FIPS error state (panic) and reboots.

If the KATs succeed, the system displays “Passed” for each successful test and updates the system log file to display the tests that were executed.

To display the system log file, enter the **file show /var/log/messages** command.

The KATs are also run automatically during the startup process and when you enable FIPS mode on a switch. If a test fails, the system is unable to start up and halts the boot process.

**Required Privilege Level** none

**List of Sample Output** request system fips self-test on page 1544

**Output Fields** When you issue this command, you are provided feedback on the status of your request.

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### request system fips self-test

```
user@switch> request system fips self-test Testing file integrity:
File integrity Known Answer Test:                  Passed
Testing crypto integrity:
   Crypto integrity Known Answer Test:              Passed
Testing kernel KATS:
   DES3-CBC Known Answer Test:                      Passed
   HMAC-SHA1 Known Answer Test:                     Passed
   HMAC-SHA2-256 Known Answer Test:                 Passed
   SHA-2 Known Answer Test:                         Passed
   AES128-CMAC Known Answer Test:                   Passed
   AES-CBC Known Answer Test:                       Passed
Testing libmd KATS:
   HMAC-SHA1 Known Answer Test:                     Passed
   HMAC-SHA2-256 Known Answer Test:                 Passed
Testing OpenSSL KATS:
   FIPS RNG Known Answer Test:                      Passed
   FIPS DSA Known Answer Test:                      Passed
   FIPS ECDSA Known Answer Test:                    Passed
   FIPS ECDH Known Answer Test:                     Passed
   FIPS RSA Known Answer Test:                      Passed
   DES3-CBC Known Answer Test:                      Passed
   HMAC-SHA1 Known Answer Test:                     Passed
   SHA-2 Known Answer Test:                         Passed
   AES-CBC Known Answer Test:                       Passed
   ECDSA-SIGN Known Answer Test:                    Passed
   KDF-IKE-V1 Known Answer Test:                    Passed
Testing SSH IPsec KATS:
   DES3-CBC Known Answer Test:                      Passed
   HMAC-SHA1 Known Answer Test:                     Passed
   HMAC-SHA2-256 Known Answer Test:                 Passed
   SHA-2 Known Answer Test:                         Passed
   AES-CBC Known Answer Test:                       Passed
   SSH-RSA-ENC Known Answer Test:                   Passed
   SSH-RSA-SIGN Known Answer Test:                  Passed
   KDF-IKE-V1 Known Answer Test:                    Passed
Expect an exec Authentication error...
exec: /opt/sbin/kats/cannot-exec.real: Authentication error
```


Copyright © 2013, Juniper Networks, Inc.

## request system license update

**Syntax** request system license update

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** Starts autoupdating license keys from the LMS server.

This command is supported on J-series devices.

**Options** **trial**—Starts autoupdating trial license keys from LMS server.

**Required Privilege Level** maintenance

**Related Documentation**

- Device Configuration
- UTM Basics for Security Devices
- Unified Threat Management

**List of Sample Output**

request system license update on page 1545
request system license update trial on page 1545

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request system license update

```
user@host> request system license update

Request to automatically update license keys from https://ae1.juniper.net has
been sent, use show system license to check status.
```

request system license update trial

```
user@host> request system license update trial

Request to automatically update trial license keys from https://ae1.juniper.net
has been sent, use show system license to check status.
```

Copyright © 2013, Juniper Networks, Inc.

## request system partition compact-flash

**Syntax** request system partition compact-flash

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Reboots the device and repartitions the compact flash. The compact flash is repartitioned only if it is possible to restore all the data on the compact flash. Otherwise, the operation is aborted, and a message is displayed indicating that the current disk usage needs to be reduced.

**Required Privilege Level** maintenance

**Related Documentation**
- Upgrades and Downgrades

**List of Sample Output**
request system partition compact-flash (If Yes) on page 1546
request system partition compact-flash (If No) on page 1546

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request system partition compact-flash (If Yes)

```
user@host> request system partition compact-flash
Are you sure you want to reboot
and partition the compact-flash ? [yes,no] yes
Initiating repartition operation.
The operation may take several minutes to complete.
System will reboot now...
<System reboots>
<Repartition operation is performed>
<System reboots and starts up normally>
```

### Sample Output

request system partition compact-flash (If No)

```
user@host> request system partition compact-flash
Are you sure you want to reboot
and partition the compact-flash ? [yes,no] no
```


Copyright © 2013, Juniper Networks, Inc.

## request system services dhcp

**Syntax** request system services dhcp (release *interface-name* | renew *interface-name)*

**Release Information** Command introduced in Release 8.5 of Junos OS.

**Description** Release or renew the acquired IP address for a specific interface.

To view the status of the Dynamic Host Configuration Protocol (DHCP) clients on the specified interfaces, enter the **show system services dhcp client** *interface-name* command.

**Options**

- **release** *interface-name* —Clears other resources received earlier from the server, and reinitializes the client state to INIT for the particular interface.
- **renew** *interface-name* —Reacquires an IP address from the server for the interface. When you use this option, the command sends a discover message if the client state is INIT and a renew request message if the client state is BOUND. For all other states it performs no action.

**Required Privilege Level** maintenance

**Related Documentation**

- dhcp on page 181
- show system services dhcp client on page 2259
- Device Configuration

**List of Sample Output**

request system services dhcp client release ge-1/0/1 on page 1547
request system services dhcp client renew ge-1/0/1 on page 1547

**Output Fields** This command produces no output.

### Sample Output

request system services dhcp client release ge-1/0/1

```
user@host> request system services dhcp client release ge-1/0/1
```

### Sample Output

request system services dhcp client renew ge-1/0/1

```
user@host> request system services dhcp client renew ge-1/0/1
```

Copyright © 2013, Juniper Networks, Inc.

## request system snapshot (Maintenance)

**Syntax** request system snapshot

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Back up the currently running and active file system partitions on the device.

**Options**

- factory— (Optional) Specifies that only the files shipped from the factory are included in the snapshot.
- media— (Optional) Specifies the media to be included in the snapshot:
  - internal— Copies the snapshot to internal media. This is the default.
  - usb— Copies the snapshot to the USB storage device.
  - external— Copies the snapshot to an external storage device. This option is available for the compact flash on the SRX650 Services Gateway.
- partition - (Default) Specifies that the target media should be repartitioned before the backup is saved to it.

NOTE: The target media is partitioned whether or not it is specified in the command, because this is a mandatory option.

- slice— (Optional) Takes a snapshot of the root partition the system has currently booted from to another slice in the same media.
  - alternate— (Optional) Stores the snapshot on the other root partition in the system.

NOTE: The slice option cannot be used along with the other request system snapshot options, because the options are mutually exclusive. If you use the factory, media, or partition option, you cannot use the slice option; if you use the slice option, you cannot use any of the other options.

**Required Privilege Level** maintenance

**Related Documentation**

- Upgrades and Downgrades

### Example

```
user@host# request system snapshot media usb partition

user@host# request system snapshot media usb partition factory
```


Copyright © 2013, Juniper Networks, Inc.

## request system software abort in-service-upgrade (ICU)

**Syntax** request system software abort in-service-upgrade

**Release Information** Command introduced in Release 11.2 of Junos OS.

**Description** Abort an in-band cluster upgrade (ICU). This command must be issued from a router session other than the one on which you issued the **request system in-service-upgrade** command that launched the ICU. If an ICU is in progress, this command aborts it. If the node is being upgraded, this command will cancel the upgrade. The command is also helpful in recovering the node in case of a failed ICU.

**Options** This command has no options.

**Required Privilege Level** view

**Related Documentation**

- request system software in-service-upgrade (Maintenance) on page 1551
- Upgrades and Downgrades

**List of Sample Output** request system software abort in-service-upgrade on page 1549

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request system software abort in-service-upgrade

```
user@host> request system software abort in-service-upgrade
In-Service-Upgrade aborted
```

Copyright © 2013, Juniper Networks, Inc.

## request system software add (Maintenance)

**Syntax** request system software add *package-name*

**Release Information** Partition option introduced in the command in Release 10.1. of Junos OS.

**Description** Installs the new software package on the device.

**Options**

- delay–restart — Installs the software package but does not restart the software process
- best-effort-load— Activate a partial load and treat parsing errors as warnings instead of errors
- no-copy — Installs the software package but does not saves the copies of package files
- no-validate— Does not check the compatibility with current configuration before installation starts
- partition — Formats and re-partitions the media before installation
- reboot— Reboots the device after installation is completed
- unlink—Removes the software package after successful installation
- validate—Checks the compatibility with current configuration before installation starts

**Required Privilege Level** maintenance

**Related Documentation**

- Device Configuration
- Upgrades and Downgrades

### Example

**user@host# request system software add junos-srxsme-10.0R2-domestic.tgz no-copy no-validate partition reboot**


Copyright © 2013, Juniper Networks, Inc.

## request system software in-service-upgrade (Maintenance)

**Syntax**

request system software in-service-upgrade *image_name*
<no-copy>
<no-sync>
<no-tcp-syn-check>
<no-validate>
<reboot>
<unlink>

**Release Information**

For SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices, command introduced in Release 9.6 of Junos OS and support for **reboot** as a required parameter added in Release 11.2R2 of Junos OS. For SRX100, SRX210, SRX220, SRX240, and SRX650 devices, command introduced in Release 11.2R2 of Junos OS.

**Description**

The in-service software upgrade (ISSU) feature allows a chassis cluster pair to be upgraded from supported Junos OS versions with a traffic impact similar to that of redundancy group failovers. Before upgrading, you should perform failovers so that all redundancy groups are active on only one device. We recommend that graceful restart for routing protocols be enabled before you initiate an ISSU.

For SRX100, SRX210, SRX220, SRX240, and SRX650 devices, you must use the **no-sync** parameter to perform an in-band cluster upgrade (ICU). This allows a chassis cluster pair to be upgraded with a minimal service disruption of approximately 30 seconds.

**Options**

- *image_name*—Location and name of the software upgrade package to be installed.
- **no-copy**—(Optional) Installs the software upgrade package but does not save the copies of package files.
- **no-sync**—Stops the flow state from synchronizing when the old secondary node has booted with a new Junos OS image.

  This parameter applies to SRX100, SRX210, SRX220, SRX240, and SRX650 devices only. It is required for an ICU.
- **no-tcp-syn-check**—(Optional) Creates a window wherein the TCP SYN check for the incoming packets is disabled. The default value for the window is 7200 seconds (2 hours).

  This parameter applies to SRX100, SRX210, SRX220, SRX240, and SRX650 devices only.
- **no-validate**—(Optional) Disables the configuration validation step at installation. The system behavior is similar to that of the **request system software add** command.

  This parameter applies to SRX100, SRX210, SRX220, SRX240, and SRX650 devices only.
- **reboot**—Reboots each device in the chassis cluster pair after installation is completed.

Copyright © 2013, Juniper Networks, Inc.

This parameter applies to SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices only. It is required for an ISSU. (The devices in a cluster are automatically rebooted following an ICU.)

- **unlink**—(Optional) Removes the software package after successful installation.

**Required Privilege Level** maintenance

**Related Documentation**
- Chassis Cluster for Security Devices

**List of Sample Output**
request system software in-service-upgrade (High-End SRX Series Devices) on page 1552
request system software in-service-upgrade (Branch SRX Series Devices) on page 1553

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

## Sample Output

request system software in-service-upgrade

```
user@host> request system software in-service-upgrade
/var/tmp/junos-srx1k3k-11.2R2.5-domestic.tgz no-copy reboot
Chassis ISSU Started
node0:
```


Copyright © 2013, Juniper Networks, Inc.

(High-End SRX Series Devices)

```
--------------------------------------------------------------------------
Chassis ISSU Started
ISSU: Validating Image
Inititating in-service-upgrade

node0:
--------------------------------------------------------------------------
Inititating in-service-upgrade
Checking compatibility with configuration
mgd: commit complete
Validation succeeded
ISSU: Preparing Backup RE
Finished upgrading secondary node node0
Rebooting Secondary Node

node0:
--------------------------------------------------------------------------
Shutdown NOW!
[pid 3257]
ISSU: Backup RE Prepare Done
Waiting for node0 to reboot.
node0 booted up.
Waiting for node0 to become secondary
node0 became secondary.
Waiting for node0 to be ready for failover
ISSU: Preparing Daemons
Secondary node0 ready for failover.
Failing over all redundancy-groups to node0
ISSU: Preparing for Switchover
Initiated failover for all the redundancy groups to node1
Waiting for node0 take over all redundancy groups

Exiting in-service-upgrade window

node0:
--------------------------------------------------------------------------
Exiting in-service-upgrade window
Exiting in-service-upgrade window
Chassis ISSU Aborted

node0:
--------------------------------------------------------------------------
Chassis ISSU Ended
ISSU completed successfully, rebooting...
Shutdown NOW!
[pid 4294]
```

## Sample Output

request system software in-service-upgrade

```
user@host> request system software in-service-upgrade
/var/tmp/junos-srxsme-11.2R2.2-domestic.tgz no-sync
ISSU: Validating package
WARNING: in-service-upgrade shall reboot both the nodes
```

(Branch SRX Series Devices)

```
          in your cluster. Please ignore any subsequent
          reboot request message
ISSU: start downloading software package on secondary node
Pushing bundle to node1
NOTICE: Validating configuration against junos-srxsme-11.2R2.2-domestic.tgz.
NOTICE: Use the 'no-validate' option to skip this if desired.
Formatting alternate root (/dev/ad0s1a)...
/dev/ad0s1a: 630.5MB (1291228 sectors) block size 16384, fragment size 2048
        using 4 cylinder groups of 157.62MB, 10088 blks, 20224 inodes.
super-block backups (for fsck -b #) at:
 32, 322848, 645664, 968480
Checking compatibility with configuration
Initializing...
Verified manifest signed by PackageProduction_11_2_0
Verified junos-11.2R2.2-domestic signed by PackageProduction_11_2_0
Using junos-11.2R2.2-domestic from
/altroot/cf/packages/install-tmp/junos-11.2R2.2-domestic
Copying package ...
Saving boot file package in /var/sw/pkg/junos-boot-srxsme-11.2R2.2.tgz
Verified manifest signed by PackageProduction_11_2_0
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
cp: /cf/var/validate/chroot/var/etc/resolv.conf and /etc/resolv.conf are identical
 (not copied).
cp: /cf/var/validate/chroot/var/etc/hosts and /etc/hosts are identical (not
copied).
mgd: commit complete
Validation succeeded
Installing package '/altroot/cf/packages/install-tmp/junos-11.2R2.2-domestic' ...
Verified junos-boot-srxsme-11.2R2.2.tgz signed by PackageProduction_11_2_0
Verified junos-srxsme-11.2R2.2-domestic signed by PackageProduction_11_2_0
Saving boot file package in /var/sw/pkg/junos-boot-srxsme-11.2R2.2.tgz
JUNOS 11.2R2.2 will become active at next reboot
WARNING: A reboot is required to load this software correctly
WARNING:     Use the 'request system reboot' command
WARNING:         when software installation is complete
Saving state for rollback ...
ISSU: finished upgrading on secondary node node1
ISSU: start upgrading software package on primary node
NOTICE: Validating configuration against junos-srxsme-11.2R2.2-domestic.tgz.
NOTICE: Use the 'no-validate' option to skip this if desired.
Formatting alternate root (/dev/ad0s1a)...
/dev/ad0s1a: 630.9MB (1292176 sectors) block size 16384, fragment size 2048
        using 4 cylinder groups of 157.75MB, 10096 blks, 20224 inodes.
super-block backups (for fsck -b #) at:
 32, 323104, 646176, 969248
Checking compatibility with configuration
Initializing...
Verified manifest signed by PackageProduction_11_2_0
Verified junos-11.2R2.2-domestic signed by PackageProduction_11_2_0
Using junos-11.2R2.2-domestic from
/altroot/cf/packages/install-tmp/junos-11.2R2.2-domestic
Copying package ...
Saving boot file package in /var/sw/pkg/junos-boot-srxsme-11.2R2.2.tgz
Verified manifest signed by PackageProduction_11_2_0
Hardware Database regeneration succeeded
Validating against /config/juniper.conf.gz
cp: /cf/var/validate/chroot/var/etc/resolv.conf and /etc/resolv.conf are identical
 (not copied).
cp: /cf/var/validate/chroot/var/etc/hosts and /etc/hosts are identical (not
copied).
```


Copyright © 2013, Juniper Networks, Inc.

```
mgd: commit complete
Validation succeeded
Installing package '/altroot/cf/packages/install-tmp/junos-11.2R2.2-domestic' ...
Verified junos-boot-srxsme-11.2R2.2.tgz signed by PackageProduction_11_2_0
Verified junos-srxsme-11.2R2.2-domestic signed by PackageProduction_11_2_0
Saving boot file package in /var/sw/pkg/junos-boot-srxsme-11.2R2.2.tgz
JUNOS 11.2R2.2 will become active at next reboot
WARNING: A reboot is required to load this software correctly
WARNING:     Use the 'request system reboot' command
WARNING:         when software installation is complete
Saving state for rollback ...
ISSU: failover all redundancy-groups 1...n to primary node
node0:
--------------------------------------------------------------------------
Successfully reset all redundancy-groups priority back to configured ones.
Redundancy-groups-0 will not be reset and the primaryship remains unchanged.

node1:
--------------------------------------------------------------------------
Successfully reset all redundancy-groups priority back to configured ones.
Redundancy-groups-0 will not be reset and the primaryship remains unchanged.

node0:
--------------------------------------------------------------------------
Initiated manual failover for all redundancy-groups to node0
Redundancy-groups-0 will not failover and the primaryship remains unchanged.
ISSU: rebooting Secondary Node

node1:
--------------------------------------------------------------------------
Shutdown NOW!
[pid 7023]
ISSU: Waiting for secondary node node1 to reboot.
ISSU: node 1 went down
ISSU: Waiting for node 1 to come up
ISSU: node 1 came up
ISSU: secondary node node1 booted up.
Shutdown NOW!
[pid 45056]
```

Copyright © 2013, Juniper Networks, Inc.

## request system software reboot

**Syntax** request system software reboot *<at time> <in minutes><media><message 'text">*

**Release Information** Command introduced in Release 10.1 of Junos OS.

**Description** Reboots the software.

**Options**

- at time— Specifies the time at which to reboot the device . You can specify time in one of the following ways:
  - now— Reboots the device immediately. This is the default.
  - +minutes— Reboots the device in the number of minutes from now that you specify.
  - yymmddhhmm— Reboots the device at the absolute time on the date you specify. Enter the year, month, day, hour (in 24-hour format), and minute.
  - hh:mm— Reboots the device at the absolute time you specify, on the current day. Enter the time in 24-hour format, using a colon (:) to separate hours from minutes.
- in minutes — Specifies the number of minutes from now to reboot the device. This option is a synonym for the at +minutes option
- media type— Specifies the boot device to boot the device from:
  - internal— Reboots from the internal media. This is the default.
  - usb— Reboots from the USB storage device.
  - external— Reboots from the external compact flash. This option is available on the SRX650 Services Gateway.
- message "text"— Provides a message to display to all system users before the device reboots.

**Required Privilege Level** maintenance

**Related Documentation**

- Device Configuration
- Upgrades and Downgrades

### Example

**user@host# request system reboot at 5 in 50 media internal message stop**


Copyright © 2013, Juniper Networks, Inc.

## request system software rollback (Maintenance)

**Syntax** request system software rollback

**Release Information** Command introduced in Release 10.1 of Junos OS.

**Description** Revert to the software that was loaded at the last successful **request system software add** command.

**Required Privilege Level** maintenance

**Related Documentation**

- Device Configuration
- Upgrades and Downgrades

### Example

**user@host# request system software rollback**

Copyright © 2013, Juniper Networks, Inc.

## request wan-acceleration login

**Syntax** request wan-acceleration login fpc *slot-number*

**Release Information** Command introduced in Release 8.5 of Junos OS.

**Description** Log in to the WXC Integrated Services Module (ISM 200) from J Series devices running Junos OS to access the WXOS CLI.

To view the slot number, enter the **show chassis fpc pic-status** command. You require interface permission for read-only access, and interface-control and configure permission for read-write access.

**Options** fpc *slot-number* —Higher number of the two slots in the device chassis occupied by the WXC ISM 200.

**Required Privilege Level** maintenance

**Related Documentation**
- show chassis fpc (View) on page 1601
- show wan-acceleration status on page 2272

**List of Sample Output**
request wan-acceleration login fpc 3 (permissions set) on page 1558
request wan-acceleration login fpc 3 (permissions not set) on page 1558

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

This user has a user account with interface-control and configure permissions set for read-write access to WXOS or has interface permissions set for read-only access.

request wan-acceleration login fpc 3 (permissions set)

```
user@host> request wan-acceleration login fpc 3
Copyright 2001-2006 Juniper Networks, Inc. All Rights Reserved.
```

### Sample Output

This user has a user account without the correct permissions set and does not gain access to WXOS.

request wan-acceleration login fpc 3 (permissions not set)

```
user@host> request wan-acceleration login fpc 3
FPCLOGIN_LOGIN_FAILURE: fpclogin failed: user permissions not set.
```


Copyright © 2013, Juniper Networks, Inc.

## request wlan access-point firmware upgrade

**Syntax** request wlan access-point firmware upgrade ( *name* | all ) file *image*

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Upgrade access point software.

**Options**
- *name*—Upgrade software on a specific access point on the services gateway.
- **all**—Upgrade software on all access points on the services gateway.
- **file**—Software to be upgraded onto the access point(s).

**Required Privilege Level** maintenance

**Related Documentation**
- WLAN Configuration and Administration

**List of Sample Output**
request wlan access-point firmware upgrade wap-3 on page 1559
request wlan access-point firmware upgrade all on page 1559

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request wlan access-point firmware upgrade wap-3

```
user@host> request wlan access-point firmware upgrade wap-3 file
/var/tmp/upgrade_10_1_0_1.tar
Firmware upgraded initiated for access point wap-3.
Upgrade will take approximately 6 minutes.
Access point will be unavailable during upgrade.
Please do not power down the access point while upgrade is in progress.
```

### Sample Output

request wlan access-point firmware upgrade all

```
user@host> request wlan access-point firmware upgrade all file /var/tmp/upgrade_10_1_0_1.tar
Firmware upgraded initiated for all access points.
```

## request wlan access-point restart

**Syntax** request wlan access-point restart *name*

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Restart the access point.

**Options** *name*—Restart a specific access point on the services gateway.

**Required Privilege Level** maintenance

**Related Documentation**
- WLAN Configuration and Administration

**List of Sample Output** request wlan access-point restart wap-3 on page 1560

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

### Sample Output

request wlan access-point restart wap-3

```
user@host> request wlan access-point restart wap-3
Successfully restarted the access point.
```


Copyright © 2013, Juniper Networks, Inc.

## request wireless-wan adapter firmware upgrade

**Syntax** request wireless-wan adapter firmware upgrade

**Release Information** Command introduced in Junos Release 11.4R2.

**Description** Upgrade the firmware on the CX111 adapter.

**Options** **auto**— Automatically upgrades the firmware. In this mode, the most current firmware image from the Junos Cloud server is used for the upgrade. The 3G WAN link on CX111 adpater must be connected.

**manual**—Manually upgrades the firmware. In this mode, you must provide the URL for the firmware image to be used for upgrade.

Firmware upgrade is possible with or without 3G WAN link connection on CX111 adapter.

The URL can point to a HTTP server running on:

- **SRX Series device**

  If 3G WAN link on CX111 adapter is not connected, then firmware image can be copied to SRX device for upgrade, and the web server on an SRX Series device can be used for upgrade.

Steps for firmware upgrade with the file path on an SRX Series device:

1. Configure HTTP server on the port to which CX111 adapter is connected on SRX device.

   For example: set system services web-management http interface <*physical interface connected to CX111*>

   

   NOTE: The upgrade from web server running on an SRX Series device works, when the server is running on the same subnet as the management VLAN subnet of CX111 adapter.

2. Copy the firmware image to **/jail/var/tmp/** location on SRX device.

   

   NOTE: Use binary mode to transfer the firmware image to the SRX device. The filename must have .bin as suffix.

3. Enter the firmware upgrade command with the URL pointing to the firmware image on an SRX Series device.

   For example: http://<*ip-address-of-http-port*> /cx_fw/ <*image.bin*>

Copyright © 2013, Juniper Networks, Inc.

- **External HTTP server**

  If 3G WAN link on CX111 adapter is connected, then HTTP URL pointing to firmware image on public web server can be used for upgrade.

Steps for firmware upgrade with the file on external HTTP server

1. Copy the firmware image file to the external web server HTTP root directory.
2. Enter the firmware upgrade command with the URL listed as follows:

   For example: http://*<web-server-address>*/*<image.bin>*



NOTE: If there are packet drops to the external web server over CX111 adapter 3G WAN connection, then the firmware upgrade might fail.

**Required Privilege Level** maintenance

**Related Documentation**
- show wireless-wan adapter on page 2278
- WLAN Configuration and Administration

**List of Sample Output**
request wireless-wan adapter firmware upgrade on page 1562
request wireless-wan adapter firmware upgrade auto on page 1562
request wireless-wan adapter firmware upgrade manual on page 1562

**Output Fields** When you enter this command, you are shown the options.

## Sample Output

request wireless-wan adapter firmware upgrade

```
user@host> request wireless-wan adapter firmware upgrade
Possible completions
auto
manual
```

request wireless-wan adapter firmware upgrade auto

```
user@host> request wireless-wan adapter firmware upgrade auto CX111-0
Firmware upgrade initiated for adapter CX111-0.
Upgrade will take few minutes.
Use 'show wireless-wan adapter firmware upgrade status CX111-0' to view upgrade
status. Adapter will be unavailable during upgrade. Please do not power down the
 Adapter while upgrade is in progress.
```

request wireless-wan adapter firmware upgrade manual

```
user@host> request wireless-wan adapter firmware upgrade manual CX111-0 url
http://192.168.0.10/cx_fw/u_cx111_1.1.1.bin
Firmware upgrade initiated for adapter CX111-0.
Upgrade will take few minutes.
Use 'show wireless-wan adapter firmware upgrade status CX111-0' to view upgrade
status. Adapter will be unavailable during upgrade. Please do not power down the
 Adapter while upgrade is in progress.
```


Copyright © 2013, Juniper Networks, Inc.

CHAPTER 27

# Restart Commands

This section contains the following topics:


- Restart Commands Overview on page 1563


## Restart Commands Overview

Use the **restart** operational commands to restart software processes on the device. Operational commands are organized alphabetically.

**Related Documentation**

- CLI User Guide
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

Copyright © 2013, Juniper Networks, Inc.

## restart (Reset)

**Syntax**

restart
<audit-process | chassis-control | class-of-service | **dhcp** | **dialer-services** |event-processing | firewall | **group-key-server** | interface-control | ipsec-key-management | **isdn-signaling** | l2ald | l2-learning | mib-process | pgm | ppp | pppoe | remote-operations | routing <logical-system *logical-system-name*> | sampling | service-deployment | snmp | **usb-control** | **wan-acceleration** | **web-management**>
<gracefully | immediately | soft>

**Release Information**

Command introduced before Release 7.4 of Junos OS.
**wan-acceleration** option added in Release 8.5 of Junos OS.
**group-key-server** option added in Release 10.2 of Junos OS.

**Description**

Restart a Junos OS process.



CAUTION: Never restart a software process unless instructed to do so by a customer support engineer. A restart might cause the router to drop calls and interrupt transmission, resulting in possible loss of data.

**Options**

- dhcp—(Optional) Restart the software process for a Dynamic Host Configuration Protocol (DHCP) server. A DHCP server allocates network IP addresses and delivers configuration settings to client hosts without user intervention.
- dialer-services—(Optional) Restart the ISDN dial out process.
- group-key-server—(Optional) Restart the group VPN server process. The group VPN server loses all its data, including TEK and KEK keys, when it restarts. New keys are generated, but the keys are not available to group members until they reregister.
- isdn-signaling—(Optional) Restart the ISDN signaling process, which initiates ISDN connections.
- usb-control—(Optional) Restart the USB control process.
- wan-acceleration—(J Series devices only.) (Optional) Restart the WAN acceleration process. If the WXC Integrated Services Module (ISM 200) is not accessible, or is not responding, you can use this command to restart the WAN acceleration process.
- web-management—(Optional) Restart the Web management process.

**Required Privilege Level**

reset

**List of Sample Output**

restart interfaces on page 1565

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

**restart interfaces**

```
user@host> restart interfaces
interfaces process terminated
interfaces process restarted
```

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

CHAPTER 28

# Show Commands

This section contains the following topics:


- Show Commands Overview on page 1567


## Show Commands Overview

Use the **show** operational commands to review and verify the validity of your configurations and monitor device operation. Operational commands are organized alphabetically.

**Related Documentation**

- Junos OS Operational Mode Commands
- Junos OS Operational Mode Commands
- Junos OS Operational Mode Commands
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*

Copyright © 2013, Juniper Networks, Inc.

## show accounting

**Syntax**

**show accounting**
**<profile>**
**<records>**

**Release Information**

Command introduced in Release 11.4 of Junos OS.

**Description**

Display accounting profile information and records.

**Options**

- profile—Display accounting profile information.
- records—Display accounting records.

**Required Privilege Level**

view

**Related Documentation**

- show firewall (View) on page 1656
- clear firewall on page 1374


Copyright © 2013, Juniper Networks, Inc.

## show accounting profile (View)

**Syntax** show accounting profile

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Display sampled accounting profile.

**Options**
- profile—Display profile name.

**Required Privilege Level** view

**Related Documentation**
- show accounting on page 1568
- show accounting records (View) on page 1570
- show firewall (View) on page 1656
- clear firewall on page 1374

Copyright © 2013, Juniper Networks, Inc.

## show accounting records (View)

**Syntax** show accounting records *profile-name*
<since *time*>
<utc_timestamp>

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Display sampled accounting records.

**Options** *profile-name*—Name of the accounting profile.

since *time*—Display accounting statistics since the specified time (*YYYY-MM-DD-HH:MM:SS*)

utc_timestamp—Display the timestamp in Coordinated Universal Time (UTC) format.

**Required Privilege Level** view

**Related Documentation**

- show accounting on page 1568
- show accounting profile (View) on page 1569
- show firewall (View) on page 1656
- clear firewall on page 1374


Copyright © 2013, Juniper Networks, Inc.

## show bgp neighbor (View)

**Syntax** **show bgp neighbor**
< *neighbor-address*>
<**instance** *instance* >

**Release Information** Command modified in Release 8.5 of Junos OS.

**Description** Display the state of the specified Border Gateway Protocol (BGP) neighbor. If a peer is forced to Idle state because of license check failure, the output displays the state and the reason—**LicenseCheckFailed**.

**Options**
- **instance** ***instance***—(Optional) Display peer information for a particular routing instance.
- ***neighbor-address***—(Optional) Display information for only the BGP peer at the specified IP address.

**Required Privilege Level** view

**Related Documentation**
- MPLS for Security Devices
- Junos OS Operational Mode Commands

**List of Sample Output**
show bgp neighbor 5.5.5.2 on page 1574
show bgp neighbor instance master on page 1574

**Output Fields** Table 8 on page 1571 lists the output fields for the **show bgp neighbor** command. Output fields are listed in the approximate order in which they appear.

### Table 8: show bgp neighbor Output Fields

| Field Name | Field Description |
|---|---|
| **Peer** | Address of the BGP neighbor. The address is followed by the neighbor's port number. |
| **AS** | AS number of the peer. |
| **Local** | Address of the local device. The address is followed by the peer's port number. |
| **Type** | Type of peer: Internal or External. |

Copyright © 2013, Juniper Networks, Inc.

Table 8: show bgp neighbor Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **State** | Current state of the BGP session:<br>• **Active**—BGP is initiating a transport protocol connection in an attempt to connect to a peer. If the connection is successful, BGP sends an open message.<br>• **Connect**—BGP is waiting for the transport protocol connection to complete.<br>• **Established**—The BGP session has been established, and the peers are exchanging update messages.<br>• **Idle**—Either the BGP license check failed, or this is the first stage of a connection and BGP is waiting for a Start event.<br>• **OpenConfirm**—BGP has acknowledged receipt of an open message from the peer and is waiting to receive a keepalive or notification message.<br>• **OpenSent**—BGP has sent an open message and is waiting to receive an open message from the peer. |
| **Flags** | Internal BGP flags:<br>• **Aggregate Label**—BGP has aggregated a set of incoming labels (labels received from the peer) into a single forwarding label.<br>• **CleanUp**—The peer session is being shut down.<br>• **Delete**—This peer has been deleted.<br>• **Idled**—This peer has been permanently idled.<br>• **Initializing**—The peer session is initializing.<br>• **SendRtn**—Messages are being sent to the peer.<br>• **Sync**—This peer is synchronized with the rest of the peer group.<br>• **TryConnect**—Another attempt is being made to connect to the peer.<br>• **Unconfigured**—This peer is not configured.<br>• **WriteFailed**—An attempt to write to this peer failed.<br>• **Last State**—Previous state of the BGP session. |
| **Last State** | Previous state of the BGP session. |
| **Last Event** | Last activity that occurred in the BGP session:<br>• **Closed**—The BGP session closed.<br>• **ConnectRetry**—The transport protocol connection failed, and BGP is trying again to connect.<br>• **HoldTime**—The session ended because the hold timer expired.<br>• **KeepAlive**—The local device sent a BGP keepalive message to the peer.<br>• **Open**—The local device sent a BGP open message to the peer.<br>• **OpenFail**—The local device did not receive an acknowledgment of a BGP open message from the peer.<br>• **RecvKeepAlive**—The local device received a BGP keepalive message from the peer.<br>• **RecvNotify**—The local device received a BGP notification message from the peer.<br>• **RecvOpen**—The local device received a BGP open message from the peer.<br>• **RecvUpdate**—The local device received a BGP update message from the peer.<br>• **Start**—The peering session started.<br>• **Stop**—The peering session stopped.<br>• **TransportError**—A TCP error occurred. |


Copyright © 2013, Juniper Networks, Inc.

Table 8: show bgp neighbor Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Last Error** | Last error that occurred in the BGP session:<br>• **Cease**—An error occurred, such as a version mismatch, that caused the session to close.<br>• **Finite State Machine Error**—In setting up the session, BGP received a message that it did not understand.<br>• **Hold Time Expired**—The session's hold time expired.<br>• **Message Header Error**—The header of a BGP message was malformed.<br>• **Open Message Error**—A BGP open message contained an error.<br>• **None**—No errors occurred in the BGP session.<br>• **Update Message Error**—A BGP update message contained an error. |
| **Export** | Name of the export policy that is configured on the peer. |
| **Import** | Name of the import policy that is configured on the peer. |
| **Options** | Configured BGP options:<br>• **AddressFamily**—Configured address family: inet or inet-vpn.<br>• **GracefulRestart**—Graceful restart is configured.<br>• **HoldTime**—Hold time configured with the **hold-time** statement. The hold time is three times the interval at which keepalive messages are sent.<br>• **Local Address**—Address configured with the **local-address** statement.<br>• **NLRI**—Configured multicast BGP state for the BGP group: multicast, unicast, or both if you have configured **nlri any**.<br>• **Peer AS**—Configured peer autonomous system (AS).<br>• **Preference**—Preference value configured with the **preference** statement.<br>• **Refresh**—Configured to refresh automatically when the policy changes.<br>• **Rib-group**—Configured routing table group. |
| **Address families configured** | Names of configured address families for the VPN. |
| **Local Address** | Address of the local device. |
| **Holdtime** | Hold time configured with the **hold-time** statement. The hold time is three times the interval at which keepalive messages are sent. |
| **Preference** | Preference value configured with the **preference** statement. |
| **Number of flaps** | Number of times the BGP session has gone down and then come back up. |
| **Trace file** | Name of the file to receive the output of the tracing operation. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show bgp neighbor 5.5.5.2

```
user@host> show bgp neighbor 5.5.5.2
  Type: Internal    State: Idle (LicenseCheckFailed)   Flags: <ImportEval Sync>
Peer: 5.5.5.2 AS 200           Local: unspecified AS 200
  Type: Internal    State: Idle (LIcenseCheckFailed)       (route reflector
client)Flags: <ImportEval>
  Last State: Idle          Last Event: Start
  Last Error: None
  Options: <Preference LogUpDown Cluster AddressFamily PeerAS Rib-group Refresh>

  Address families configured: inet-unicast inet-vpn-unicast l2vpn-signaling
  Holdtime: 90 Preference: 170
  Number of flaps: 0
  Trace options:  all
  Trace file: /var/log/bgp size 131072 files 10
```

## Sample Output

### show bgp neighbor instance master

```
user@host> show bgp neighbor instance master
Peer: 5.5.5.1 AS 200           Local: 5.5.5.2 AS 200
  Type: Internal    State: Idle (LicenseCheckFailed)         Flags: <>
  Last State: Idle          Last Event: Start
  Last Error: Cease
  Export: [ static ]
  Options: <Preference LocalAddress LogUpDown AddressFamily PeerAS Rib-group
Refresh>
  Address families configured: inet-unicast inet-vpn-unicast
  Local Address: 5.5.5.2 Holdtime: 90 Preference: 170
  Number of flaps: 4
  Last flap event: RecvUpdate
  Error: 'Update Message Error' Sent: 3 Recv: 0
  Error: 'Cease' Sent: 2 Recv: 0
  Trace file: /var/log/bgp size 131072 files 10
```


Copyright © 2013, Juniper Networks, Inc.

## show configuration chassis cluster traceoptions

**Syntax** show configuration chassis cluster traceoptions

**Release Information** Command introduced in Release 12.1 of Junos OS.

**Description** Display tracing options for the chassis cluster redundancy process.

**Required Privilege Level** view

**Related Documentation**
- Chassis Cluster for Security Devices
- traceoptions (Chassis Cluster) on page 106

**List of Sample Output** show configuration chassis cluster traceoptions on page 1575

**Output Fields** Table 9 on page 1575 lists the output fields for the **show configuration chassis cluster traceoptions** command. Output fields are listed in the approximate order in which they appear.

Table 9: show configuration chassis cluster traceoptions Output Fields

| Field Name | Field Description |
|---|---|
| **file** | Name of the file that receives the output of the tracing operation. |
| **size** | Size of each trace file. |
| **files** | Maximum number of trace files. |

### Sample Output

show configuration chassis cluster traceoptions

```
user@host> show configuration chassis cluster traceoptions
file chassis size 10k files 300;
level all;
```

Copyright © 2013, Juniper Networks, Inc.

## show chassis alarms

**Syntax** show chassis alarms

**Release Information** Command introduced in Junos OS Release 11.1 for SRX Series devices.

**Description** Display information about the conditions that have been configured to trigger alarms.

**Options** This command has no options.

**Additional Information** You cannot clear the alarms for chassis components. Instead, you must remedy the cause of the alarm. When a chassis alarm is lit, it indicates that you are running the device in a manner that we do not recommend.

On routers, you can manually silence external devices connected to the alarm relay contacts by pressing the alarm cutoff button, located on the craft interface. Silencing the device does not remove the alarm messages from the display (if present on the router) or extinguish the alarm LEDs. In addition, new alarms that occur after you silence an external device reactivate the external device.

In Junos OS Release 11.1 and later, alarms for fans also show the slot number of the fans in the CLI output.

**Required Privilege Level** view

**Related Documentation**

- show system alarms on page 2246
- Device and Routing Operations Monitoring

**List of Sample Output** show chassis alarms on page 1577

**Output Fields** Table 10 on page 1576 lists the output fields for the **show chassis alarms** command. Output fields are listed in the approximate order in which they appear.

### Table 10: show chassis alarms Output Fields

| Field Name | Field Description |
|---|---|
| **Alarm time** | Date and time the alarm was first recorded. |
| **Class** | Severity class for this alarm: Minor or Major. |
| **Description** | Information about the alarm. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show chassis alarms

```
user@host> show chassis alarms
4 alarms currently active
Alarm time               Class  Description
2012-05-29 16:47:18 UTC  Major  /var partition usage crossed critical threshold
2012-05-29 16:47:18 UTC  Minor  /var partition usage crossed high threshold
2012-05-29 16:47:18 UTC  Major  /root partition usage crossed critical threshold
2012-05-29 16:47:18 UTC  Minor  /root partition usage crossed high threshold
```

Copyright © 2013, Juniper Networks, Inc.

## show chassis cluster control-plane statistics

**Syntax** **show chassis cluster control-plane statistics**

**Release Information** Command introduced in Release 9.3 of Junos OS. Output changed to support dual control ports in Release 10.0 of Junos OS.

**Description** Display information about chassis cluster control plane statistics.

**Required Privilege Level** view

**Related Documentation**
- Chassis Cluster for Security Devices
- clear chassis cluster control-plane statistics on page 1358

**List of Sample Output**
show chassis cluster control-plane statistics on page 1579
show chassis cluster control-plane statistics (SRX3000 and SRX5000 line devices) on page 1579

**Output Fields** Table 11 on page 1578 lists the output fields for the **show chassis cluster control-plane statistics** command. Output fields are listed in the approximate order in which they appear.

Table 11: show chassis cluster control-plane statistics Output Fields

| Field Name | Field Description |
|---|---|
| **Control link statistics** | Statistics of the control link used by chassis cluster traffic. Statistics for **Control link 1** are displayed when you use dual control links (SRX3000 and SRX5000 lines only).<br>• **Heartbeat packets sent**—Number of heartbeat messages sent on the control link.<br>• **Heartbeat packets received**—Number of heartbeat messages received on the control link.<br>• **Heartbeat packet errors**—Number of heartbeat packets received with errors on the control link. |
| **Fabric link statistics** | Statistics of the fabric link used by chassis cluster traffic. Statistics for **Child Link 1** are displayed when you use dual fabric links.<br>• **Probes sent**—Number of probes sent on the fabric link.<br>• **Probes received**—Number of probes received on the fabric link. |
| **Switch fabric link statistics** | Statistics of the switch fabric link used by chassis cluster traffic.<br>• **Probe state**—State of the probe, **UP** or **DOWN**.<br>• **Probes sent**—Number of probes sent.<br>• **Probes received**—Number of probes received.<br>• **Probe recv error** —Error in receiving probe.<br>• **Probe send error**—Error in sending probe. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show chassis cluster control-plane statistics

```
user@host> show chassis cluster control-plane statistics
Control link statistics:
    Control link 0:
        Heartbeat packets sent: 11646
        Heartbeat packets received: 8343
        Heartbeat packet errors: 0
Fabric link statistics:
    Child link 0
        Probes sent: 11644
        Probes received: 8266
   Switch fabric link statistics:
    Probe state : DOWN
    Probes sent: 8145
    Probes received: 8013
    Probe recv errors: 0
    Probe send errors: 0
```

## Sample Output

show chassis cluster control-plane statistics (SRX3000 and SRX5000 line devices)

```
user@host> show chassis cluster control-plane statistics
Control link statistics:
    Control link 0:
        Heartbeat packets sent: 258698
        Heartbeat packets received: 258693
        Heartbeat packet errors: 0
   Control link 1:
        Heartbeat packets sent: 258698
        Heartbeat packets received: 258693
        Heartbeat packet errors: 0
Fabric link statistics:
    Child link 0
        Probes sent: 258690
        Probes received: 258690
    Child link 1
        Probes sent: 258505
        Probes received: 258505
```

Copyright © 2013, Juniper Networks, Inc.

## show chassis cluster data-plane interfaces

**Syntax** **show chassis cluster data-plane interfaces**

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display the status of the data plane interface (also known as a fabric interface) in a chassis cluster configuration.

**Required Privilege Level** view

**Related Documentation**
- Chassis Cluster for Security Devices

**List of Sample Output** show chassis cluster data-plane interfaces on page 1580

**Output Fields** Table 12 on page 1580 lists the output fields for the **show chassis cluster data-plane interfaces** command. Output fields are listed in the approximate order in which they appear.

Table 12: show chassis cluster data-plane interfaces Output Fields

| Field Name | Field Description |
|---|---|
| **fab0/fab1** | Name of the logical fabric interface.<br>• **Name**—Name of the physical Ethernet interface.<br>• **Status**—State of the fabric interface: **up** or **down**. |

### Sample Output

**show chassis cluster data-plane interfaces**

```
user@host> show chassis cluster data-plane interfaces
fab0:
    Name                Status
    ge-2/1/9            up
    ge-2/2/5            up
fab1:
    Name                Status
    ge-8/1/9            up
    ge-8/2/5            up
```


Copyright © 2013, Juniper Networks, Inc.

## show chassis cluster data-plane statistics

**Syntax** **show chassis cluster data-plane statistics**

**Release Information** Command introduced in Release 9.3 of Junos OS.

**Description** Display information about chassis cluster data plane statistics.

**Required Privilege Level** view

**Related Documentation**
- Chassis Cluster for Security Devices
- clear chassis cluster data-plane statistics on page 1359
- Application Layer Gateways for Security Devices

**List of Sample Output** show chassis cluster data-plane statistics on page 1582

**Output Fields** Table 13 on page 1581 lists the output fields for the **show chassis cluster data-plane statistics** command. Output fields are listed in the approximate order in which they appear.

### Table 13: show chassis cluster data-plane statistics Output Fields

| Field Name | Field Description |
|---|---|
| Services Synchronized | • **Service name**—Name of the service.<br>• **Rtos sent**—Number of runtime objects (RTOs) sent.<br>• **Rtos received**—Number of RTOs received.<br>• **Translation context**—Messages synchronizing Network Address Translation (NAT) translation context.<br>• **Incoming NAT**—Messages synchronizing incoming Network Address Translation (NAT) service.<br>• **Resource manager**—Messages synchronizing resource manager groups and resources.<br>• **Session create**—Messages synchronizing session creation.<br>• **Session close**—Messages synchronizing session close.<br>• **Session change**—Messages synchronizing session change.<br>• **Gate create**—Messages synchronizing creation of pinholes (temporary openings in the firewall).<br>• **Session ageout refresh request**—Messages synchronizing request session after age-out.<br>• **Session ageout refresh reply**—Messages synchronizing reply session after age-out.<br>• **IPsec VPN**—Messages synchronizing VPN session.<br>• **Firewall user authentication**—Messages synchronizing firewall user authentication session.<br>• **MGCP ALG**—Messages synchronizing MGCP ALG sessions.<br>• **H323 ALG**—Messages synchronizing H.323 ALG sessions.<br>• **SIP ALG**—Messages synchronizing SIP ALG sessions.<br>• **SCCP ALG**—Messages synchronizing SCCP ALG sessions.<br>• **PPTP ALG**—Messages synchronizing PPTP ALG sessions.<br>• **RTSP ALG**—Messages synchronizing RTSP ALG sessions. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show chassis cluster data-plane statistics

```
user@host> show chassis cluster data-plane statistics
Services Synchronized:
    Service name                                RTOs sent    RTOs received
    Translation context                         0            0
    Incoming NAT                                0            0
    Resource manager                            0            0
    Session create                              0            0
    Session close                               0            0
    Session change                              0            0
    Gate create                                 0            0
    Session ageout refresh requests             0            0
    Session ageout refresh replies              0            0
    IPsec VPN                                   0            0
    Firewall user authentication                0            0
    MGCP ALG                                    0            0
    H323 ALG                                    0            0
    SIP ALG                                     0            0
    SCCP ALG                                    0            0
    PPTP ALG                                    0            0
    RTSP ALG                                    0            0
```


Copyright © 2013, Juniper Networks, Inc.

## show chassis cluster ethernet-switching interfaces

**Syntax** show chassis cluster ethernet-switching interfaces

**Release Information** Command introduced in Release 11.1 of Junos OS.

**Description** Display the status of the switch fabric interfaces (swfab) in a chassis cluster.

**Required Privilege Level** view

**Related Documentation**
- Chassis Cluster for Security Devices

**List of Sample Output** show chassis cluster ethernet-switching interfaces on page 1583

**Output Fields** Table 14 on page 1583 lists the output fields for the **show chassis cluster ethernet-switching interfaces** command. Output fields are listed in the approximate order in which they appear.

### Table 14: show chassis cluster ethernet-switching interfaces Output Fields

| Field Name | Field Description |
|---|---|
| **swfab0/swfab1** | Name of the switch fabric interface.<br>• Name—Name of the physical interface.<br>• Status—State of the swfab interface: up or down. |

## Sample Output

### show chassis cluster ethernet-switching interfaces

```
user@host> show chassis cluster ethernet-switching interfaces
swfab0:
    Name                Status
    ge-0/0/9            up
    ge-0/0/10           up
swfab1:
    Name                Status
    ge-5/0/9            up
    ge-5/0/10           up
```

Copyright © 2013, Juniper Networks, Inc.

## show chassis cluster ethernet-switching status

**Syntax** show chassis cluster ethernet-switching status

**Release Information** Command introduced in Release 11.1 of Junos OS.

**Description** Display the Ethernet switching status of the chassis cluster.

**Required Privilege Level** view

**List of Sample Output** show chassis cluster ethernet-switching status on page 1585

**Output Fields** Table 15 on page 1584 lists the output fields for the **show chassis cluster ethernet-switching status** command. Output fields are listed in the approximate order in which they appear.

### Table 15: show chassis cluster ethernet-switching status Output Fields

| Field Name | Field Description |
|---|---|
| **Cluster ID** | ID number (1-15) of a cluster. |
| **Redundancy-Group** | ID number (1-255) of a redundancy group in the chassis cluster. |
| **Node name** | Node (device) in the chassis cluster (**node0** or **node1**). |
| **Priority** | Assigned priority for the redundancy group on that node. |
| **Status** | State of the redundancy group (**Primary**, **Secondary**, **Lost**, or **Unavailable**).<br>• **Primary**—Redundancy group is active and passing traffic.<br>• **Secondary**—Redundancy group is passive and not passing traffic.<br>• **Lost**—Node loses contact with the other node through the control link. Most likely to occur when both nodes are in a cluster and due to control link failure, one node cannot exchange heartbeats, or when the other node is rebooted.<br>• **Unavailable**—Node has not received a single heartbeat over the control link from the other node since the other node booted up. Most likely to occur when one node boots up before the other node, or if only one node is present in the cluster. |
| **Preempt** | • **Yes**: Mastership can be preempted based on priority.<br>• **No**: Change in priority will not preempt mastership. |
| **Manual failover** | • **Yes**: If mastership is set manually through the CLI.<br>• **No**: Mastership is not set manually through the CLI. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show chassis cluster ethernet-switching status

```
user@host> show chassis cluster ethernet-switching status
Cluster ID: 10
Node                  Priority          Status    Preempt  Manual failover

Redundancy group: 0 , Failover count: 1
    node0                   1           primary        no       no
    node1                   0           lost           n/a      n/a

Switch fabric link statistics:
    Probe state : DOWN
    Probes sent: 8145
    Probes received: 8013
    Probe recv errors: 0
    Probe send errors: 0
```

Copyright © 2013, Juniper Networks, Inc.

## show chassis cluster interfaces

**Syntax** **show chassis cluster interfaces**

**Release Information** Command modified in Junos OS Release 9.0. Output changed to support dual control ports in Junos OS Release 10.0. Output changed to support control interfaces in Junos OS Release 11.2. Output changed to support redundant pseudointerfaces in Junos OS Release 12.1X44-D10.

**Description** Display the status of the control interface in a chassis cluster configuration.

**Required Privilege Level** view

**Related Documentation**
- Chassis Cluster for Security Devices

**List of Sample Output**
show chassis cluster interfaces on page 1588
show chassis cluster interfaces (SRX3000 and SRX5000 line devices) on page 1588

**Output Fields** Table 16 on page 1586 lists the output fields for the **show chassis cluster interfaces** command. Output fields are listed in the approximate order in which they appear.

### Table 16: show chassis cluster interfaces Output Fields

| Field Name | Field Description |
|---|---|
| **Control link status** | State of the chassis cluster control interface: **up** or **down**. |
| **Control interfaces** | • **Index**—Index number of the chassis cluster control interface.<br>• **Name**—Name of the chassis cluster control interface.<br>• **Status**—State of the interface: **up** or **down**. |
| **Fabric link status** | State of the fabric interface: **up** or **down**. |
| **Fabric interfaces** | • **Name**—Name of the fabric interface.<br>• **Child-interface**—Name of the child fabric interface.<br>• **Status**—State of the interface: **up** or **down**. |
| **Redundant-ethernet Information** | • **Name**—Name of the redundant Ethernet interface.<br>• **Status**—State of the interface: **up** or **down**.<br>• **Redundancy-group**—Identification number (1–255) of the redundancy group associated with the redundant Ethernet interface. |
| **Redundant-pseudo-interface Information** | • **Name**—Name of the redundant pseudo interface.<br>• **Status**—State of the redundant pseudo interface: **up** or **down**.<br>• **Redundancy-group**—Identification number (1–255) of the redundancy group associated with the redundant pseudo interface. |


Copyright © 2013, Juniper Networks, Inc.

Table 16: show chassis cluster interfaces Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Interface Monitoring** | • **Interface**—Name of the interface to be monitored.<br>• **Weight**—Relative importance of the interface to redundancy group operation.<br>• **Status**—State of the interface: **up** or **down**.<br>• **Redundancy-group**—Identification number of the redundancy group associated with the interface. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show chassis cluster interfaces

```
user@host> show chassis cluster interfaces
Control link status: Up

Control interfaces:
    Index   Interface        Status
    0       em0              Up
    1       em1              Down

Fabric link status: Up

Fabric interfaces:
    Name    Child-interface    Status
    fab0    ge-0/1/0           Up
    fab0
    fab1    ge-6/1/0           Up
    fab1

Redundant-ethernet Information:
    Name         Status      Redundancy-group
    reth0        Up          1
    reth1        Up          2
    reth2        Down        Not configured
    reth3        Down        Not configured
    reth4        Down        Not configured
    reth5        Down        Not configured
    reth6        Down        Not configured
    reth7        Down        Not configured
    reth8        Down        Not configured
    reth9        Down        Not configured
    reth10       Down        Not configured
    reth11       Down        Not configured

Redundant-pseudo-interface Information:
    Name        Status       Redundancy-group
     lo0          Up               1

Interface Monitoring:
    Interface         Weight    Status    Redundancy-group
    ge-0/1/9          100       Up        0
    ge-0/1/9          100       Up
```

## Sample Output

### show chassis cluster interfaces (SRX3000

```
user@host> show chassis cluster interfaces
Control link status: Up
```


Copyright © 2013, Juniper Networks, Inc.

and SRX5000 line devices)

```
Control interfaces:
    Index   Interface        Status
    0       em0              Up
    1       em1              Down

Fabric link status: Up

Fabric interfaces:
    Name    Child-interface    Status
    fab0    ge-0/1/0           Up
    fab0
    fab1    ge-6/1/0           Up
    fab1

Redundant-ethernet Information:
    Name         Status      Redundancy-group
    reth0        Up          1
    reth1        Up          2
    reth2        Down        Not configured
    reth3        Down        Not configured
    reth4        Down        Not configured
    reth5        Down        Not configured
    reth6        Down        Not configured
    reth7        Down        Not configured
    reth8        Down        Not configured
    reth9        Down        Not configured
    reth10       Down        Not configured
    reth11       Down        Not configured

Redundant-pseudo-interface Information:
    Name        Status       Redundancy-group
     lo0          Up               1

Interface Monitoring:
    Interface         Weight    Status    Redundancy-group
    ge-0/1/9          100       Up        0
    ge-0/1/9          100       Up
```

Copyright © 2013, Juniper Networks, Inc.

## show chassis cluster ip-monitoring status redundancy-group

**Syntax** **show chassis cluster ip-monitoring status <redundancy-group *group-number* >**

**Release Information** Command added in Release 9.6 of Junos OS.

**Description** Display the status of all monitored IP addresses for a redundancy group.

**Options**
- none— Display the status of monitored IP addresses for all redundancy groups on the node.
- **redundancy-group *group-number*** — Display the status of monitored IP addresses under the specified redundancy group.

**Required Privilege Level** view

**Related Documentation**
- IP Monitoring
- Chassis Cluster for Security Devices
- redundancy-group (Interfaces) on page 204
- clear chassis cluster failover-count on page 1360
- request chassis cluster failover node on page 1488
- request chassis cluster failover reset on page 1489

**List of Sample Output**
show chassis cluster ip-monitoring status on page 1592
show chassis cluster ip-monitoring status redundancy-group on page 1592

**Output Fields** Table 17 on page 1590 lists the output fields for the **show chassis cluster ip-monitoring status** command.

### Table 17: show chassis cluster ip-monitoring status Output Fields

| Field Name | Field Description |
|---|---|
| **Redundancy-group** | ID number (0 - 255) of a redundancy group in the cluster. |
| **IP Address** | Monitored IP address in the redundancy group. |
| **Status** | Current reachability state of the monitored IP address.<br><br>Values for this field are: **reachable**, **unreachable**, and **unknown**. The status is “unknown” if packet forwarding engines (PFEs) are not yet up and running. |
| **Failure count** | Number of attempts to reach an IP address. |
| **Reason** | Explanation for the reported status. See Table 18 on page 1591. |


Copyright © 2013, Juniper Networks, Inc.

Expanded reason output fields for unreachable IP addresses added in Release 10.1 of Junos OS. You might see any of the following reasons displayed.

Table 18: show chassis cluster ip-monitoring status redundancy group Reason Fields

| Reason | Reason Description |
|---|---|
| **No route to host** | The router could not resolve the ARP, which is needed to send the ICMP packet to the host with the monitored IP address. |
| **No auxiliary IP found** | The redundant Ethernet interface does not have an auxiliary IP address configured. |
| **Reth child not up** | A child interface of a redundant Ethernet interface is down. |
| **redundancy-group state unknown** | Unable to obtain the state (primary, secondary, secondary-hold, disable) of a redundancy-group. |
| **No reth child MAC address** | Could not extract the MAC address of the redundant Ethernet child interface. |
| **Secondary link not monitored** | The secondary link may be down (the secondary child interface of a redundant Ethernet interface is either down or non-functional). |
| **Unknown** | The IP address has just been configured and the router still does not know the status of this IP.<br><br>or<br><br>Do not know the exact reason for the failure. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show chassis cluster ip-monitoring status

```
user@host> show chassis cluster ip-monitoring status
node0:
--------------------------------------------------------------------------

Redundancy group: 1

IP address              Status        Failure count  Reason
10.254.5.44             reachable       0            n/a
2.2.2.1                 reachable       0            n/a
1.1.1.5                 reachable       0            n/a
1.1.1.4                 reachable       0            n/a
1.1.1.1                 reachable       0            n/a

node1:
--------------------------------------------------------------------------

Redundancy group: 1

IP address              Status        Failure count  Reason
10.254.5.44             reachable       0            n/a
2.2.2.1                 reachable       0            n/a
1.1.1.5                 reachable       0            n/a
1.1.1.4                 reachable       0            n/a
1.1.1.1                 reachable       0            n/a
```

## Sample Output

### show chassis cluster ip-monitoring status redundancy-group

```
user@host> show chassis cluster ip-monitoring status redundancy-group 1
node0:
--------------------------------------------------------------------------

Redundancy group: 1

IP address              Status        Failure count  Reason
10.254.5.44             reachable       0            n/a
2.2.2.1                 reachable       0            n/a
1.1.1.5                 reachable       0            n/a
1.1.1.4                 reachable       0            n/a
1.1.1.1                 reachable       0            n/a

node1:
--------------------------------------------------------------------------

Redundancy group: 1

IP address              Status        Failure count  Reason
10.254.5.44             reachable       0            n/a
2.2.2.1                 reachable       0            n/a
1.1.1.5                 reachable       0            n/a
1.1.1.4                 reachable       0            n/a
1.1.1.1                 reachable       0            n/a
```


Copyright © 2013, Juniper Networks, Inc.

## show chassis cluster statistics

**Syntax** **show chassis cluster statistics**

**Release Information** Command modified in Release 9.0 of Junos OS. Output changed to support dual control ports in Release 10.0 of Junos OS.

**Description** Display information about chassis cluster services and interfaces.

**Required Privilege Level** view

**Related Documentation**

- Chassis Cluster for Security Devices
- clear chassis cluster statistics on page 1364
- Application Layer Gateways for Security Devices

**List of Sample Output**

show chassis cluster statistics on page 1595
show chassis cluster statistics (SRX3000 and SRX5000 line devices) on page 1595
show chassis cluster statistics (SRX3000 and SRX5000 line devices) on page 1596

**Output Fields** Table 19 on page 1593 lists the output fields for the **show chassis cluster statistics** command. Output fields are listed in the approximate order in which they appear.

### Table 19: show chassis cluster statistics Output Fields

| Field Name | Field Description |
|---|---|
| **Control link statistics** | Statistics of the control link used by chassis cluster traffic. Statistics for **Control link 1** are displayed when you use dual control links (SRX3000 and SRX5000 lines only). Note that the output for the SRX3000 and SRX5000 lines will always show **Control link 0** and **Control link 1** statistics, even though only one control link is active or working.<br>• **Heartbeat packets sent**—Number of heartbeat messages sent on the control link.<br>• **Heartbeat packets received**—Number of heartbeat messages received on the control link.<br>• **Heartbeat packet errors**—Number of heartbeat packets received with errors on the control link. |
| **Fabric link statistics** | Statistics of the fabric link used by chassis cluster traffic. Statistics for **Child Link 1** are displayed when you use dual fabric links.<br>• **Probes sent**—Number of probes sent on the fabric link.<br>• **Probes received**—Number of probes received on the fabric link. |

Copyright © 2013, Juniper Networks, Inc.

Table 19: show chassis cluster statistics Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Services Synchronized** | • **Service name**—Name of the service.<br>• **Rtos sent**—Number of runtime objects (RTOs) sent.<br>• **Rtos received**—Number of RTOs received.<br>• **Translation context**—Messages synchronizing Network Address Translation (NAT) translation context.<br>• **Incoming NAT**—Messages synchronizing incoming Network Address Translation (NAT) service.<br>• **Resource manager**—Messages synchronizing resource manager groups and resources.<br>• **Session create**—Messages synchronizing session creation.<br>• **Session close**—Messages synchronizing session close.<br>• **Session change**—Messages synchronizing session change.<br>• **Gate create**—Messages synchronizing creation of pinholes (temporary openings in the firewall).<br>• **Session ageout refresh request**—Messages synchronizing request session after age-out.<br>• **Session ageout refresh reply**—Messages synchronizing reply session after age-out.<br>• **IPsec VPN**—Messages synchronizing VPN session.<br>• **Firewall user authentication**—Messages synchronizing firewall user authentication session.<br>• **MGCP ALG**—Messages synchronizing MGCP ALG sessions.<br>• **H323 ALG**—Messages synchronizing H.323 ALG sessions.<br>• **SIP ALG**—Messages synchronizing SIP ALG sessions.<br>• **SCCP ALG**—Messages synchronizing SCCP ALG sessions.<br>• **PPTP ALG**—Messages synchronizing PPTP ALG sessions.<br>• **RTSP ALG**—Messages synchronizing RTSP ALG sessions.<br>• **MAC address learning**—Messages synchronizing MAC address learning. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show chassis cluster statistics

```
user@host> show chassis cluster statistics
Control link statistics:
    Control link 0:
        Heartbeat packets sent: 798
        Heartbeat packets received: 784
        Heartbeat packets errors: 0
Fabric link statistics:
    Child link 0
        Probes sent: 793
        Probes received: 0
Services Synchronized:
    Service name                                RTOs sent    RTOs received
    Translation context                         0            0
    Incoming NAT                                0            0
    Resource manager                            0            0
    Session create                              0            0
    Session close                               0            0
    Session change                              0            0
    Gate create                                 0            0
    Session ageout refresh requests             0            0
    Session ageout refresh replies              0            0
    IPsec VPN                                   0            0
    Firewall user authentication                0            0
    MGCP ALG                                    0            0
    H323 ALG                                    0            0
    SIP ALG                                     0            0
    SCCP ALG                                    0            0
    PPTP ALG                                    0            0
    RTSP ALG                                    0            0
    MAC address learning                        0            0
```

## Sample Output

### show chassis cluster statistics (SRX3000

```
user@host> show chassis cluster statistics
Control link statistics:
    Control link 0:
```

and SRX5000 line devices)

```
        Heartbeat packets sent: 258689
        Heartbeat packets received: 258684
        Heartbeat packets errors: 0
    Control link 1:
        Heartbeat packets sent: 258689
        Heartbeat packets received: 258684
        Heartbeat packets errors: 0
Fabric link statistics:
    Child link 0
        Probes sent: 258681
        Probes received: 258681
    Child link 1
        Probes sent: 258501
        Probes received: 258501
Services Synchronized:
    Service name                            RTOs sent    RTOs received
    Translation context                     0            0
    Incoming NAT                            0            0
    Resource manager                        0            0
    Session create                          1            0
    Session close                           1            0
    Session change                          0            0
    Gate create                             0            0
    Session ageout refresh requests         0            0
    Session ageout refresh replies          0            0
    IPSec VPN                               0            0
    Firewall user authentication            0            0
    MGCP ALG                                0            0
    H323 ALG                                0            0
    SIP ALG                                 0            0
    SCCP ALG                                0            0
    PPTP ALG                                0            0
    RPC ALG                                 0            0
    RTSP ALG                                0            0
    RAS ALG                                 0            0
    MAC address learning                    0            0
    GPRS GTP                                0            0
```

## Sample Output

show chassis cluster statistics (SRX3000

```
user@host> show chassis cluster statistics
Control link statistics:
    Control link 0:
```


Copyright © 2013, Juniper Networks, Inc.

and SRX5000 line devices)

```
            Heartbeat packets sent: 82371
            Heartbeat packets received: 82321
            Heartbeat packets errors: 0
        Control link 1:
            Heartbeat packets sent: 0
            Heartbeat packets received: 0
            Heartbeat packets errors: 0
    Fabric link statistics:
        Child link 0
            Probes sent: 258681
            Probes received: 258681
        Child link 1
            Probes sent: 258501
            Probes received: 258501
    Services Synchronized:
        Service name                            RTOs sent    RTOs received
        Translation context                     0            0
        Incoming NAT                            0            0
        Resource manager                        0            0
        Session create                          1            0
        Session close                           1            0
        Session change                          0            0
        Gate create                             0            0
        Session ageout refresh requests         0            0
        Session ageout refresh replies          0            0
        IPSec VPN                               0            0
        Firewall user authentication            0            0
        MGCP ALG                                0            0
        H323 ALG                                0            0
        SIP ALG                                 0            0
        SCCP ALG                                0            0
        PPTP ALG                                0            0
        RPC ALG                                 0            0
        RTSP ALG                                0            0
        RAS ALG                                 0            0
        MAC address learning                    0            0
        GPRS GTP                                0            0
```

Copyright © 2013, Juniper Networks, Inc.

## show chassis cluster status

**Syntax**
**show chassis cluster status**
**<redundancy-group** ***group-number*** **>**

**Release Information**
Command modified in Release 9.2 of Junos OS. Output changed to support dual control ports in Release 10.0 of Junos OS.

**Description**
Display the failover status of a chassis cluster.

**Options**
- none—Display the status of all redundancy groups in the chassis cluster.
- **redundancy-group** ***group-number*** —(Optional) Display the status of the specified redundancy group.

**Required Privilege Level**
view

**Related Documentation**
- Chassis Cluster for Security Devices
- redundancy-group (Chassis Cluster) on page 102
- clear chassis cluster failover-count on page 1360
- request chassis cluster failover node on page 1488
- request chassis cluster failover reset on page 1489
- Master Administrator for Logical Systems on Security Devices

**List of Sample Output**
show chassis cluster status on page 1600
show chassis cluster status redundancy-group 2 on page 1600
show chassis cluster status on page 1600
show chassis cluster status on page 1600

**Output Fields**
Table 20 on page 1598 lists the output fields for the **show chassis cluster status** command. Output fields are listed in the approximate order in which they appear.

### Table 20: show chassis cluster status Output Fields

| Field Name | Field Description |
|---|---|
| **Cluster ID** | ID number (1-15) of a cluster. |
| **Redundancy-Group** | ID number (1-255) of a redundancy group in the chassis cluster. |
| **Node name** | Node (device) in the chassis cluster (**node0** or **node1**). |
| **Priority** | Assigned priority for the redundancy group on that node. |


Copyright © 2013, Juniper Networks, Inc.

Table 20: show chassis cluster status Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Status** | State of the redundancy group (**Primary**, **Secondary**, **Lost**, or **Unavailable**).<br>• **Primary**—Redundancy group is active and passing traffic.<br>• **Secondary**—Redundancy group is passive and not passing traffic.<br>• **Lost**—Node loses contact with the other node through the control link. Most likely to occur when both nodes are in a cluster and due to control link failure, one node cannot exchange heartbeats, or when the other node is rebooted.<br>• **Unavailable**—Node has not received a single heartbeat over the control link from the other node since the other node booted up. Most likely to occur when one node boots up before the other node, or if only one node is present in the cluster. |
| **Preempt** | • **Yes**: Mastership can be preempted based on priority.<br>• **No**: Change in priority will not preempt the mastership. |
| **Manual failover** | • **Yes**: If the Mastership is set manually through the CLI with the **request chassis cluster failover node** or **request chassis cluster failover redundancy-group** command. This overrides **Priority** and **Preempt**.<br>• **No**: Mastership is not set manually through the CLI. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show chassis cluster status

```
user@host> show chassis cluster status
Cluster ID: 3
   Node name               Priority    Status    Preempt  Manual failover
 Redundancy-group: 0, Failover count: 1
    node0                  254         primary   no       no
    node1                  2           secondary no       no
 Redundancy-group: 1, Failover count: 1
    node0                  254         primary   no       no
    node1                  1           secondary no       no
```

## Sample Output

show chassis cluster status redundancy-group 2

```
user@host> show chassis cluster status redundancy-group 2
Cluster ID: 14
   Node name          Priority    Status    Preempt  Manual failover
 Redundancy-Group: 2, Failover count: 1
    node0              50          secondary no       no
    node1              100         primary   no       no
```

## Sample Output

show chassis cluster status

```
user@host> show chassis cluster status
Cluster ID: 15
Node                  Priority          Status    Preempt  Manual failover
Redundancy group: 0 , Failover count: 5
    node0                  200         primary        no       no
    node1                  0           lost           n/a      n/a
Redundancy group: 1 , Failover count: 41
    node0                  101         primary        no       no
    node1                  0           lost           n/a      n/a
```

## Sample Output

show chassis cluster status

```
user@host> show chassis cluster status
Cluster ID: 15
Node                  Priority          Status    Preempt  Manual failover
Redundancy group: 0 , Failover count: 5
    node0                  200         primary        no       no
    node1                  0           unavailable    n/a      n/a
Redundancy group: 1 , Failover count: 41
    node0                  101         primary        no       no
    node1                  0           unavailable    n/a      n/a
```


Copyright © 2013, Juniper Networks, Inc.

## show chassis fpc (View)

**Syntax**

**show chassis fpc**
<**detail** < ***fpc-slot*** >| <node ( ***node-id*** | local | primary)>> |
<node ( ***node-id*** | local | primary)> |
<**pic-status** < ***fpc-slot*** >| <node ( ***node-id*** | local | primary)>>

**Release Information**

Command modified in Release 9.2 of Junos OS; **node**options added in Release 9.0 of Junos OS.

**Description**

Display status information about the installed Flexible PIC Concentrators (FPCs)and PICs.

**Options**

- none—Display status information for all FPCs.
- **detail**—(Optional) Display detailed FPC status information.
- ***fpc-slot*** —(Optional) Display information about the FPC in this slot.
- **node**—(Optional) For chassis cluster configurations, display status information for all FPCs or for the specified FPC on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.
- **pic-status**—(Optional) Display status information for all FPCs or for the FPC in the specified slot (see ***fpc-slot***).

**Required Privilege Level**

view

**Related Documentation**

- Junos OS Operational Mode Commands

**List of Sample Output**

show chassis fpc on page 1603
show chassis fpc (SRX1400 devices) on page 1603
show chassis fpc (SRX5600 and SRX5800 devices) on page 1603
show chassis fpc detail 2 on page 1603
show chassis fpc pic-status (SRX1400, SRX3400, and SRX3600 devices) on page 1603
show chassis fpc pic-status (SRX5600 and SRX5800 devices) on page 1604
show chassis fpc pic-status for HA (SRX3400 and SRX3600 devices) on page 1604
show chassis fpc pic-status for HA (SRX5600 and SRX5800 devices) on page 1605
show chassis fpc pic-status (SRX5600 and SRX5800 devices with NG-SPC) on page 1605

**Output Fields**

Table 21 on page 1602 lists the output fields for the **show chassis fpc** command. Output fields are listed in the approximate order in which they appear.

Copyright © 2013, Juniper Networks, Inc.

### Table 21: show chassis fpc Output Fields

| Field Name | Field Description |
|---|---|
| **Slot or Slot State** | Slot number and state. The state can be one of the following conditions:<br>• **Dead**—Held in reset because of errors.<br>• **Diag**—Slot is being ignored while the device is running diagnostics.<br>• **Dormant**—Held in reset.<br>• **Empty**—No FPC is present.<br>• **Online**—FPC is online and running.<br>• **Present**—FPC is detected by the device, but is either not supported by the current version of Junos OS or inserted in the wrong slot. The output also states either **Hardware Not Supported** or **Hardware Not In Right Slot**. FPC is coming up but not yet online.<br>• **Probed**—Probe is complete; awaiting restart of the Packet Forwarding Engine (PFE).<br>• **Probe-wait**—Waiting to be probed. |
| **Temp (C) or Temperature** | Temperature of the air passing by the FPC, in degrees Celsius or in both Celsius and Fahrenheit. |
| **Total CPU Utilization (%)** | Total percentage of CPU being used by the FPC's processor. |
| **Interrupt CPU Utilization (%)** | Of the total CPU being used by the FPC's processor, the percentage being used for interrupts. |
| **Memory DRAM (MB)** | Total DRAM, in megabytes, available to the FPC's processor. |
| **Heap Utilization (%)** | Percentage of heap space (dynamic memory) being used by the FPC's processor. If this number exceeds 80 percent, there may be a software problem (memory leak). |
| **Buffer Utilization (%)** | Percentage of buffer space being used by the FPC's processor for buffering internal messages. |
| **Start Time** | Time when the Routing Engine detected that the FPC was running. |
| **Uptime** | How long the Routing Engine has been connected to the FPC and, therefore, how long the FPC has been up and running. |
| **PIC type** | (**pic-status** output only) Type of FPC. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show chassis fpc

```
user@host> show chassis fpc
                     Temp   CPU Utilization (%)     Memory    Utilization (%)
     Slot State        (C)    Total  Interrupt        DRAM (MB) Heap  Buffer
      0  Online          --------------------- CPU less FPC ---------------------
      1  Online          ----------------------  Not Usable ---------------------
      2  Online          --------------------- CPU less FPC ---------------------
```

## Sample Output

### show chassis fpc (SRX1400 devices)

```
user@host> show chassis fpc
                     Temp   CPU Utilization (%)      Memory    Utilization (%)
 Slot State           (C)    Total  Interrupt     DRAM (MB)    Heap     Buffer
  0  Online           49     30          0       1024         3          25
  1  Online           41     30          0       1024         3          25
  2  Online           44     30          0       1024         3          25
  3  Online           54     30          0       1024         3          25
```

## Sample Output

### show chassis fpc (SRX5600 and SRX5800 devices)

```
user@host> show chassis fpc
                     Temp   CPU Utilization (%)       Memory    Utilization (%)
Slot State           (C)    Total  Interrupt         DRAM (MB) Heap     Buffer
  0  Empty
  1  Empty
  2  Empty
  3  Online           37       3          0             1024        7     42
  4  Empty
  5  Empty
  6  Online           30        8         0             1024        23    30
  7  Empty
  8  Empty
  9  Empty
 10  Empty
 11  Empty
```

## Sample Output

### show chassis fpc detail 2

```
user@host> show chassis fpc detail 2
Slot 2 information:
  State                                 Online
  Temperature                            37
  Total CPU DRAM                       1024 MB
  Total RLDRAM                          0 MB
  Total DDR DRAM                        0 MB
  Start time:                             2012-07-18 07:18:50 PDT
  Uptime:                                 4 days, 21 hours, 51 minutes, 59 seconds

  Max Power Consumption                 0 Watts
```

## Sample Output

### show chassis fpc

```
user@host> show chassis fpc pic-status
Slot 0   Online       SRX3k SFB 12GE
```

Copyright © 2013, Juniper Networks, Inc.

pic-status (SRX1400, SRX3400, and SRX3600 devices)

```
  PIC 0  Online       8x 1GE-TX 4x 1GE-SFP
Slot 1   Online       SRX3k 2x10GE XFP
  PIC 0  Online       2x 10GE-XFP
Slot 3   Online       SRX1k3k 2x10GE NP-IOC
  PIC 0  Online       2x 10GE-SFP+
Slot 4   Online       SRX3k SPC
  PIC 0  Online       SPU Cp-Flow
Slot 5   Online       SRX1k3k 2x10GE NP-IOC
  PIC 0  Online       2x 10GE-SFP+
Slot 6   Online       SRX3k NPC
  PIC 0  Online       NPC PIC
Slot 7   Online       SRX1k3k 2x10GE NP-IOC
  PIC 0  Online       2x 10GE-SFP+- services-offload low-latency
```

## Sample Output

show chassis fpc pic-status (SRX5600 and SRX5800 devices)

```
user@host> show chassis fpc pic-status
Slot 3   Online       SRX5k SPC
  PIC 0  Online       SPU Cp
  PIC 1  Online       SPU Flow
Slot 6   Online       SRX5k DPC 4x 10GE
  PIC 0  Online       1x 10GE(LAN/WAN) RichQ
  PIC 1  Online       1x 10GE(LAN/WAN) RichQ
  PIC 2  Online       1x 10GE(LAN/WAN) RichQ
  PIC 3  Online       1x 10GE(LAN/WAN) RichQ
```

## Sample Output

show chassis fpc pic-status for HA

```
user@host> show chassis fpc pic-status
node0:
--------------------------------------------------------------------------
```


Copyright © 2013, Juniper Networks, Inc.

(SRX3400 and SRX3600 devices)

```
Slot 0   Online       SRX3k SFB 12GE
  PIC 0  Online       8x 1GE-TX 4x 1GE-SFP
Slot 1   Online       SRX3k 2x10GE XFP
  PIC 0  Online       2x 10GE-XFP
Slot 2   Online       SRX3k 16xGE SFP
  PIC 0  Online       16x 1GE-SFP
Slot 7   Online       SRX3k SPC
  PIC 0  Online       SPU Cp-Flow
Slot 11  Online       SRX3k NPC
  PIC 0  Online       NPC PIC
Slot 12  Online       SRX3k NPC
  PIC 0  Online       NPC PIC

node1:
--------------------------------------------------------------------------
Slot 0   Online       SRX3k SFB 12GE
  PIC 0  Online      8x 1GE-TX 4x 1GE-SFP
Slot 1   Online       SRX3k 2x10GE XFP
  PIC 0  Online      2x 10GE-XFP
Slot 2   Online       SRX3k 16xGE SFP
  PIC 0  Online      16x 1GE-SFP
Slot 7   Online       SRX3k SPC
  PIC 0  Online       SPU Cp-Flow
Slot 11  Online       SRX3k NPC
  PIC 0  Online      NPC PIC
Slot 12  Online       SRX3k NPC
  PIC 0  Online      NPC PIC
```

## Sample Output

show chassis fpc pic-status for HA (SRX5600 and SRX5800 devices)

```
user@host> show chassis fpc pic-status
node0:
--------------------------------------------------------------
Slot 4   Online       SRX5k DPC 40x 1GE
  PIC 0  Online       10x 1GE RichQ
  PIC 1  Online       10x 1GE RichQ
  PIC 2  Online       10x 1GE RichQ
  PIC 3  Online       10x 1GE RichQ
Slot 5   Online       SRX5k SPC
  PIC 0  Online       SPU Cp-Flow
  PIC 1  Online       SPU Flow

node1:
--------------------------------------------------------------
Slot 4   Online       SRX5k DPC 40x 1GE
  PIC 0  Online       10x 1GE RichQ
  PIC 1  Online       10x 1GE RichQ
  PIC 2  Online       10x 1GE RichQ
  PIC 3  Online       10x 1GE RichQ
Slot 5   Online       SRX5k SPC
  PIC 0  Online       SPU Cp-Flow
  PIC 1  Online       SPU Flow
```

## Sample Output

show chassis fpc pic-status (SRX5600

```
user@host> show chassis fpc pic-status

Slot 0   Online       SRX5k DPC 40x 1GE
```

and SRX5800 devices with NG-SPC)

```
    PIC 0  Online       10x 1GE RichQ
    PIC 1  Online       10x 1GE RichQ
    PIC 2  Online       10x 1GE RichQ
    PIC 3  Online       10x 1GE RichQ
Slot 2   Online       SRX5k SPC II
    PIC 0  Online       SPU Cp
    PIC 1  Online       SPU Flow
    PIC 2  Online       SPU Flow
    PIC 3  Online       SPU Flow
Slot 3   Online       SRX5k SPC II
    PIC 0  Online       SPU Flow
    PIC 1  Online       SPU Flow
    PIC 2  Online       SPU Flow
    PIC 3  Online       SPU Flow
Slot 5   Online       SRX5k SPC
    PIC 0  Online       SPU Flow
    PIC 1  Online       SPU Flow
```


Copyright © 2013, Juniper Networks, Inc.

## show chassis hardware (View)

**Syntax**

**show chassis hardware**
<**clei-models** | **detail** | **extensive** | models | node ( *node-id* | all | local | primary)>

**Release Information**

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description**

Display chassis hardware information.

**Options**

- **clei-models**—(Optional) Display Common Language Equipment Identifier Code (CLEI) barcode and model number for orderable field-replaceable units (FRUs).
- **detail** | **extensive**—(Optional) Display the specified level of output.
- **models**—(Optional) Display model numbers and part numbers for orderable FRUs.
- **node**—(Optional) For chassis cluster configurations, display chassis hardware information on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level**

view

**Related Documentation**

- Junos OS Operational Mode Commands
- Ethernet Interfaces
- Interfaces for Security Devices

**List of Sample Output**

show chassis hardware on page 1610
show chassis hardware (SRX5600 and SRX5800 devices) on page 1610
show chassis hardware detail on page 1611
show chassis hardware detail node 1 on page 1611
show chassis hardware extensive on page 1611
show chassis hardware models (SRX1400 and SRX3000 devices) on page 1612
show chassis hardware models (SRX5600 and SRX5800 devices) on page 1613
show chassis hardware clei-models (SRX5600 and SRX5800 devices) on page 1613
show chassis hardware models (SRX5600 and SRX5800 devices for next-generation SPC) on page 1613

**Output Fields**

Table 22 on page 1608 lists the output fields for the **show chassis hardware** command. Output fields are listed in the approximate order in which they appear.

Copyright © 2013, Juniper Networks, Inc.

### Table 22: show chassis hardware Output Fields

| Field Name | Field Description |
|---|---|
| **Item** | Chassis component—Information about the backplane; power supplies; fan trays; Routing Engine; each Physical Interface Module (PIM)—reported as FPC and PIC—and each fan, blower, and impeller. |
| **Version** | Revision level of the chassis component. |
| **Part Number** | Part number for the chassis component. |
| **Serial Number** | Serial number of the chassis component. The serial number of the backplane is also the serial number of the device chassis. Use this serial number when you need to contact Juniper Networks Customer Support about the device chassis. |
| **Assb ID or Assembly ID** | Identification number that describes the FRU hardware. |
| **FRU model number** | Model number of FRU hardware component. |
| **CLEI code** | Common Language Equipment Identifier code. This value is displayed only for hardware components that use ID EEPROM format v2. This value is not displayed for components that use ID EEPROM format v1. |
| **EEPROM Version** | ID EEPROM version used by hardware component: 0x01 (version 1) or 0x02 (version 2). |


Copyright © 2013, Juniper Networks, Inc.

Table 22: show chassis hardware Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Description** | Brief description of the hardware item:<br>• Type of power supply.<br>• Type of PIM. If the PIM type is not supported on the current software release, the output states **Hardware Not Supported**.<br>• Type of FPC: The FPC type corresponds to the PIM. The following shows the PIM abbreviation in the output and the corresponding PIM name:<br>  • 2x FE—Dual-Port Fast Ethernet PIM<br>  • 4x FE—4-Port Fast Ethernet ePIM<br>  • 1x GE Copper—Copper Gigabit Ethernet ePIM (one 10-mpbs, 100-Mpbs, or 1000-Mpbs port)<br>  • 1x GE SFP—SFP Gigabit Ethernet ePIM (one fiber port)<br>  • 1x SFP uPIM—1-Port Gigabit Ethernet uPIM<br>  • 6x GE SFP uPIM—6-Port Gigabit Ethernet uPIM<br>  • 8x GE SFP uPIM—8-Port Gigabit Ethernet uPIM<br>  • 16x GE SFP uPIM—16-Port Gigabit Ethernet uPIM<br>  • 4x GE Base PIC—Four built-in Gigabit Ethernet ports on a chassis (fixed PIM)<br>  • 2x Serial—Dual-Port Serial PIM<br>  • 2x T1—Dual-Port T1 PIM<br>  • 2x E1—Dual-Port E1 PIM<br>  • 2x CT1E1/PRI—Dual-Port Channelized T1/E1/ISDN PRI PIM<br>  • 1x T3—T3 PIM (one port)<br>  • 1x E3—E3 PIM (one port)<br>  • 4x BRI S/T—4-Port ISDN BRI S/T PIM<br>  • 4x BRI U—4-Port ISDN BRI U PIM<br>  • 1x ADSL Annex A—ADSL 2/2 + Annex A PIM (one port, for POTS)<br>  • 1x ADSL Annex B—ADSL 2/2 + Annex B PIM (one port, for ISDN<br>  • 2x SHDSL (ATM)—G.SHDSL PIM (2-port two-wire mode or 1-port four-wire mode)<br>  • Integrated Services Module—WXC Integrated Services Module (ISM 200)<br>• For hosts, the Routing Engine type. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show chassis hardware

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                AB1609AA0082      SRX 3600
Midplane         REV 07   710-020310   VP8136            SRX 3600 Midplane
PEM 0            rev 05   740-027644   G087E6003S05P     AC Power Supply
PEM 1            rev 05   740-027644   G087E600AT05P     AC Power Supply
CB 0             REV 11   750-021914   AAAC9887          SRX3k RE-12-10
  Routing Engine          BUILTIN      BUILTIN           Routing Engine
  CPP                     BUILTIN      BUILTIN           Central PFE Processor
  Mezz           REV 08   710-021035   AAAD9202          SRX HD Mezzanine Card
FPC 0            REV 11   750-021882   AAAD9785          SRX3k SFB 12GE
  PIC 0                   BUILTIN      BUILTIN           8x 1GE-TX 4x 1GE-SFP
    Xcvr 8       REV 01   740-011613   PDG0UMW           SFP-SX
    Xcvr 9       REV 02   740-011613   PGJ5GJF           SFP-SX
    Xcvr 11      REV 01   740-014132   62081010          SFP-T
FPC 1            REV 10   750-016077   AAAE9989          SRX3k SPC
  PIC 0                   BUILTIN      BUILTIN           SPU Cp-Flow
FPC 2            REV 11   750-016077   AAAT8490          SRX3k SPC
  PIC 0                   BUILTIN      BUILTIN           SPU Flow
FPC 5            REV 15   750-020321   AABB3820          SRX3k 2x10GE XFP
  PIC 0                   BUILTIN      BUILTIN           2x 10GE-XFP
    Xcvr 0       REV 03   740-014289   0ZT805000069      XFP-10G-SR
    Xcvr 1       REV 03   740-011571   C933BK00F         XFP-10G-SR
FPC 10           REV 12   750-043828   AAAD9501          SRX1k3k 2x10GE NP-IOC

  PIC 0                   BUILTIN      BUILTIN           2x 10GE-SFP+
Fan Tray 0       REV 06   750-021599   VR9734            SRX 3600 Fan Tray
```

## Sample Output

### show chassis hardware (SRX5600 and SRX5800 devices)

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                JN10B7005AGA      SRX 5800
Midplane         REV 03   710-013698   TR0779            SRX 5800 Backplane
FPM Board        REV 03   710-014974   KC3406            Front Panel Display
PDM              Rev 03   740-013110   QCS1122504F       Power Distribution Module
PEM 1             Rev 03   740-013683   QCS1134703V       DC Power Entry Module
PEM 2             Rev 03   740-013683   QCS1134700E       DC Power Entry Module
Routing Engine 0 REV 06   740-015113   1000696955        RE-S-1300
CB 0             REV 07   710-013385   JZ3257            SRX5k SCB
FPC 3            BB-P2-39 710-020305   JS4847            SRX5k SPC
  CPU            REV 06   710-013713   KC1180            DPC PMB
  PIC 0                   BUILTIN      BUILTIN           SPU Cp
  PIC 1                   BUILTIN      BUILTIN           SPU Flow
FPC 6            REV 03   750-020751   JT0109            SRX5k DPC 4x 10GE
  CPU            REV 06   710-013713   KC3543            DPC PMB
  PIC 0                   BUILTIN      BUILTIN           1x 10GE(LAN/WAN) RichQ
    Xcvr 0                NON-JNPR     A7C00SY           XFP-10G-SR
  PIC 1                   BUILTIN      BUILTIN           1x 10GE(LAN/WAN) RichQ
    Xcvr 0       REV 01   740-011571   C728XJ01W         XFP-10G-SR
  PIC 2                   BUILTIN      BUILTIN           1x 10GE(LAN/WAN) RichQ
  PIC 3                   BUILTIN      BUILTIN           1x 10GE(LAN/WAN) RichQ
Fan Tray 0       REV 04   740-014971   TP1432            Fan Tray
Fan Tray 1       REV 04   740-014971   TP1829            Fan Tray
```


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show chassis hardware detail

```
user@host> show chassis hardware detail
Hardware inventory:
Item             Version  Part number  Serial number     Description
    Chassis                                 JN000968AB        J4300
    Midplane         REV 05   710-010001   ad04420077
    System IO        REV 07   710-010003   AE04420393        System IO board
    Routing Engine   REV 08   750-010005   btrd43500196      RE-J.2
      ad0     488 MB  512MB CHH            504754C53A711400  Compact Flash
      ad2     488 MB  512MB CHH            504754C43A711400  Removable Compact
Flash
    FPC 2            REV 08   750-013493   NB9161            FPC
      PIC 0                                                  Integrated Services
 Module
      ANNEX          REV 08   750-013493   NB9161            Integrated Services
```

## Sample Output

### show chassis hardware detail node 1

```
user@host> show chassis hardware detail node 1
node1:
--------------------------------------------------------------------------
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                 JN108C688ADB      J6350
Midplane         REV 03   710-014593   NM7516
System IO        REV 01   710-016210   NN9781            JX350 System IO
Crypto Module                                           Crypto Acceleration
Routing Engine   REV 08   710-015273   NM6569            RE-J6350-3400
  ad0     991 MB  1GB CKS              20060000000000000800 Compact Flash
FPC 0                                                   FPC
FPC 3            REV 06   750-013492   NM1294            FPC
FPC 6            REV 11   750-015153   NP8750            FPC
```

## Sample Output

### show chassis hardware extensive

```
user@host> show chassis hardware extensive
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                 JN107a494ADA      J4350
 Jedec Code:   0x0000            EEPROM Version:    0x00
 P/N:          ..........        S/N:               JN107a494ADA
 Assembly ID:  0x0513            Assembly Version:  00.00
 Date:         00-00-0000        Assembly Flags:    0x00
 Version:      ..........
 ID: j4350
...
FPC 5            REV 08   750-013493   NB9161            FPC
 Jedec Code:   0x7fb0            EEPROM Version:    0x01
 P/N:          750-013493        S/N:               S/N NB9161
 Assembly ID:  0x073c            Assembly Version:  01.08
 Date:         03-03-2006        Assembly Flags:    0x00
 Version:      REV 08
 ID: FPC                         FRU Model Number:  SSG-EPIM-1TX
 Board Information Record:
  Address 0x00: 34 01 05 05 02 ff ff ff ff ff ff ff ff ff ff ff
 I2C Hex Data:
  Address 0x00: 7f b0 01 ff 07 3c 01 08 52 45 56 20 30 38 00 00
```

Copyright © 2013, Juniper Networks, Inc.

```
  Address 0x10: 00 00 00 00 37 35 30 2d 30 31 33 34 39 33 00 00
  Address 0x20: 53 2f 4e 20 4e 42 39 31 36 31 00 00 00 03 03 07
  Address 0x30: d6 ff ff ff 34 01 05 05 02 ff ff ff ff ff ff ff
  Address 0x40: ff ff ff ff 01 00 00 00 00 00 00 00 00 00 00 53
  Address 0x50: 53 47 2d 45 50 49 4d 2d 31 54 58 00 00 00 00 00
  Address 0x60: 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff
  Address 0x70: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
  PIC 0                                                 Integrated Services
Module
 Jedec Code:   0x7fb0            EEPROM Version:    0x01
 Assembly ID:  0x063c            Assembly Version:  01.08
 Date:         03-03-2006        Assembly Flags:    0x00
 ID: Integrated Services Module
 Board Information Record:
  Address 0x00: 34 01 05 05 02 ff ff ff ff ff ff ff ff ff ff ff
 I2C Hex Data:
  Address 0x00: 7f b0 01 ff 06 3c 01 08 00 00 00 00 00 00 00 00
  Address 0x10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  Address 0x20: 00 00 00 00 00 00 00 00 00 00 00 00 00 03 03 07
  Address 0x30: d6 ff ff ff 34 01 05 05 02 ff ff ff ff ff ff ff
  Address 0x40: ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 53
  Address 0x50: 53 47 2d 45 50 49 4d 2d 31 54 58 00 00 00 00 00
  Address 0x60: 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff
  Address 0x70: ff ff ff ff ed c0 0e 0b 00 00 00 00 00 00 00 00
  ANNEX          REV 08   750-013493   NB9161            Integrated Services
 Jedec Code:   0x7fb0            EEPROM Version:    0x01
 P/N:          750-013493        S/N:               S/N NB9161
 Assembly ID:  0x0808            Assembly Version:  01.08
 Date:         03-03-2006        Assembly Flags:    0x00
 Version:      REV 08
 ID: Integrated Services         FRU Model Number:  SSG-EPIM-1TX
 Board Information Record:
  Address 0x00: 34 01 05 05 02 ff ff ff ff ff ff ff ff ff ff ff
 I2C Hex Data:
  Address 0x00: 7f b0 01 ff 08 08 01 08 52 45 56 20 30 38 00 00
  Address 0x10: 00 00 00 00 37 35 30 2d 30 31 33 34 39 33 00 00
  Address 0x20: 53 2f 4e 20 4e 42 39 31 36 31 00 00 00 03 03 07
  Address 0x30: d6 ff ff ff 34 01 05 05 02 ff ff ff ff ff ff ff
  Address 0x40: ff ff ff ff 01 00 00 00 00 00 00 00 00 00 00 53
  Address 0x50: 53 47 2d 45 50 49 4d 2d 31 54 58 00 00 00 00 00
  Address 0x60: 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff
  Address 0x70: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
```

## Sample Output

### show chassis hardware models (SRX1400 and SRX3000 devices)

```
user@host> show chassis hardware models
Hardware inventory:
Item             Version  Part number  Serial number     FRU model number
Midplane         REV 07   710-020310   VP8136            SRX3600-CHAS
PEM 0            rev 05   740-027644   G087E6003S05P     AC Power Supply
PEM 1            rev 05   740-027644   G087E600AT05P     AC Power Supply
CB 0             REV 11   750-021914   AAAC9887          SRX3K-RE-12-10
  Routing Engine          BUILTIN      BUILTIN
  CPP                     BUILTIN      BUILTIN
FPC 0            REV 11   750-021882   AAAD9785          SRX3K-SFB-12GE
FPC 1            REV 10   750-016077   AAAE9989          SRX3K-SPC-1-10-40
FPC 2            REV 11   750-016077   AAAT8490          SRX3K-SPC-1-10-40
FPC 5            REV 15   750-020321   AABB3820          SRX3K-2XGE-XFP
FPC 10           REV 12   750-043828   AAAD9501          SRX1K3K-NP-2XGE-SFPP
Fan Tray 0       REV 06   750-021599   VR9734            SRX3600-FAN
```


Copyright © 2013, Juniper Networks, Inc.

show chassis hardware models (SRX5600 and SRX5800 devices)

```
user@host> show chassis hardware models
Hardware inventory:
Item             Version  Part number  Serial number     FRU model number
Midplane         REV 03   710-013698   TR0779            CHAS-BP-MX960-S
FPM Board        REV 03   710-014974   KC3406            CRAFT-MX960-S
Routing Engine 0 REV 06   740-015113   1000696955        RE-S-1300-2048-S
CB 0             REV 07   710-013385   JZ3257            SCB-MX960-S
```

## Sample Output

show chassis hardware clei-models (SRX5600 and SRX5800 devices)

```
user@host> show chassis hardware clei-models
Hardware inventory:
Item             Version  Part number  CLEI code         FRU model number
FPM Board        REV 02   710-017254                     CRAFT-MX480-S
Routing Engine 0 REV 06   740-015113                     RE-S-1300-2048-S
CB 0             REV 07   710-013385                     SCB-MX960-S
Fan Tray                                                 SRX5600-FAN
```

## Sample Output

show chassis hardware models (SRX5600 and SRX5800 devices for next-generation SPC)

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                               JN11C3B72AGA      SRX 5800
Midplane         REV 01   710-024803   ABAB6412          SRX 5800 Backplane
FPM Board        REV 01   710-024632   YS1437            Front Panel Display
PDM              Rev 03   740-013110   QCS152250EZ       Power Distribution Modu
le
PEM 0            Rev 05   740-023516   QCS1452F08U       DC Power Entry Module
PEM 1            Rev 05   740-023516   QCS1452F084       DC Power Entry Module
Routing Engine 0 REV 09   740-023530   9009080059        SRX5k RE-13-20
CB 0             REV 05   710-024802   ZJ7533            SRX5k SCB
CB 1             REV 05   710-024802   ZJ7603            SRX5k SCB
FPC 0            REV 25   750-020235   YF6692            SRX5k DPC 40x 1GE
  CPU            REV 03   710-024633   YF5990            SRX5k DPC PMB
  PIC 0                   BUILTIN      BUILTIN           10x 1GE RichQ
    Xcvr 0       REV 02   740-011613   PJ93U0P           SFP-SX
    Xcvr 1       REV 02   740-011613   PJ93U7C           SFP-SX
  PIC 1                   BUILTIN      BUILTIN           10x 1GE RichQ
  PIC 2                   BUILTIN      BUILTIN           10x 1GE RichQ
    Xcvr 0       REV 02   740-011613   PJ93U95           SFP-SX
    Xcvr 1       REV 02   740-011613   PJ93YZW           SFP-SX
  PIC 3                   BUILTIN      BUILTIN           10x 1GE RichQ
FPC 9            REV 02   750-044175   ZY2574            SRX5k SPC II
CPU                      BUILTIN      BUILTIN           SRX5k DPC PPC
  PIC 0                   BUILTIN      BUILTIN           SPU cp
  PIC 1                   BUILTIN      BUILTIN           SPU flow
  PIC 2                   BUILTIN      BUILTIN           SPU flow
  PIC 3                   BUILTIN      BUILTIN           SPU flow
Fan Tray 0       REV 05   740-014971   VT5896            Fan Tray
Fan Tray 1       REV 05   740-014971   VT5894            Fan Tray
```

Copyright © 2013, Juniper Networks, Inc.

## show chassis power

**Syntax** show chassis power

**Release Information** Command modified in Junos OS Release 12.1X44-D10.

**Description** Display power limits and usage information for the Power Entry Modules (PEMs).

**Options** This command has no options.

**Required Privilege Level** view

**Related Documentation**
- show chassis power sequence

**List of Sample Output** show chassis power on page 1615

**Output Fields** Table 23 on page 1614 lists the output fields for the **show chassis power** command. Output fields are listed in the approximate order in which they appear.

### Table 23: show chassis power Output Fields

| Field Name | Field Description |
|---|---|
| **PEM number** | AC or DC PEM number on the chassis. The following output fields are displayed for the PEM:<br>• State—State of the PEM:<br>  ◦ Online—PEM is present in the slot and online.<br>  ◦ Empty—PEM is not present in the slot.<br>  ◦ Present—PEM is present in the slot, but not online.<br>• AC Input —State of the AC input power feed with the number of active and expected feeds (1 or 2).<br>• Capacity—Actual power input capacity with maximum capacity displayed (in parentheses) in watts.<br>• DC Output—DC power output, in watts, for the specified zone, at the specified amps and voltage (A @ V), and load and percentage utilization of the maximum capacity for the zone. |
| **System** | Overall power statistics for the system zone:<br>• Zone number:<br>  ◦ Capacity—Maximum power capacity available for the zone, in watts.<br>  ◦ Allocated power—Actual capacity allocated for the zone, in watts, with remaining power displayed in parentheses.<br>  ◦ Actual usage—Actual power usage for the zone, in watts.<br>• Total system capacity—Cumulative power capacity of all the zones, in watts.<br>• Total remaining capacity—Difference between the total system capacity and cumulative allocated power of all zones, in watts. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show chassis power

```
user@host> show chassis power

PEM 0:
  State:     Present
  DC input:  Out of range (1 feed expected, 0 feed connected)
  DC input:  48.0 V input (0 mV)
  Capacity:  0 W (maximum 4100 W)

PEM 1:
  State:     Present
  DC input:  Out of range (1 feed expected, 0 feed connected)
  DC input:  48.0 V input (0 mV)
  Capacity:  0 W (maximum 4100 W)

PEM 2:
  State:     Online
  DC input:  OK (2 feed expected, 2 feed connected)
  DC input:  48.0 V input (57500 mV)
  Capacity:  4100 W (maximum 4100 W)
  DC output: 1881 W (zone 0, 33 A at 57 V, 45% of capacity)

PEM 3:
  State:     Online
  DC input:  OK (2 feed expected, 2 feed connected)
  DC input:  48.0 V input (56500 mV)
  Capacity:  4100 W (maximum 4100 W)
  DC output: 2464 W (zone 1, 44 A at 56 V, 60% of capacity)

System:
  Zone 0:
      Capacity:          4100 W (maximum 4100 W)
      Allocated power:   2920 W (1180 W remaining)
      Actual usage:      1881 W
  Zone 1:
      Capacity:          4100 W (maximum 4100 W)
      Allocated power:   3875 W (225 W remaining)
      Actual usage:      2464 W
  Total system capacity: 8200 W (maximum 8200 W)
  Total remaining power: 1405 W
```

Copyright © 2013, Juniper Networks, Inc.

## show chassis power sequence

**Syntax** show chassis power sequence

**Release Information** Command modified in Junos OS Release 12.1X44-D10.

**Description** Display the power-on sequence for the FPCs in the chassis. The numbers indicate the slot number of the FPCs.

**Options** This command has no options.

**Required Privilege Level** view

**Related Documentation**
- fru-poweron-sequence

**List of Sample Output** show chassis power sequence on page 1616

**Output Fields** Table 24 on page 1616 lists the output fields for the **show chassis power sequence** command. Output fields are listed in the approximate order in which they appear.

Table 24: show chassis power sequence Output Fields

| Field Name | Field Description |
|---|---|
| **Chassis FRU Power Sequence** | Power-on sequence for the FPCs in the chassis. The numbers indicate the slot number of the FPCs. |

### Sample Output

show chassis power sequence

```
user@host> show chassis power sequence
Chassis FRU Power On Sequence: 0 1 2 3 4 5 6 7 8 9 10 11
```


Copyright © 2013, Juniper Networks, Inc.

## show chassis routing-engine (View)

**Syntax** show chassis routing-engine

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** Display the Routing Engine status of the chassis cluster.

**Required Privilege Level** view

**Related Documentation**
- Device Configuration

**List of Sample Output**
show chassis routing-engine on page 1618
show chassis routing-engine on page 1618

**Output Fields** Table 25 on page 1617 lists the output fields for the **show chassis routing-engine** command. Output fields are listed in the approximate order in which they appear.

### Table 25: show chassis routing-engine Output Fields

| Field Name | Field Description |
|---|---|
| **Temperature** | Routing Engine temperature. |
| **CPU temperature** | CPU temperature. |
| **Total memory** | Total memory available on the system. |
| **Control plane memory** | Memory available for the control plane. |
| **Data plane memory** | Memory reserved for data plane processing. |
| **CPU utilization** | Current CPU utilization statistics on the control plane core. |
| **User** | Current CPU utilization in user mode on the control plane core. |
| **Background** | Current CPU utilization in nice mode on the control plane core. |
| **Kernel** | Current CPU utilization in kernel mode on the control plane core. |
| **Interrupt** | Current CPU utilization in interrupt mode on the control plane core. |
| **Idle** | Current CPU utilization in idle mode on the control plane core. |
| **Model** | Routing Engine model. |
| **Start time** | Routing Engine start time. |
| **Uptime** | Length of time the Routing Engine has been up (running) since the last start. |

Copyright © 2013, Juniper Networks, Inc.

Table 25: show chassis routing-engine Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Last reboot reason** | Reason for the last reboot of the Routing Engine. |
| **Load averages** | The average number of threads waiting in the run queue or currently executing over 1-, 5-, and 15-minute periods. |

## Sample Output

### show chassis routing-engine

```
user@host> show chassis routing-engine (Sample 1)
Routing Engine status:
    Temperature                38 degrees C / 100 degrees F
    CPU temperature            36 degrees C / 96 degrees F
    Total memory              512 MB Max   435 MB used ( 85 percent)
      Control plane memory    344 MB Max   296 MB used ( 86 percent)
      Data plane memory       168 MB Max   138 MB used ( 82 percent)
    CPU utilization:
      User                     8 percent
      Background               0 percent
      Kernel                   4 percent
      Interrupt                0 percent
      Idle                    88 percent
    Model                        RE-SRX240-LOWMEM
    Serial ID                    AAAP8652
    Start time                   2009-09-21 00:04:54 PDT
    Uptime                       52 minutes, 47 seconds
    Last reboot reason           0x200:chassis control reset
    Load averages:               1 minute   5 minute  15 minute
                                     0.12       0.15       0.10
```

## Sample Output

### show chassis routing-engine

```
user@host> show chassis routing-engine (Sample 2)
Routing Engine status:
    Temperature                46 degrees C / 114 degrees F
    CPU temperature            46 degrees C / 114 degrees F
    Total memory             1024 MB Max   737 MB used ( 72 percent)
      Control plane memory    600 MB Max   426 MB used ( 71 percent)
      Data plane memory       424 MB Max   314 MB used ( 74 percent)
    CPU utilization:
      User                    40 percent
      Background               0 percent
      Kernel                  11 percent
      Interrupt                0 percent
      Idle                    49 percent
    Model                        RE-SRXSME-SRE6
    Start time                   2009-09-19 20:04:18 PDT
    Uptime                       1 day, 4 hours, 51 minutes, 11 seconds
    Last reboot reason           0x200:chassis control reset
    Load averages:               1 minute   5 minute  15 minute
                                     0.27       0.53       0.78
```


Copyright © 2013, Juniper Networks, Inc.

## show chassis usb storage

**Syntax** show chassis usb storage

**Release Information** Command introduced in Junos OS Release 11.4 R2.

**Description** Displays the current status of any USB mass storage device and whether the USB ports are enabled or disabled.

**Required Privilege Level** view

**Related Documentation**
- Upgrades and Downgrades

**List of Sample Output**
show chassis hardware detail on page 1619
show chassis usb storage on page 1619

### Sample Output

show chassis hardware detail

```
user@host> show chassis hardware detail
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                BV4911AA0005      SRX240H2-POE
Routing Engine   REV 01   750-043613   AAEC1923          RE-SRX240H2-POE
  usb0 (addr 1)  DWC OTG root hub 0    vendor 0x0000     uhub0
  usb0 (addr 2)  product 0x005a 90     vendor 0x0409     uhub1
  usb0 (addr 3)  ST72682  High Speed Mode 64218 STMicroelectronics umass0
  usb0 (addr 4)  Mass Storage Device 4096 JetFlash       umass1
FPC 0                                                  FPC
  PIC 0                                                16x GE Base PIC
Power Supply 0
```

show chassis usb storage

```
user@host> show chassis usb storage
USB Disabled
```

## show class-of-service application-traffic-control counter

**Syntax** show class-of-service application-traffic-control counter

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Display AppQoS DSCP marking and honoring statistics based on layer-7 application classifiers.

**Required Privilege Level** view

**Related Documentation**
- Application Quality of Service
- CoS Virtual Channels and Tunnels
- CoS Components

**List of Sample Output** show class-of-service application-traffic-control counter on page 1621

**Output Fields** Table 26 on page 1620 lists the output fields for the **show class-of-service application-traffic-control counter** command. Output fields are listed in the approximate order in which they appear.

Table 26: show class-of-service application-traffic-control counter Output Fields

| Field Name | Field Description |
|---|---|
| **pic** | PIC number of the accumulated statistics. |
| **Sessions processed** | The number of sessions where the class of service was checked. |
| **Sessions marked** | The number of sessions marked based on application-aware DSCP marking. |
| **Sessions honored** | The number of sessions honored based on application-aware traffic honoring. |
| **Sessions rate limited** | The number of sessions that have been rate limited. |
| **Client-to-server flows rate limited** | The number of client-to-server flows that have been rate limited. |
| **Server-to-client flows rate limited** | The number of server-to-client flows that have been rate limited. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show class-of-service application-traffic-control counter

```
user@host> show class-of-service application-traffic-control counter
pic: 2/1
  Counter type                                          Value
  Sessions processed                                    300
  Sessions marked                                       200
  Sessions honored                                      0
  Sessions rate limited                                 100
  Client-to-server flows rate limited                   100
  Server-to-client flows rate limited                   70

pic: 2/0
  Counter type                                          Value
  Sessions processed                                    400
  Sessions marked                                       300
  Sessions honored                                      0
  Sessions rate limited                                 200
  Client-to-server flows rate limited                   200
  Server-to-client flows rate limited                   100
```

Copyright © 2013, Juniper Networks, Inc.

## show class-of-service application-traffic-control statistics rate-limiter

**Syntax** show class-of-service application-traffic-control statistics rate-limiter

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Display AppQoS real-time run information about application rate limiting of current or recent sessions.

**Required Privilege Level** view

**Related Documentation**
- Application Quality of Service
- CoS Virtual Channels and Tunnels
- CoS Components

**List of Sample Output** show class-of-service application-traffic-control statistics rate-limiter on page 1623

**Output Fields** Table 27 on page 1622 lists the output fields for the **show class-of-service application-traffic-control statistics rate-limiter** command. Output fields are listed in the approximate order in which they appear.

Table 27: show class-of-service application-traffic-control statistics rate-limiter Output Fields

| Field Name | Field Description |
|---|---|
| **pic** | PIC number. |
| **Ruleset** | The ruleset applied on the sesssion. |
| **Application** | The application match for applying the ruleset. |
| **Client-to-server** | The rate limiter applied from client to server. |
| **Rate(bps)** | The rate in the client-to-server direction |
| **Server-to-client** | The rate limiter applied from server to client. |
| **Rate(bps)** | The rate in the server-to-client direction. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show class-of-service application-traffic-control statistics rate-limiter

```
user@host> show class-of-service application-traffic-control statistics rate-limiter
pic: 2/1
  Ruleset       Application  Client-to-server   Rate(bps)   Server-to-client
Rate(bps)
  my-ruleset-1  HTTP         my-http-c2s-rl     10000000    my-http-s2c-rl
20000000
  my-ruleset-2  HTTP         my-http-c2s-rl-2   20000000    my-http-s2c-rl-2
30000000
  my-ruleset-2  FTP          my-ftp-c2s-rl      50000       my-ftp-s2c-rl
50000
  ...

pic: 2/0
  Ruleset       Application  Client-to-server   Rate(bps)   Server-to-client
Rate(bps)
  my-ruleset-1  HTTP         my-http-c2s-rl     10000000    my-http-s2c-rl
20000000
  my-ruleset-2  HTTP         my-http-c2s-rl-2   20000000    my-http-s2c-rl-2
30000000
  my-ruleset-2  FTP          my-ftp-c2s-rl      50000       my-ftp-s2c-rl
50000
```

Copyright © 2013, Juniper Networks, Inc.

## show class-of-service application-traffic-control statistics rule

**Syntax** show class-of-service application-traffic-control statistics rule

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Display AppQoS counters identifying rule hits.

**Required Privilege Level** view

**Related Documentation**
- Application Quality of Service
- CoS Virtual Channels and Tunnels
- CoS Components

**List of Sample Output** show class-of-service application-traffic-control statistics rule on page 1624

**Output Fields** Table 28 on page 1624 lists the output fields for the **show class-of-service application-traffic-control statistics rule** command. Output fields are listed in the approximate order in which they appear.

Table 28: show class-of-service application-traffic-control statistics rule Output Fields

| Field Name | Field Description |
|---|---|
| **pic** | PIC number where the rule is applied. |
| **Ruleset** | The ruleset containing the rule. |
| **Rule** | The rule to which the statistic applies. |
| **Hits** | The number of times a match for the rule was encountered. |

### Sample Output

show class-of-service application-traffic-control statistics rule

```
user@host> show class-of-service application-traffic-control statistics rule
pic: 2/0
  Ruleset          Rule          Hits
  my-ruleset-1     ftp-rule      100
  my-ruleset-1     httpp-rule    100
  my-ruleset-2     telnet-rule   300
  my-ruleset-2     smtp-rule     300
  ...

pic: 2/1
  Ruleset          Rule          Hits
  my-ruleset-1     ftp-rule      200
  my-ruleset-1     httpp-rule    300
  my-ruleset-2     telnet-rule   400
  my-ruleset-2     smtp-rule     500
```


Copyright © 2013, Juniper Networks, Inc.

## show class-of-service forwarding-class

**Syntax** show class-of-service forwarding-class

**Release Information** Command introduced before Release 12.1 of Junos OS.

**Description** Display mapping of forwarding class names to queues.

**Required Privilege Level** view

**Related Documentation**
- IDP Class of Service Action for Security Devices
- CoS Virtual Channels and Tunnels
- CoS Components

**List of Sample Output** show class-of-service forwarding-class on page 1626

**Output Fields** Table 29 on page 1625 lists the output fields for the **show class-of-service forwarding-class** command. Output fields are listed in the approximate order in which they appear.

### Table 29: show class-of-service forwarding-class Output Fields

| Field Name | Field Description |
|---|---|
| **Forwarding class** | Forwarding class name. |
| **ID** | ID number assigned to the forwarding class. |
| **Queue** | Queue number. |
| **Restricted queue** | Restricted queue number. |
| **Fabric priority** | Fabric priority, either low or high. |
| **Policing priority** | Layer 2 policing, either premium or normal. |
| **SPU priority** | Services Processing Unit (SPU) priority queue, either high or low. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show class-of-service forwarding-class

```
user@host> show class-of-service forwarding-class
Forwarding class        ID  Queue  Restricted queue  Fabric priority  Policing
priority  SPU priority
  best-effort            0   0          0             low              normal
          low
  expedited-forwarding   1   1          1             low              normal
          high
  assured-forwarding     2   2          2             low              normal
          low
  network-control        3   3          3             low              normal
          low
```


Copyright © 2013, Juniper Networks, Inc.

## show configuration smtp

**Syntax** show configuration smtp

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Display complete SMTP information.

**Options**
- apply-groups—Groups from which SMTP inherits configuration data.
- apply-groups-except—Groups from which SMTP restricts inheriting configuration data.

**Required Privilege Level** view

**List of Sample Output** show configuration smtp on page 1627

**Output Fields** Table 30 on page 1627 describes the output fields for the **show configuration smtp** command.

### Table 30: show configuration smtp

| Field Name | Field Description | Level of Output |
|---|---|---|
| **address** | SMTP server's IPv4 address | All levels |
| login | Configure a mail sender account to the server | All levels |
| password | Default sender password for user authentication | All levels |

### Sample Output

show configuration smtp

```
user@host> show configuration smtp
primary-server {
    address 218.102.48.213;
    login "dayone@netvigator.com" {
        password "$9$YhgoZ.PQ6CuTQlKMLN-qmP"; ## SECRET-DATA
    }
}
```

Copyright © 2013, Juniper Networks, Inc.

## show dhcp client binding

**Syntax**

show dhcp client binding
[<address> |interface <interface-name>]
routing-instance <routing-instance name>
[brief | detail | summary ]

**Release Information**

Statement introduced in Junos OS Release 12.1X44-D10.

**Description**

Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) client table.

**Options**

**address**—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:

- ip-address—The specified IP address.
- mac-address—The specified MAC address.

**routing-instance <routing-instance name>**—(Optional) Display DHCP binding information for DHCP clients on the specified routing instance.

**interface <interface-name>**—(Optional) Perform this operation on the specified interface.

**brief**—(Optional) Display brief information about the active client bindings.

**detail**—(Optional) Display detailed client binding information.

**summary**—(Optional) Display a summary of DHCP client information.

**Required Privilege Level**

view

**Related Documentation**

- clear dhcp client binding on page 1365
- Device Configuration

**List of Sample Output**

show dhcp client binding on page 1629

**Output Fields**

Table 31 on page 1628 lists the output fields for the **show dhcp client binding** command. Output fields are listed in the approximate order in which they appear.

### Table 31: show dhcp client binding Output Fields

| Field Name | Field Description |
|---|---|
| IP address | IP address of the DHCP client. |
| Hardware address | Hardware address of the DHCP client. |
| Server | IP address of the DHCP server. |


Copyright © 2013, Juniper Networks, Inc.

Table 31: show dhcp client binding Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| Expires | Number of seconds in which the lease expires. |
| State | State of the address binding table on the DHCP local server. |
| Interface | Interface on which the request was received. |
| Lease Expires | Date and time at which the client's IP address lease expires. |
| Lease Expires in | Number of seconds in which the lease expires. |
| Lease Start | Date and time at which the client's IP address lease started. |
| Vendor Identifier | Vendor identifier. |
| Server Identifier | IP address of the DHCP server. |
| Client IP Address | IP address of the DHCP client. |

## Sample Output

### show dhcp client binding

```
user@host> show dhcp client binding
2 clients, (2 bound,  0 init, 0 discover, 0 renew, 0 rebind)

              IP address      Hardware address     Server      Expires     State
     Interface
              10.1.1.89       00:0a:12:00:12:12    10.1.1.1    348         BOUND
     fe-0/0/1.0
              20.1.1.90       00:0a:12:00:12:34    20.1.1.1    568         BOUND
     fe-0/0/2.0

user@host> show dhcp client binding interface fe-0/0/1.0 detail
Client Interface: fe-0/0/1.0
                  Hardware address:       00:0a:12:00:12:12
                  State:                  BOUND
                  Lease Expires:          2010-09-16 14:45:41 UTC
                  Lease Expires in:       528 seconds
                  Lease Start:            2010-09-16 14:35:41 UTC
                  Vendor Identifier:      ether
                  Server Identifier:      10.1.1.1
                  Client IP Address:      10.1.1.89
                  update server           enabled

                DHCP Options :
                    Name: name-server, Value: [ 10.209.194.131, 2.2.2.2, 3.3.3.3 ]
                    Name: server-identifier, Value: 10.1.1.1
                    Name: router, Value: [ 10.1.1.80 ]
                    Name: domain-name, Value: netscreen-50

user@host> show dhcp client binding 10.1.1.89
```

Copyright © 2013, Juniper Networks, Inc.

```
IP address      Hardware address     Server      Expires     State      Interface

        10.1.1.89       00:0a:12:00:12:12    10.1.1.1    348         BOUND
 fe-0/0/1.0
```


Copyright © 2013, Juniper Networks, Inc.

## show dhcp client statistics

**Syntax** show dhcp client statistics
routing-instance <routing-instance-name>

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Display Dynamic Host Configuration Protocol (DHCP) client statistics.

**Options** **routing-instance routing-instance-name**—(Optional) Display the statistics for DHCP clients on the specified routing instance.

**Required Privilege Level** view

**Related Documentation**
- clear dhcp client statistics on page 1366
- Device Configuration

**List of Sample Output** show dhcp client statistics on page 1632

**Output Fields** Table 32 on page 1631 lists the output fields for the **show dhcp client statistics** command. Output fields are listed in the approximate order in which they appear.

Table 32: show dhcp client statistics

| Field Name | Field Description |
|---|---|
| Packets dropped | Number of packets discarded by the DHCP local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears. |
| Messages received | Number of DHCP messages received.<br>• BOOTREPLY—Number of BOOTP protocol data units (PDUs) received<br>• DHCPOFFER—Number of DHCP PDUs of type OFFER received<br>• DHCPACK—Number of DHCP PDUs of type ACK received<br>• DHCPNACK—Number of DHCP PDUs of type NACK received<br>• DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW received |

Copyright © 2013, Juniper Networks, Inc.

Table 32: show dhcp client statistics *(continued)*

| Field Name | Field Description |
|---|---|
| Messages sent | Number of DHCP messages sent.<br>• BOOTREQUEST—Number of BOOTP protocol data units (PDUs) transmitted<br>• DHCPDECLINE—Number of DHCP PDUs of type DECLINE transmitted<br>• DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER transmitted<br>• DHCPREQUEST—Number of DHCP PDUs of type REQUEST transmitted<br>• DHCPINFORM—Number of DHCP PDUs of type INFORM transmitted<br>• DHCPRELEASE—Number of DHCP PDUs of type RELEASE transmitted<br>• DHCPRENEW—Number of DHCP PDUs of type RENEW transmitted<br>• DHCPREBIND—Number of DHCP PDUs of type REBIND transmitted |

## Sample Output

### show dhcp client statistics

```
user@host> show dhcp client statistics
Packets dropped:
    Total                     0
Messages received:
    BOOTREPLY                 0
    DHCPOFFER                 0
    DHCPACK                   0
    DHCPNAK                   0
    DHCPFORCERENEW            0
Messages sent:
    BOOTREQUEST               0
    DHCPDECLINE               0
    DHCPDISCOVER              0
    DHCPREQUEST               0
    DHCPINFORM                0
    DHCPRELEASE               0
    DHCPRENEW                 0
    DHCPREBIND                0
```


Copyright © 2013, Juniper Networks, Inc.

## show dhcp relay binding

**Syntax**

Show dhcp relay binding
[<address> |interface <interface-name>]
routing-instance <routing-instance name>
[brief | detail | summary]

**Release Information**

Statement introduced in Junos OS Release 12.1X44-D10.

**Description**

Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) relay client table.

**Options**

**address**—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:

- ip-address—The specified IP address.
- mac-address—The specified MAC address.

**routing-instance <routing-instance name>**—(Optional) Display DHCP binding information on the specified routing instance.

**interface <interface-name>**—(Optional) Perform this operation on the specified interface.

**brief**—(Optional) Display brief information about the active client bindings.

**detail**—(Optional) Display detailed client binding information.

**summary**—(Optional) Display a summary of DHCP client information.

**Required Privilege Level**

view

**Related Documentation**

- clear dhcp relay binding on page 1367
- Device Configuration

**List of Sample Output**

show dhcp relay binding on page 1634

**Output Fields**

Table 33 on page 1633 lists the output fields for the **show dhcp relay binding** command. Output fields are listed in the approximate order in which they appear.

### Table 33: show dhcp relay binding Output Fields

| Field Name | Field Description |
|---|---|
| IP address | IP address of the DHCP client. |
| Hardware address | Hardware address of the DHCP client. |
| Request received on | Interface on which the request was received. |

Copyright © 2013, Juniper Networks, Inc.

Table 33: show dhcp relay binding Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| Type | Type of DHCP packet processing performed on the device. |
| Obtained at | Date and time at which the client's IP address lease started. |
| Expires at | Date and time at which the client's IP address lease expires. |
| State | State of the address binding table on the DHCP local server. |

## Sample Output

### show dhcp relay binding

```
user@host> show dhcp relay binding detail
IP address       Hardware address   Type     Lease expires            State
       100.20.32.1      90:00:00:01:00:01  active   2007-01-17 11:38:47 PST
rebind
       100.20.32.3      90:00:00:02:00:01  active   2007-01-17 11:38:41 PST
rebind
       100.20.32.4      90:00:00:03:00:01  active   2007-01-17 11:38:01 PST
rebind
       100.20.32.5      90:00:00:04:00:01  active   2007-01-17 11:38:07 PST
rebind
       100.20.32.6      90:00:00:05:00:01  active   2007-01-17 11:38:47 PST
rebind


user@host> show dhcp relay binding 100.20.32.1
Active binding information:
           IP address               100.20.32.1
           Hardware address         90:00:00:01:00:01

       Lease information:
          Type               DHCP
          Obtained at        2007-01-17 11:28:47 PST
          Expires at         2007-01-17 11:38:47 PST

       > show dhcp relay binding 100.20.32.1 detail
       Active binding information:
           IP address              100.20.32.1
           Hardware address        90:00:00:01:00:01
           Request received on     fe-0/0/2.0, relayed by 100.20.32.2

       Lease information:
           Type                DHCP
           Obtained at         2007-01-17 11:28:47 PST
           Expires at          2007-01-17 11:38:47 PST
           State               rebind
```


Copyright © 2013, Juniper Networks, Inc.

## show dhcp relay statistics

**Syntax** show dhcp relay statistics
[<routing-instance>]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Display Dynamic Host Configuration Protocol (DHCP) relay statistics.

**Options** **routing-instance**—(Optional) Display the DHCP relay statistics on the specified routing instance.

**Required Privilege Level** view

**Related Documentation**
- clear dhcp relay statistics on page 1368
- Device Configuration

**List of Sample Output** show dhcp relay statistics on page 1636

**Output Fields** Table 34 on page 1635 lists the output fields for the **show dhcp relay statistics** command. Output fields are listed in the approximate order in which they appear.

### Table 34: show dhcp relay statistics

| Field Name | Field Description |
|---|---|
| Messages received | Number of DHCP messages sent.<br>• BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received<br>• DHCPDECLINE—Number of DHCP PDUs of type DECLINE received<br>• DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received<br>• DHCPREQUEST—Number of DHCP PDUs of type REQUEST received<br>• DHCPINFORM—Number of DHCP PDUs of type INFORM received<br>• DHCPRELEASE—Number of DHCP PDUs of type RELEASE received |
| Messages sent | Number of DHCP messages received.<br>• BOOTREPLY—Number of BOOTP PDUs transmitted<br>• DHCPOFFER—Number of DHCP PDUs of type OFFER transmitted<br>• DHCPACK—Number of DHCP PDUs of type ACK transmitted<br>• DHCPNACK—Number of DHCP PDUs of type NACK transmitted<br>• DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW transmitted |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show dhcp relay statistics

```
user@host> show dhcp relay statistics
Messages received:
    BOOTREQUEST                 0
    DHCPDECLINE                 0
    DHCPDISCOVER                0
    DHCPINFORM                  0
    DHCPRELEASE                 0
    DHCPREQUEST                 0

Messages sent:
    BOOTREPLY                   0
    DHCPOFFER                   0
    DHCPACK                     0
    DHCPNAK                     0
    DHCPFORCERENEW              0
```


Copyright © 2013, Juniper Networks, Inc.

## show dhcp server binding

**Syntax**

show dhcp server binding
[interface <interface name>]
<brief | detail | summary | verbose>
<ip-address | MAC address>
<routing-instance routing-instance-name>

**Release Information**

Statement introduced in Junos OS Release 12.1X44-D10.

**Description**

Display the address bindings in the client table on the Dynamic Host Configuration Protocol (DHCP) local server.

**Options**

**interface <interface name>**—(Optional) Display information about active client bindings on the specified interface.

**brief | detail | summary**—(Optional) Display the specified level of output about active client bindings. The default is brief, which produces the same output as **show dhcp server binding**.

**ip-address**—Display DHCP binding information for a specific client identified by the specified IP address.

**MAC address**—Display DHCP binding information for a specific client identified by the specified MAC address.

**routing-instance routing-instance-name**—(Optional) Display information about active client bindings for DHCP clients on the specified routing instance.

**Required Privilege Level**

view

**Related Documentation**

- clear dhcp server binding on page 1369
- Device Configuration

**List of Sample Output**

show dhcp server binding on page 1638

**Output Fields**

Table 35 on page 1637 lists the output fields for the show dhcp server binding command. Output fields are listed in the approximate order in which they appear.

### Table 35: show dhcp server binding Output Fields

| Field Name | Field Description |
|---|---|
| IP address | IP address of the DHCP client. |
| Hardware address | Hardware address of the DHCP client. |
| Request received on | Interface on which the request was received. |

Table 35: show dhcp server binding Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| Type | Type of DHCP packet processing performed on the device. |
| Obtained at | Date and time at which the client's IP address lease started. |
| Expires at | Date and time at which the client's IP address lease expires. |
| State | State of the address binding table on the DHCP local server. |

## Sample Output

### show dhcp server binding

```
user@host> show dhcp server binding 100.20.32.1 detail
Active binding information:
                IP address             100.20.32.1
                Hardware address       90:00:00:01:00:01
                Request received on    fe-0/0/2.0, relayed by 100.20.32.2

            Lease information:
                Type                   DHCP
                Obtained at            2007-01-17 11:28:47 PST
                Expires at             2007-01-17 11:38:47 PST
                State                  rebind
```


Copyright © 2013, Juniper Networks, Inc.

## show dhcp server statistics

**Syntax** show dhcp server statistics
<routing-instance>

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Display d Dynamic Host Configuration Protocol (DHCP) local server statistics.

**Options** **routing-instance**—(Optional) Display information about DHCP local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.

**Required Privilege Level** view

**Related Documentation**
- clear dhcp server statistics on page 1370
- Device Configuration

**List of Sample Output** show dhcp server statistics on page 1640

**Output Fields** Table 36 on page 1639 lists the output fields for the **show dhcp server statistics** command. Output fields are listed in the approximate order in which they appear.

### Table 36: show dhcp server statistics

| Field Name | Field Description |
|---|---|
| Packets dropped | Number of packets discarded by the DHCP local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears. |
| Messages received | Number of DHCP messages sent.<br>• BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received<br>• DHCPDECLINE—Number of DHCP PDUs of type DECLINE received<br>• DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received<br>• DHCPREQUEST—Number of DHCP PDUs of type REQUEST received<br>• DHCPINFORM—Number of DHCP PDUs of type INFORM received<br>• DHCPRELEASE—Number of DHCP PDUs of type RELEASE received |
| Messages sent | Number of DHCP messages received.<br>• BOOTREPLY—Number of BOOTP PDUs transmitted<br>• DHCPOFFER—Number of DHCP PDUs of type OFFER transmitted<br>• DHCPACK—Number of DHCP PDUs of type ACK transmitted<br>• DHCPNACK—Number of DHCP PDUs of type NACK transmitted<br>• DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW transmitted |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show dhcp server statistics

```
user@host> show dhcp server statistics
Packets dropped:
    Total                     0

Messages received:
    BOOTREQUEST               0
    DHCPDECLINE               0
    DHCPDISCOVER              0
    DHCPINFORM                0
    DHCPRELEASE               0
    DHCPREQUEST               0

Messages sent:
    BOOTREPLY                 0
    DHCPOFFER                 0
    DHCPACK                   0
    DHCPNAK                   0
    DHCPFORCERENEW            0
```


Copyright © 2013, Juniper Networks, Inc.

## show dhcpv6 server binding (View)

**Syntax**

**show dhcpv6 server binding**
**<brief | detail | summary>**
**<interface *interface-name*>**
**<routing-instance *routing-instance-name*>**

**Release Information**

Command introduced in Release 10.4 of Junos OS.

**Description**

Display the address bindings in the client table for DCHPv6 local server.

**Options**

- brief | detail | summary—(Optional) Display the specified level of output about active client bindings. The default is **brief**, which produces the same output as **show dhcpv6 server binding**.
- interface *interface-name*—(Optional) Display information about active client bindings on the specified interface.
- routing-instance *routing-instance-name*—(Optional) Display information about active client bindings for DHCPv6 clients on the specified routing instance.

**Required Privilege Level**

view

**Related Documentation**

- clear dhcpv6 server binding (Local Server) on page 1371
- Device Configuration

**List of Sample Output**

show dhcpv6 server binding on page 1643
show dhcpv6 server binding detail on page 1643
show dhcpv6 server binding interface on page 1643
show dhcpv6 server binding interface detail on page 1643
show dhcpv6 server binding prefix on page 1644
show dhcpv6 server binding session-id on page 1644
show dhcpv6 server binding summary on page 1644

**Output Fields**

Table 37 on page 1641 lists the output fields for the **show dhcpv6 server binding** command. Output fields are listed in the approximate order in which they appear.

### Table 37: show dhcv6p server binding Output Fields

| Field Name | Field Description | Level of Output |
|---|---|---|
| *number* clients, (*number* init, *number* bound, *number* selecting, *number* requesting, *number* renewing, *number* releasing) | Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state. | summary |

Copyright © 2013, Juniper Networks, Inc.

Table 37: show dhcv6p server binding Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **Prefix** | Client's DHCPv6 prefix. | **brief**<br>**detail** |
| **Session Id** | Session ID of the subscriber session. | **brief**<br>**detail** |
| **Expires** | Number of seconds in which lease expires. | **brief**<br>**detail** |
| **State** | State of the address binding table on the DHCPv6 local server:<br>• **BOUND**—Client has active IP address lease.<br>• **INIT**—Initial state.<br>• **RELEASE**—Client is releasing IP address lease.<br>• **RECONFIGURE**—Client has received reconfigure message from server.<br>• **RENEWING**—Client sending request to renew IP address lease.<br>• **REQUESTING**—Client requesting a DHCPv6 server.<br>• **SELECTING**—Client receiving offers from DHCPv6 servers. | **brief**<br>**detail** |
| **Interface** | Interface on which the DHCPv6 request was received. | **brief** |
| **Client DUID** | Client's DHCP Unique Identifier (DUID). | **brief**<br>**detail** |
| **Lease expires** | Date and time at which the client's IP address lease expires. | **detail** |
| **Lease expires in** | Number of seconds in which lease expires. | **detail** |
| **Lease Start** | Date and time at which the client's address lease was obtained. | **detail** |
| **Incoming Client Interface** | Client's incoming interface. | **detail** |
| **Server IP Address** | IP address of DHCPv6 server. | **detail** |
| **Server Interface** | Interface of DHCPv6 server. | **detail** |
| **Client Id length** | Length of the DHCPv6 client ID, in bytes. | **detail** |
| **Client Id** | ID of the DHCPv6 client. | **detail** |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show dhcpv6 server binding

```
user@host> show dhcpv6 server binding


Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:bd8:1111:2222::/64 6           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:01
2001:bd8:1111:2222::/64 7           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:02
2001:bd8:1111:2222::/64 8           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
2001:bd8:1111:2222::/64 9           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:04
2001:bd8:1111:2222::/64 10          86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:05
```

### show dhcpv6 server binding detail

```
user@host> show dhcpv6 server binding detail
Session Id:  6
     Client IPv6 Prefix:                   2001:bd8:1111:2222::/64
     Client DUID:                         LL_TIME0x1-0x2e159c0-00:10:94:00:00:01

     State:                                BOUND(bound)
     Lease Expires:                        2009-07-21 10:41:15 PDT
     Lease Expires in:                     86308 seconds
     Lease Start:                          2009-07-20 10:41:15 PDT
     Incoming Client Interface:            ge-1/0/0.0
     Server Ip Address:                    0.0.0.0
     Server Interface:                     none
     Client Id Length:                     14
     Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0001

Session Id:  7
     Client IPv6 Prefix:                   2001:bd8:1111:2222::/64
     Client DUID:                         LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

     State:                                BOUND(bound)
     Lease Expires:                        2009-07-21 10:41:15 PDT
     Lease Expires in:                     86308 seconds
     Lease Start:                          2009-07-20 10:41:15 PDT
     Incoming Client Interface:            ge-1/0/0.0
     Server Ip Address:                    0.0.0.0
     Server Interface:                     none
     Client Id Length:                     14
     Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002
```

### show dhcpv6 server binding interface

```
user@host> show dhcp6 server binding interface ge-1/0/0:10-101
Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:bd8:1111:2222::/64 1           86055    BOUND    ge-1/0/0.100
LL_TIME0x1-0x4b0a53b9-00:10:94:00:00:01
```

### show dhcpv6 server binding interface detail

```
user@host> show dhcp6 server binding interface ge-1/0/0:10-101 detail
Session Id:  7
     Client IPv6 Prefix:                   2001:bd8:1111:2222::/64
```

Copyright © 2013, Juniper Networks, Inc.

```
    Client DUID:                          LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

    State:                                  BOUND(bound)
    Lease Expires:                          2009-07-21 10:41:15 PDT
    Lease Expires in:                       86136 seconds
    Lease Start:                            2009-07-20 10:41:15 PDT
    Incoming Client Interface:              ge-1/0/0.0
    Server Ip Address:                      0.0.0.0
    Server Interface:                       none
    Client Id Length:                       14
    Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002
```

### show dhcpv6 server binding prefix

```
user@host> show dhcp6 server binding 14/0x00010001/0x02b3be8f/0x00109400/0x0005
detail
Session Id:  7
    Client IPv6 Prefix:                   2001:bd8:1111:2222::/64
    Client DUID:                          LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

    State:                                  BOUND(bound)
    Lease Expires:                          2009-07-21 10:41:15 PDT
    Lease Expires in:                       86136 seconds
    Lease Start:                            2009-07-20 10:41:15 PDT
    Incoming Client Interface:              ge-1/0/0.0
    Server Ip Address:                      0.0.0.0
    Server Interface:                       none
    Client Id Length:                       14
    Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002
```

### show dhcpv6 server binding session-id

```
user@host> show dhcpv6 server binding 8
Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:bd8:1111:2222::/64 8           86235    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
```

### show dhcpv6 server binding summary

```
user@host> show dhcpv6 server binding summary

5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)
```


Copyright © 2013, Juniper Networks, Inc.

## show dhcpv6 server statistics (View)

**Syntax**

**show dhcpv6 server statistics**
<**logical-system** *logical-system-name*>
<**routing-instance** *routing-instance-name*>

**Release Information**

Command introduced in Release 10.4 of Junos OS.

**Description**

Display DHCPv6 local server statistics.

**Options**

**logical-system** *logical-system-name*—(Optional) Display information about extended DHCPv6 local server statistics on the specified logical system. If you do not specify a logical system, statistics are displayed for the default logical system.

**routing-instance** *routing-instance-name*—(Optional) Display information about DHCPv6 local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.

**Required Privilege Level**

view

**Related Documentation**

- clear dhcpv6 server statistics (Local Server) on page 1372
- Device Configuration

**List of Sample Output**

show dhcpv6 server statistics on page 1647

**Output Fields**

Table 38 on page 1646 lists the output fields for the **show dhcpv6 server statistics** command. Output fields are listed in the approximate order in which they appear.

Copyright © 2013, Juniper Networks, Inc.

### Table 38: show dhcpv6 server statistics Output Fields

| Field Name | Field Description |
|---|---|
| **Dhcpv6 Packets dropped** | Number of packets discarded by the DHCPv6 local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.<br>• **Total**—Total number of packets discarded by the DHCPv6 local server<br>• **Strict Reconfigure**—Number of solicit messages discarded because the client does not support reconfiguration<br>• **Bad hardware address**—Number of packets discarded because an invalid hardware address was specified<br>• **Bad opcode**—Number of packets discarded because an invalid operation code was specified<br>• **Bad options**—Number of packets discarded because invalid options were specified<br>• **Invalid server address**—Number of packets discarded because an invalid server address was specified<br>• **No available addresses**—Number of packets discarded because there were no addresses available for assignment<br>• **No interface match**—Number of packets discarded because they did not belong to a configured interface<br>• **No routing instance match**—Number of packets discarded because they did not belong to a configured routing instance<br>• **No valid local address**—Number of packets discarded because there was no valid local address<br>• **Packet too short**—Number of packets discarded because they were too short<br>• **Read error**—Number of packets discarded because of a system read error<br>• **Send error**—Number of packets that the DHCPv6 local server could not send |
| **Messages received** | Number of DHCPv6 messages received.<br>• **DHCPV6_CONFIRM**—Number of DHCPv6 CONFIRM PDUs received.<br>• **DHCPV6_DECLINE**—Number of DHCPv6 DECLINE PDUs received.<br>• **DHCPV6_INFORMATION_REQUEST**—Number of DHCPv6 INFORMATION-REQUEST PDUs received.<br>• **DHCPV6_REBIND**—Number of DHCPv6 REBIND PDUs received.<br>• **DHCPV6_RELAY_FORW**—Number of DHCPv6 RELAY-FORW PDUs received from a relay by the DHCPv6 server.<br>• **DHCPV6_RELEASE**—Number of DHCPv6 RELEASE PDUs received.<br>• **DHCPV6_RENEW**—Number of DHCPv6 RENEW PDUs received.<br>• **DHCPV6_REQUEST**—Number of DHCPv6 REQUEST PDUs received.<br>• **DHCPV6_SOLICIT**—Number of DHCPv6 SOLICIT PDUs received. |
| **Messages sent** | Number of DHCPv6 messages sent.<br>• **DHCPV6_ADVERTISE**—Number of DHCPv6 ADVERTISE PDUs transmitted.<br>• **DHCPV6_REPLY**—Number of DHCPv6 ADVERTISE PDUs transmitted.<br>• **DHC6_RECONFIGURE**—Number of DHCPv6 RECONFIGURE PDUs transmitted.<br>• **DHCPV6_RELAY_REPL**—Number of DHCPv6 RELAY-REPL PDUs sent from DHCPv6 server to DHCPv6 relay. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show dhcpv6 server statistics

```
user@host> show dhcpv6 server statistics
Dhcpv6 Packets dropped:
    Total               0

Messages received:
    DHCPV6_DECLINE             0
    DHCPV6_SOLICIT             9
    DHCPV6_INFORMATION_REQUEST 0
    DHCPV6_RELEASE             0
    DHCPV6_REQUEST             5
    DHCPV6_CONFIRM             0
    DHCPV6_RENEW               0
    DHCPV6_REBIND              0
    DHCPV6_RELAY_FORW          0
   Messages sent:
    DHCPV6_ADVERTISE           9
    DHCPV6_REPLY               5
    DHCPV6_RECONFIGURE         0
    DHCPV6_RELAY_REPL          0
```

Copyright © 2013, Juniper Networks, Inc.

## show ethernet-switching mac-learning-log (View)

**Syntax** **show ethernet-switching mac-learning-log**

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** Displays the event log of learned MAC addresses.

**Required Privilege Level** view

**Output Fields** lists the output fields for the show ethernet-switching mac-learning-log command. Output fields are listed in the approximate order in which they appear.

### Table 39: show interfaces Output Fields

| Field Name | Field Description |
|---|---|
| **Date and Time** | Timestamp when the MAC address was added or deleted from the log. |
| **VLAN-IDX** | VLAN index. An internal value assigned by Junos OS for each VLAN. |
| **MAC** | Learned MAC address. |
| **Deleted \| Added** | MAC address deleted or added to the MAC learning log. |
| **Blocking** | The forwarding state of the interface:<br>• blocked—Traffic is not being forwarded on the interface.<br>• unblocked—Traffic is forwarded on the interface. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show ethernet-switching mac-learning-log

```
user@host> show ethernet-switching mac-learning-log
Wed Mar 18 08:07:05 2009
vlan_idx 7 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 9 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 10 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 11 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 12 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 13 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 14 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 15 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 16 mac 00:00:00:00:00:00 was deleted
Wed Mar 18 08:07:05 2009
vlan_idx 4 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 6 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 7 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 9 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 10 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 11 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 12 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 13 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 14 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 15 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 16 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 5 mac 00:00:00:00:00:00 was added
Wed Mar 18 08:07:05 2009
vlan_idx 18 mac 00:00:05:00:00:05 was learned
Wed Mar 18 08:07:05 2009
vlan_idx 5 mac 00:30:48:90:54:89 was learned
Wed Mar 18 08:07:05 2009
vlan_idx 6 mac 00:00:5e:00:01:00 was learned
Wed Mar 18 08:07:05 2009
vlan_idx 16 mac 00:00:5e:00:01:08 was learned
Wed Mar 18 08:07:05 2009
vlan_idx 7 mac 00:00:5e:00:01:09 was learned
Wed Mar 18 08:07:05 2009
vlan_idx 8 mac 00:19:e2:50:ac:00 was learned
Wed Mar 18 08:07:05 2009
vlan_idx 12 mac 00:00:5e:00:01:04 was learned
[output truncated]
```

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

## show ethernet-switching table (View)

**Syntax** **show ethernet-switching table**
**<brief | detail | extensive >**
**interface *interface-name* >**

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** Displays the Ethernet switching table.

**Options**
- **none**—(Optional) Display brief information about the Ethernet-switching table.
- **brief | detail | extensive**—(Optional) Display the specified level of output.
- **interface-name**—(Optional) Display the Ethernet-switching table for a specific interface.

**Required Privilege Level** view

**Output Fields** lists the output fields for the show ethernet-switching table command. Output fields are listed in the approximate order in which they appear.

### Table 40: show ethernet-switching table Output Fields

| Field Name | Field Description |
|---|---|
| **VLAN** | The name of a VLAN. |
| **MAC address** | The MAC address associated with the VLAN. |
| **Type** | The type of MAC address. Values are:<br>• static—The MAC address is manually created.<br>• learn—The MAC address is learned dynamically from a packet's source MAC address.<br>• flood—The MAC address is unknown and flooded to all members. |
| **Age** | The time remaining before the entry ages out and is removed from the Ethernet switching table. |
| **Interfaces** | Interface associated with learned MAC addresses or All-members (flood entry). |
| **Learned** | For learned entries, the time which the entry was added to the Ethernet-switching table. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show ethernet-switching table

```
user@host> show ethernet-switching table
Ethernet-switching table: 57 entries, 17 learned
VLAN MAC address Type Age Interfaces
F2 * Flood - All-members
F2 00:00:05:00:00:03 Learn 0 ge-0/0/44.0
F2 00:19:e2:50:7d:e0 Static - Router
Linux * Flood - All-members
Linux 00:19:e2:50:7d:e0 Static - Router
Linux 00:30:48:90:54:89 Learn 0 ge-0/0/47.0
T1 * Flood - All-members
T1 00:00:05:00:00:01 Learn 0 ge-0/0/46.0
T1 00:00:5e:00:01:00 Static - Router
T1 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
T1 00:19:e2:50:7d:e0 Static - Router
T10 * Flood - All-members
T10 00:00:5e:00:01:09 Static - Router
T10 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
T10 00:19:e2:50:7d:e0 Static - Router
T111 * Flood - All-members
T111 00:19:e2:50:63:e0 Learn 0 ge-0/0/15.0
T111 00:19:e2:50:7d:e0 Static - Router
T111 00:19:e2:50:ac:00 Learn 0 ge-0/0/15.0
T2 * Flood - All-members
T2 00:00:5e:00:01:01 Static - Router
T2 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
T2 00:19:e2:50:7d:e0 Static - Router
T3 * Flood - All-members
T3 00:00:5e:00:01:02 Static - Router
T3 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
T3 00:19:e2:50:7d:e0 Static - Router
T4 * Flood - All-members
T4 00:00:5e:00:01:03 Static - Router
T4 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
[output truncated]
```

## Sample Output

show ethernet-switching table brief

```
user@host> show ethernet-switching table brief
Ethernet-switching table: 57 entries, 17 learned
VLAN MAC address Type Age Interfaces
F2 * Flood - All-members
F2 00:00:05:00:00:03 Learn 0 ge-0/0/44.0
F2 00:19:e2:50:7d:e0 Static - Router
Linux * Flood - All-members
Linux 00:19:e2:50:7d:e0 Static - Router
Linux 00:30:48:90:54:89 Learn 0 ge-0/0/47.0
T1 * Flood - All-members
T1 00:00:05:00:00:01 Learn 0 ge-0/0/46.0
T1 00:00:5e:00:01:00 Static - Router
T1 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
T1 00:19:e2:50:7d:e0 Static - Router
T10 * Flood - All-members
T10 00:00:5e:00:01:09 Static - Router
T10 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
T10 00:19:e2:50:7d:e0 Static - Router
T111 * Flood - All-members
T111 00:19:e2:50:63:e0 Learn 0 ge-0/0/15.0
```


Copyright © 2013, Juniper Networks, Inc.

```
T111 00:19:e2:50:7d:e0 Static - Router
T111 00:19:e2:50:ac:00 Learn 0 ge-0/0/15.0
T2 * Flood - All-members
T2 00:00:5e:00:01:01 Static - Router
T2 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
T2 00:19:e2:50:7d:e0 Static - Router
T3 * Flood - All-members
T3 00:00:5e:00:01:02 Static - Router
T3 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
T3 00:19:e2:50:7d:e0 Static - Router
T4 * Flood - All-members
T4 00:00:5e:00:01:03 Static - Router
T4 00:19:e2:50:63:e0 Learn 0 ge-0/0/46.0
[output truncated]
```

## Sample Output

### show ethernet-switching table detail

```
user@host> show ethernet-switching table detail
Ethernet-switching table: 57 entries, 17 learned
F2, *
Interface(s): ge-0/0/44.0
Type: Flood
F2, 00:00:05:00:00:03
Interface(s): ge-0/0/44.0
Type: Learn, Age: 0, Learned: 2:03:09
F2, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
Linux, *
Interface(s): ge-0/0/47.0
Type: Flood
Linux, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
Linux, 00:30:48:90:54:89
Interface(s): ge-0/0/47.0
Type: Learn, Age: 0, Learned: 2:03:08
T1, *
Interface(s): ge-0/0/46.0
Type: Flood
T1, 00:00:05:00:00:01
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:07
T1, 00:00:5e:00:01:00
Interface(s): Router
Type: Static
T1, 00:19:e2:50:63:e0
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:07
T1, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
T10, *
Interface(s): ge-0/0/46.0
Type: Flood
T10, 00:00:5e:00:01:09
Interface(s): Router
Type: Static
T10, 00:19:e2:50:63:e0
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:08
```

Copyright © 2013, Juniper Networks, Inc.

```
T10, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
T111, *
Interface(s): ge-0/0/15.0
Type: Flood
[output truncated]
```

## Sample Output

### show ethernet-switching table extensive

```
user@host> show ethernet-switching table extensive
Ethernet-switching table: 57 entries, 17 learned
F2, *
Interface(s): ge-0/0/44.0
Type: Flood
F2, 00:00:05:00:00:03
Interface(s): ge-0/0/44.0
Type: Learn, Age: 0, Learned: 2:03:09
F2, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
Linux, *
Interface(s): ge-0/0/47.0
Type: Flood
Linux, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
Linux, 00:30:48:90:54:89
Interface(s): ge-0/0/47.0
Type: Learn, Age: 0, Learned: 2:03:08
T1, *
Interface(s): ge-0/0/46.0
Type: Flood
T1, 00:00:05:00:00:01
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:07
T1, 00:00:5e:00:01:00
Interface(s): Router
Type: Static
T1, 00:19:e2:50:63:e0
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:07
T1, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
T10, *
Interface(s): ge-0/0/46.0
Type: Flood
T10, 00:00:5e:00:01:09
Interface(s): Router
Type: Static
T10, 00:19:e2:50:63:e0
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:08
T10, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
T111, *
Interface(s): ge-0/0/15.0
Type: Flood
[output truncated]
```


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show ethernet-switching table interface ge-0/0/1

```
user@host> show ethernet-switching table interface ge-0/0/1
Ethernet-switching table: 1 unicast entries
VLAN     MAC address         Type     Age Interfaces
V1       *                   Flood    - All-members
V1       00:00:05:00:00:05   Learn    0 ge-0/0/1.0
```

## show firewall (View)

**Syntax**

**show firewall**
**<filter *filter-name*>**
**<counter *counter-name*>**
**<log>**
**<prefix-action-stats>**
**<terse>**

**Release Information**

Command introduced before Release 10.0 of Junos OS.

**Description**

Display statistics about configured firewall filters.

**Options**

**none**—Display statistics about configured firewall filters.

**filter *filter-name***—Name of a configured filter.

**counter *counter-name***—Name of a filter counter.

**log**—Display log entries for firewall filters.

**prefix-action-stats**—Display prefix action statistics for firewall filters.

**terse**—Display firewall filter names only.

**Required Privilege Level**

view

**Related Documentation**

- clear firewall on page 1374
- Device Configuration

**List of Sample Output**

show firewall on page 1657

**Output Fields**

Table 41 on page 1656 lists the output fields for the **show firewall** command. Output fields are listed in the approximate order in which they appear.

### Table 41: show firewall Output Fields

| Field Name | Field Description |
|---|---|
| **Filter** | Name of a filter that has been configured with the **filter** statement at the **[edit firewall]** hierarchy level.<br><br>When an interface-specific filter is displayed, the name of the filter is followed by the full interface name and by either **-i** for an input filter or **-o** for an output filter.<br><br>When dynamic filters are displayed, the name of the filter is followed by the full interface name and by either **-in** for an input filter or **-out** for an output filter. When a logical system–specific filter is displayed, the name of the filter is prefixed with two underscore (__) characters and the name of the logical system (for example, **__ls1/filter1**). |


Copyright © 2013, Juniper Networks, Inc.

Table 41: show firewall Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Counters** | Display filter counter information:<br>• **Name**—Name of a filter counter that has been configured with the **counter** firewall filter action.<br>• **Bytes**—Number of bytes that match the filter term under which the **counter** action is specified.<br>• **Packets**—Number of packets that matched the filter term under which the **counter** action is specified. |
| **Policers** | Display policer information:<br>• **Name**—Name of policer.<br>• **Bytes**—Number of bytes that match the filter term under which the policer action is specified. This is only the number out-of-specification (out-of-spec) byte counts, not all the bytes in all packets policed by the policer.<br>• **Packets**—Number of packets that matched the filter term under which the policer action is specified. This is only the number of out-of-specification (out-of-spec) packet counts, not all packets policed by the policer. |

## Sample Output

### show firewall

```
user@host> show firewall
Filter: ef_path
Counters:
Name                                            Bytes              Packets
def-count                                       0                    0
video-count                                     0                    0
voice-count                                     0                    0

Filter: __default_bpdu_filter__

Filter: deep
Counters:
Name                                            Bytes              Packets
deep2                                           302076               5031

Filter: deep-flood
Counters:
Name                                            Bytes              Packets
deep_flood_def                                  302136               5032
deep1                                           0                    0
Policers:
Name                                                        Packets
deep-pol-op-first                                             0
```

## show gtp tunnels

**Syntax** **show security gprs gtp tunnels <brief | summary>**

**Release Information** Command introduced in Release 10.0 of Junos OS. Support for GTPv2 added in Release 11.4 of Junos OS.

**Description** Display all existing GTP tunnels.

**Options**
- brief—Display a short listing of all GTP tunnels.
- summary—Display a summary of all GTP tunnels.

**Required Privilege Level** view

**Related Documentation**
- General Packet Radio Service for Security Devices

**List of Sample Output**
show security gprs gtp tunnels on page 1658
show security gprs gtp tunnels summary on page 1658

### Sample Output

show security gprs gtp tunnels

```
user@host> show security gprs gtp tunnels

FPC 7 PIC 0:

 Index: 72000002, EBI/LBI: 5/5(V2)to sgw, Timeout: 1440m
 User: 61.0.0.102, 12345678 --> 62.0.0.102, 00000021
 Control: 61.0.0.101, 00325ac1 --> 62.0.0.101, 00000001

 FPC 8 PIC 0:
 Index: 81000001, Tunnel ID: 0x0000000000000011(V0), Timeout: 1440m
 User: 54.0.0.101 --> 55.0.0.101
 Control: 54.0.0.101 --> 55.0.0.101

 Index: 81000002, NSAPI: 5(V1), Timeout: 1440m
 User: 54.0.0.101, 00000011 --> 55.0.0.101, 00000011
 Control: 54.0.0.100, 00000011 --> 55.0.0.100, 00000011

 3 tunnels active in total
```

show security gprs gtp tunnels summary

```
user@host> show security gprs gtp tunnels summary

FPC 1 PIC 0:

FPC 1 PIC 1:

FPC 2 PIC 0:

FPC 2 PIC 1:

2 tunnels active in total
```


Copyright © 2013, Juniper Networks, Inc.

## show security gprs gtp counters

**Syntax** show security gprs gtp counters <*all* | *error* | *ha* | *message* <*message-name*> | *packet* | *request* | *tunnel*>

**Release Information** Command introduced in Junos OS Release 12.1X44-D2.

**Description** Display counters that can be used to indicate the number of GTP tunnel counters (Allocated and Freed), GTP packet counters (Received, Passed, and Dropped), Brief message counters (Receive, Forward, and Drop), Error counters, Request counters, and HA counters.

**Options**

- **all**—Show all GTP counters.
- **error**—Show GTP error counters.
- **ha**—Show GTP HA counters.
- **message** ***message-name***—Show GTP message counters.
- **packet**—Show GTP packet counters.
- **request**—Show GTP request counters.
- **tunnel**—Show GTP tunnel counters.

**Required Privilege Level** view

**Related Documentation**

- General Packet Radio Service for Security Devices
- clear security gprs gtp counters on page 1428

**List of Sample Output**

show security gprs gtp counters all on page 1661
show security gprs gtp counters error on page 1663
show security gprs gtp counters ha on page 1664
show security gprs gtp counters message v0-create-aa-pdp-req on page 1664
show security gprs gtp counters packet on page 1664
show security gprs gtp counters request on page 1664
show security gprs gtp counters tunnel on page 1664

**Output Fields** Lists the output fields for the **show security gprs gtp counters** command.

Table 42: show security gprs gtp counters all Output Fields

| Field Name | Field Description |
|---|---|
| **Tunnel counters** | Tunnel counters are used to track the number of tunnels that are created on the device.<br>There are two entries:<br>• Allocated<br>• Freed<br>Active tunnel number = Number of Allocated counters - Number of Freed counters |

Copyright © 2013, Juniper Networks, Inc.

Table 42: show security gprs gtp counters all Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Packet counters** | Packet counters indicate the number of GTP packets that are received and processed on the device.<br><br>There are three entries:<br><br>• Received – Number of GTP packet messages received.<br>• Passed – Number of GTP packet messages passed.<br>• Dropped – Number of GTP packet messages dropped because of an error.<br><br>Number of Received counters = Number of Dropped counters + Number of Passed counters |
| **Brief message counters** | GTP messages counters indicate the number of GTP messages that are received and processed on the device.<br><br>There are three entries:<br><br>• Receive – Number of GTP messages received.<br>• Forward – Number of GTP messages forwarded.<br>• Drop – Number of GTP messages dropped because of an error.<br><br>Number of Received counters = Number of Dropped counters + Number of Forward counters |
| **Error counters** | Drop reason and drop counters indicate the number of GTP packets that are dropped as a result of an error.<br><br>Total error = Sum of all the following errors (see Sample Output) |
| **Request counters** | Request counters indicate the number of GTP request messages that are received and processed on the device. This information can be used for debugging purpose. |
| **HA counters** | HA counters indicate the number of messages that are received or sent by the device. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security gprs gtp counters all

```
user@host> show security gprs gtp counters all

 Tunnel counters:
                 Total      GTPv0    GTPv1-c    GTPv1-u    GTPv2-c    GTPv2-u
  Allocated          0          0          0          0          0          0
  Freed              0          0          0          0          0          0

Packet counters:
                 Total      GTPv0      GTPv1      GTPv2       GTP'
  Received           0          0          0          0          0
  Passed             0          0          0          0          0
  Dropped            0          0          0          0          0

Brief message counters:
                                 Receive    Forward       Drop
GTPv0
  Create PDP Request                   0          0          0
  Create PDP Response                  0          0          0
  Update PDP Request                   0          0          0
  Update PDP Response                  0          0          0
  Delete PDP Request                   0          0          0
  Delete PDP Response                  0          0          0
  Create AA PDP Request                0          0          0
  Create AA PDP Response               0          0          0
  Delete AA PDP Request                0          0          0
  Delete AA PDP Response               0          0          0
  Others                               0          0          0
GTPv1
  Create PDP Request                   0          0          0
  Create PDP Response                  0          0          0
  Update PDP Request                   0          0          0
  Update PDP Response                  0          0          0
  Delete PDP Request                   0          0          0
  Delete PDP Response                  0          0          0
  Others                               0          0          0
GTPv2
  Create Session Request               0          0          0
  Create Session Response              0          0          0
  Delete Session Request               0          0          0
  Delete Session Response              0          0          0
  Create Bearer Request                0          0          0
  Create Bearer Response               0          0          0
  Modify Bearer Request                0          0          0
  Modify Bearer Response               0          0          0
  Delete Bearer Request                0          0          0
  Delete Bearer Response               0          0          0
  Others                               0          0          0

Error counters:
        Total error             : 0
        Exception               : 0
        Gate failed             : 0
        Invalid header          : 0
        Message length          : 0
        Zero IMSI               : 0
        Zero charge ID          : 0
        Sequence                : 0
```

Copyright © 2013, Juniper Networks, Inc.

```
        APN filter             : 0
        Port not match         : 0
        GTP-in-GTP             : 0
        Message too short      : 0
        Message too long       : 0
        GSN not exist          : 0
        Over GSN rate limit    : 0
        Request not found      : 0
        Retransmit response    : 0
        Missing IE             : 0
        Unexpected IE          : 0
        Unknown IE type        : 0
        IE order               : 0
        IE length              : 0
        Duplicate IE           : 0
        Non-digit TID/TEID     : 0
        Non-zero TID/TEID      : 0
        Zero TID/TEID          : 0
        Control TID/TEID       : 0
        Data TID/TEID          : 0
        Control GSN IE         : 0
        Data GSN IE            : 0
        End user IE            : 0
        GGSN IP for handover   : 0
        Disallowed v0 message  : 0
        Disallowed v1 message  : 0
        Disallowed v2 message  : 0
        Invalid message type   : 0
        No tunnel0             : 0
        No control tunnel      : 0
        No user tunnel         : 0
        Invalid tunnel0        : 0
        Invalid control tunnel : 0
        Invalid user tunnel    : 0
        Create tunnel0         : 0
        Create control tunnel  : 0
        Create user tunnel     : 0
        No request             : 0
        Out of request         : 0
        No action              : 0
        Out of action          : 0
        GTPv2 TEID not exist   : 0
        GTPv2 Missing TEID     : 0
        GTPv2 Non-zero EBI     : 0
        GTPv2 EBI not found    : 0
        GTPv2 IE context       : 0

HA counters:
        Total message received              : 0
        Message received success            : 0
        Bad message received                : 0
        Unknown message type received       : 0
        Unknown message version received    : 0
        Total message send                  : 0
        Message send success                : 0
        Message send failed                 : 0
        Memory allocate failed              : 0

Request counters:
        Request allocated           : 0
        Request freed               : 0
```


Copyright © 2013, Juniper Networks, Inc.

```
                Request activated           : 0
                Request died                : 0
                Request action allocated    : 0
                Request action freed        : 0
```

### show security gprs gtp counters error

```
user@host> show security gprs gtp counters error
Error counters:
                Total error             : 0
                Exception               : 0
                Gate failed             : 0
                Invalid header          : 0
                Message length          : 0
                Zero IMSI               : 0
                Zero charge ID          : 0
                Sequence                : 0
                APN filter              : 0
                Port not match          : 0
                GTP-in-GTP              : 0
                Message too short       : 0
                Message too long        : 0
                GSN not exist           : 0
                Over GSN rate limit     : 0
                Request not found       : 0
                Retransmit response     : 0
                Missing IE              : 0
                Unexpected IE           : 0
                Unknown IE type         : 0
                IE order                : 0
                IE length               : 0
                Duplicate IE            : 0
                Non-digit TID/TEID      : 0
                Non-zero TID/TEID       : 0
                Zero TID/TEID           : 0
                Control TID/TEID        : 0
                Data TID/TEID           : 0
                Control GSN IE          : 0
                Data GSN IE             : 0
                End user IE             : 0
                GGSN IP for handover    : 0
                Disallowed v0 message   : 0
                Disallowed v1 message   : 0
                Disallowed v2 message   : 0
                Invalid message type    : 0
                No tunnel0              : 0
                No control tunnel       : 0
                No user tunnel          : 0
                Invalid tunnel0         : 0
                Invalid control tunnel  : 0
                Invalid user tunnel     : 0
                Create tunnel0          : 0
                Create control tunnel   : 0
                Create user tunnel      : 0
                No request              : 0
                Out of request          : 0
                No action               : 0
                Out of action           : 0
                GTPv2 TEID not exist    : 0
                GTPv2 Missing TEID      : 0
                GTPv2 Non-zero EBI      : 0
                GTPv2 EBI not found     : 0
                GTPv2 IE context        : 0
```

Copyright © 2013, Juniper Networks, Inc.

### show security gprs gtp counters ha

```
user@host> show security gprs gtp counters ha
HA counters:
        Total message received              : 0
        Message received success            : 0
        Bad message received                : 0
        Unknown message type received       : 0
        Unknown message version received    : 0
        Total message send                  : 0
        Message send success                : 0
        Message send failed                 : 0
        Memory allocate failed              : 0
```

### show security gprs gtp counters message v0-create-aa-pdp-req

```
user@host> show security gprs gtp counters message v0-create-aa-pdp-req
Message counters:
  Received              0
  Forwarded             0
  Dropped               0
```

### show security gprs gtp counters packet

```
user@host> show security gprs gtp counters packet
Packet counters:
                 Total      GTPv0      GTPv1      GTPv2       GTP'
  Received           0          0          0          0          0
  Passed             0          0          0          0          0
  Dropped            0          0          0          0          0
```

### show security gprs gtp counters request

```
user@host> show security gprs gtp counters request

Request counters:
        Request allocated           : 0
        Request freed               : 0
        Request activated           : 0
        Request died                : 0
        Request action allocated    : 0
        Request action freed        : 0
```

### show security gprs gtp counters tunnel

```
user@host> show security gprs gtp counters tunnel
Tunnel counters:
                 Total      GTPv0    GTPv1-c    GTPv1-u    GTPv2-c    GTPv2-u
  Allocated          0          0          0          0          0          0
  Freed              0          0          0          0          0          0
```


Copyright © 2013, Juniper Networks, Inc.

## show igmp-snooping route (View)

**Syntax** <**brief** | **detail**>
<**ethernet-switching** <**brief** | **detail** | **vlan** (*vlan-id* | *vlan-name* ) >>
<**inet** <**brief** | **detail** |**vlan** ( **vlan-id** |*vlan-name* )>>
<**vlan** ( **vlan-id** | *vlan-name* )>>

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** Display IGMP snooping route information.

**Options**
- **none**—Display general parameters.
- **brief** | **detail**—(Optional) Display the specified level of output.
- **ethernet-switching**—(Optional) Display Ethernet switching information.
- **inet**—(Optional) Display inet information.
- **vlan** *vlan-id* |*vlan-name*—(Optional) Display route information for the specified VLAN.

**Required Privilege Level** view

**Output Fields** lists the output fields for the **show igmp-snooping route** command. Output fields are listed in the approximate order in which they appear.

Table 43: show igmp-snooping route Output Fields

| Field Name | Field Description |
|---|---|
| **VLAN** | Name of the VLAN. |
| **Group** | Multicast group address. |
| **Next-hop** | ID associated with the next-hop device. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show igmp-snooping route

```
user@host> show igmp-snooping route
VLAN       Group          Next-hop
v11         224.1.1.1, *   533
Interfaces: ge-0/0/13.0, ge-0/0/1.0
v12         224.1.1.3, *   534
Interfaces: ge-0/0/13.0, ge-0/0/0.0
```

### show igmp-snooping route vlan v1

```
user@host> show igmp-snooping route vlan v1
Table: 0
VLAN      Group              Next-hop
v1        224.1.1.1, *       1266
Interfaces: ge-0/0/0.0
v1        224.1.1.3, *       1266
Interfaces: ge-0/0/0.0
v1        224.1.1.5, *       1266
Interfaces: ge-0/0/0.0
v1        224.1.1.7, *       1266
Interfaces: ge-0/0/0.0
v1        224.1.1.9, *       1266
Interfaces: ge-0/0/0.0
v1        224.1.1.11, *      1266
Interfaces: ge-0/0/0.0
```


Copyright © 2013, Juniper Networks, Inc.

## show igmp-snooping vlans (View)

**Syntax** **show igmp-snooping vlans**
<**brief** | **detail** >
<vlan *vlan-id* | *vlan-name* >

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** Display IGMP snooping VLAN information.

**Options**
- **none**—Display general parameters.
- **brief** | **detail**—(Optional) Display the specified level of output.
- **vlan** *vlan-id* | *vlan-name* —(Optional) Display VLAN information for the specified VLAN.

**Required Privilege Level** view

**Output Fields** lists the output fields for the **show igmp-snooping vlans** command. Output fields are listed in the approximate order in which they appear.

### Table 44: show igmp-snooping vlans

| Field Name | Field Description |
|---|---|
| **VLAN** | Name of the VLAN. |
| **Interfaces** | Number of interfaces in the VLAN. |
| **Groups** | Number of groups in the VLAN. |
| **MRouters** | Number of multicast routers associated with the VLAN. |
| **Receivers** | Number of host receivers in the VLAN. |
| **Tag** | Numerical identifier of the VLAN. |
| **vlan-interface** | Internal VLAN interface identifier. |
| **Membership timeout** | Membership timeout value. |
| **Querier timeout** | Timeout value for interfaces dynamically marked as router interfaces (interfaces that receive queries). When the querier timeout is reached, the switch marks the interface as a host interface. |
| **Interface** | Name of the interface. |
| **Reporters** | Number of dynamic groups on an interface. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show igmp-snooping vlans

```
user@host> show igmp-snooping vlans
VLAN  Interfaces  Groups  MRouters  Receivers
default  0           0       0         0
v1       11          50      0         0
v10      1           0       0         0
v11      1           0       0         0
v180     3           0       1         0
v181     3           0       0         0
v182     3           0       0         0
```

## Sample Output

### show igmp-snooping vlans vlan v10

```
user@host> show igmp-snooping vlans vlan v10
VLAN    Interfaces   Groups  MRouters   Receivers
v10     1            0       0          0
```

## Sample Output

### show igmp-snooping vlans vlan v10 detail

```
user@host> sshow igmp-snooping vlans vlan v10 detail
VLAN: v10, Tag: 10, vlan-interface: vlan.10
Membership timeout: 260, Querier timeout: 255
Interface: ge-0/0/10.0, tagged, Groups: 0, Reporters: 0
```


Copyright © 2013, Juniper Networks, Inc.

## show interfaces (View J Series and SRX Series)

**Syntax**

**show interfaces**
< ***interface-name*** >
<**extensive | terse**>

**Release Information**

Command modified in Release 9.5 of Junos OS.

**Description**

Display status information and statistics about interfaces on J Series and SRX Series devices running Junos OS.

On SRX Series devices, on configuring identical IPs on a single interface, you will not see a warning message; instead, you will see a syslog message.

**Options**

- ***interface-name*** —(Optional) Display standard information about the specified interface. Following is a list of typical interface names. Replace pim with the PIM slot and port with the port number. For a complete list, see the Layer 2 Bridging and Switching for Security Devices.
  - **at-** ***pim*****/0/*****port***—ATM-over-ADSL or ATM-over-SHDSL interface.
  - **br-*****pim*****/0/*****port***—Basic Rate Interface for establishing ISDN connections.
  - **ce1-*****pim*****/0/ *****port***—Channelized E1 interface.
  - **cl-0/0/8**—3G wireless modem interface for SRX210 devices.
  - **ct1-*****pim*****/0/*****port***—Channelized T1 interface.
  - **dl0**—Dialer Interface for initiating ISDN and USB modem connections.
  - **e1-*****pim*****/0/*****port***—E1 interface.
  - **e3-*****pim*****/0/*****port***—E3 interface.
  - **fe-*****pim*****/0/*****port***—Fast Ethernet interface.
  - **ge-*****pim*****/0/*****port***—Gigabit Ethernet interface.
  - **se-*****pim*****/0/*****port***—Serial interface.
  - **t1-*****pim*****/0/*****port***—T1 (also called DS1) interface.
  - **t3-*****pim*****/0/*****port***—T3 (also called DS3) interface.
  - **wx-*****slot*****/0/0**—WAN acceleration interface, for the WXC Integrated Services Module (ISM 200).
- **extensive | terse**—(Optional) Display the specified level of output.

**Required Privilege Level**

view

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices

Copyright © 2013, Juniper Networks, Inc.

- Layer 2 Bridging and Switching for Security Devices
- Junos OS Operational Mode Commands
- Interfaces for Security Devices
- Device and Routing Operations Monitoring

**List of Sample Output**

show interfaces Gigabit Ethernet on page 1671
show interfaces extensive (Gigabit Ethernet) on page 1671
show interfaces terse on page 1672
show interfaces extensive (WAN Acceleration) on page 1673
show interfaces extensive (3G Wireless Modem) on page 1674

**Output Fields**

Table 45 on page 1670 lists the output fields for the **show interfaces** command. Output fields are listed in the approximate order in which they appear.

### Table 45: show interfaces Output Fields

| Field Name | Field Description |
|---|---|
| **Allowed host inbound traffic** | The allowed traffic through the interface. |
| **Traffic statistics** | Number of packets and bytes transmitted and received on the physical interface. |
| **Local statistics** | Number of packets and bytes transmitted and received on the physical interface. |
| **Transit statistics** | Number of packets and bytes transiting the physical interface. |
| **Flow input statistics** | Statistics on packets received by flow module. |
| **Flow output statistics** | Statistics on packets sent by flow module. |
| **Flow error statistics** | Statistics on errors in the flow module. |
| **Admin** | The interface is enabled (up) or disabled (down). |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show interfaces Gigabit Ethernet

```
user@host> show interfaces ge-0/0/1.0
Logical interface ge-0/0/1.0 (Index 67) (SNMP ifIndex 36)
      Flags: Device-Down SNMP-Traps Encapsulation: ENET2
      Protocol inet, MTU: 1500
        Flags: None
        Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
          Destination: 4.4.4/24, Local: 4.4.4.254, Broadcast: 4.4.4.255
     Security: Zone: Untrust, ident-reset: on
Allowed host-inbound traffic: bfd bgp bootp dhcp dvmrp finger ftp
                                    http https ike ident-reset igmp ldp mld
                                    msdp netconf ospf ospf3 pgm pim ping rip
                                    ripng rlogin router-discovery rpm rsh
                                    rsvp sap snmp snmp-trap ssh telnet
                                    traceroute vrrp xnm-clear xnm-sslshow
  interfaces <interface-name> extensive
```

## Sample Output

show interfaces extensive (Gigabit Ethernet)

```
user@host> show interfaces ge-0/0/1.0 extensive
      Logical interface ge-0/0/1.0 (Index 67) (SNMP ifIndex 37) (Generation 134)

        Flags: SNMP-Traps VLAN-Tag [ 0x8100.100 ]  Encapsulation: ENET2
        Traffic statistics:
         Input  bytes  :                   0
         Output bytes  :                   0
         Input  packets:                   0
         Output packets:                   0
         Input  bytes  :              IPv6 0
         Output bytes  :              IPv6 0
         Input  packets:              IPv6 0
         Output packets:              IPv6 0
        Local statistics:
         Input  bytes  :                   0
         Output bytes  :                   0
         Input  packets:                   0
         Output packets:                   0
         Input  bytes  :              IPv6 0
         Output bytes  :              IPv6 0
         Input  packets:              IPv6 0
         Output packets:              IPv6 0
        Transit statistics:
         Input  bytes  :                   0                 0 bps
         Output bytes  :                   0                 0 bps
         Input  packets:                   0                 0 pps
         Output packets:                   0                 0 pps
         Input  bytes  :              IPv6 0
         Output bytes  :              IPv6 0
         Input  packets:              IPv6 0
         Output packets:              IPv6 0
Flow statistics:
       Flow input statistics:
        Self packets  :                  0
        ICMP packets  :                  113
        VPN packets   :                  0
        Bytes permitted by policy:       0
        Connections established:         11
       Flow output statistics:
```

```
    Multicast packets  :              0
    Bytes permitted by policy:        0
   Flow error statistics (Packets dropped due to):
    Policy denied:                    0
    No parent for a gate:             0
    Syn-attack protection:            0
    Incoming NAT errors:              0
    No session found:                 0
    No more sessions:                 0
    Invalid zone received packet:     0
    User authentication errors:       0
    Multiple user authentications:    0
    Multiple Incoming NAT:            0
    Address spoofing:                 0
    No zone or NULL zone binding      0
    No NAT gate:                      0
    No minor session:                 0
    No session for a gate:            0
    TCP sequence number out of window: 0
    No Route present:                 0
    Authentication failed:            0
    Security association not active:  0
    No SA for incoming SPI:           0
    No one interested in self packets: 0
    Protocol inet, MTU: 1500, Generation: 139, Route table: 0
      Flags: None
      Addresses, Flags: None
        Destination: Unspecified, Local: 2.2.2.2, Broadcast: Unspecified,
        Generation: 137
      Addresses, Flags: Primary Is-Primary
        Destination: Unspecified, Local: 3.3.3.3, Broadcast: Unspecified,
        Generation: 139
```

## Sample Output

### show interfaces terse

```
user@host> show interfaces terse
    Interface               Admin Link Proto    Local                 Remote
    ge-0/0/0                up    up
    ge-0/0/0.0              up    up   inet     10.209.4.61/18
    gr-0/0/0                up    up
    ip-0/0/0                up    up
    st0                     up    up
    st0.1                   up    ready inet
    ls-0/0/0                up    up
    lt-0/0/0                up    up
    mt-0/0/0                up    up
    pd-0/0/0                up    up
    pe-0/0/0                up    up
    e3-1/0/0                up    up
    t3-2/0/0                up    up
    e1-3/0/0                up    up
    se-4/0/0                up    down
    t1-5/0/0                up    up
    br-6/0/0                up    up
    dc-6/0/0                up    up
    dc-6/0/0.32767          up    up
    bc-6/0/0:1              down  up
    bc-6/0/0:1.0            up    down
    dl0                     up    up
    dl0.0                   up    up   inet
    dsc                     up    up
```


Copyright © 2013, Juniper Networks, Inc.

```
    gre                    up    up
    ipip                   up    up
    lo0                    up    up
    lo0.16385              up    up   inet     10.0.0.1            --> 0/0
                                             10.0.0.16           --> 0/0
    lsi                    up    up
    mtun                   up    up
    pimd                   up    up
    pime                   up    up
    pp0                    up    up
```

## Sample Output

### show interfaces extensive (WAN Acceleration)

```
user@host> show interfaces wx-6/0/0 extensive
Physical interface: wx-6/0/0, Enabled, Physical link is Up
  Interface index: 142, SNMP ifIndex: 41, Generation: 143
  Type: PIC-Peer, Link-level type: PIC-Peer, MTU: 1522, Clocking: Unspecified,
  Speed: 1000mbps
  Device flags   : Present Running
  Interface flags: Point-To-Point Promiscuous SNMP-Traps Internal: 0x4000
  Link type      : Full-Duplex
  Link flags     : None
  Physical info  : Unspecified
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: Unspecified, Hardware address: Unspecified
  Alternate link address: Unspecified
  Last flapped   : 2007-08-01 05:19:35 UTC (02:12:04 ago)
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :               58427                 0 bps
   Output bytes  :              115078                 0 bps
   Input  packets:                 847                 0 pps
   Output packets:                 972                 0 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
    Policed discards: 0, Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
    Resource errors: 0
Logical interface wx-6/0/0.0 (Index 68) (SNMP ifIndex 43) (Generation 135)
    Flags: Point-To-Point SNMP-Traps Encapsulation: PIC-Peering
    Security: Zone: wx-zone
    Allowed host-inbound traffic : any-service bootp bfd bgp  dns dvmrp
    igmp ldp msdp nhrp ospf pgm pim rip router-discovery rsvp sap vrrp dhcp
    finger ftp tftp ident-reset http https ike netconf ping rlogin rpm rsh snmp
    snmp-trap ssh telnet traceroute xnm-clear-text xnm-ssl
    Flow Statistics :
    Flow Input statistics :
      Self packets :                    0
      ICMP packets :                    0
      VPN packets :                     0
      Bytes permitted by policy :       70137
      Connections established :         4
    Flow Output statistics:
      Multicast packets :               0
      Bytes permitted by policy :       2866
    Flow error statistics (Packets dropped due to):
      Address spoofing:                 0
      Authentication failed:            0
      Incoming NAT errors:              0
      Invalid zone received packet:     0
```

Copyright © 2013, Juniper Networks, Inc.

```
    Multiple user authentications:     0
    Multiple incoming NAT:             0
    No parent for a gate:              0
    No one interested in self packets: 0
    No minor session:                  0
    No more sessions:                  0
    No NAT gate:                       0
    No route present:                  0
    No SA for incoming SPI:            0
    No tunnel found:                   0
    No session for a gate:             0
    No zone or NULL zone binding       0
    Policy denied:                     0
    Security association not active:   0
    TCP sequence number out of window: 0
    Syn-attack protection:             0
    User authentication errors:        0
  Protocol inet, MTU: 1500, Generation: 141, Route table: 0
    Flags: None
    Addresses, Flags: Is-Preferred Is-Primary
      Destination: 10.87.13.2, Local: 3.3.3.3, Broadcast: Unspecified,
      Generation: 142
```

## Sample Output

### show interfaces extensive (3G Wireless Modem)

```
user@host> show interfaces cl-0/0/8 extensive
Physical interface: cl-0/0/8, Enabled, Physical link is Up
  Interface index: 67, SNMP ifIndex: 25, Generation: 4
  Type: Async-Serial, Link-level type: PPP-Subordinate, MTU: 1504,
  Clocking: Unspecified, Speed: MODEM
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link flags     : None
  Hold-times     : Up 0 ms, Down 0 ms
  CoS queues     : 8 supported, 8 maximum usable queues
  Last flapped   : Never
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :                   0                   0 bps
   Output bytes  :                 868                   0 bps
   Input  packets:                   0                   0 pps
   Output packets:                  16                   0 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
    Policed discards: 0, Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
    Resource errors: 0
  Egress queues: 8 supported, 4 in use
  Queue counters:       Queued packets  Transmitted packets      Dropped packets

    0 best-effort              6                   6                   0
    1 expedited-fo             0                   0                   0
    2 assured-forw             0                   0                   0
    3 network-cont            10                  10                   0
  MODEM status:
    Modem type                    : Sierra-USB-3G Data/Fax Modem Version 2.27m
    Initialization command string : ATS0=2
    Initialization status         : Ok
    Call status                   : Connected to 14591
    Call duration                 : 134316 seconds
```


Copyright © 2013, Juniper Networks, Inc.

```
Call direction                : Dialout
Baud rate                     : <x> bps
```

Copyright © 2013, Juniper Networks, Inc.

## show interfaces (View Aggregated Ethernet)

**Syntax**

show interfaces <ae*number* | reth*number* >
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index *snmp-index*>
<statistics>

**Release Information**

Command modified in Release 10.2 of Junos OS.

**Description**

Display status information about the specified aggregated Ethernet interface or redundant Ethernet interface. If you do not specify an interface name, status information for all interfaces is displayed.

**Options**

- ae*number* | reth*number*—(Optional) Display standard information about the specified aggregated Ethernet interface or redundant Ethernet interface.
- brief | detail | extensive | terse—(Optional) Display the specified level of output.
- descriptions—(Optional) Display interface description strings.
- media—(Optional) Display media-specific information.
- snmp-index *snmp-index*—(Optional) Display information for the specified SNMP index of the interface.
- statistics—(Optional) Display static interface statistics.

**Required Privilege Level**

view

**List of Sample Output**

show interfaces extensive (Aggregated Ethernet) on page 1684

**Output Fields**

Table 46 on page 1676 lists the output fields for the **show interfaces** (Aggregated Ethernet) command. Output fields are listed in the approximate order in which they appear.

### Table 46: Aggregated Ethernet show interfaces Output Fields

| Field Name | Field Description | Level of Output |
|---|---|---|
| Physical Interface | | |
| **Physical interface** | Name of the physical interface and state of the interface. | All levels |
| **Enabled** | State of the physical interface. For descriptions of possible values, see the "Common Output Fields" chapter in the Junos OS Operational Mode Commands. | All levels |
| **Interface index** | Index number of the physical interface, which reflects its initialization sequence. | All levels |
| **SNMP ifIndex** | SNMP index number for the physical interface. | **detail extensive** none |
| **Generation** | Unique number for use by Juniper Networks technical support only. | **detail extensive** |


Copyright © 2013, Juniper Networks, Inc.

Table 46: Aggregated Ethernet show interfaces Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **Link-level type** | Encapsulation being used on the physical interface. | All levels |
| **MTU** | Maximum transmission unit size on the physical interface. | All levels |
| **Speed** | Speed at which the interface is running. | All levels |
| **Loopback** | Loopback status: **Enabled** or **Disabled**. If loopback is enabled, type of loopback: **Local** or **Remote**. | All levels |
| **Source filtering** | Source filtering status: **Enabled** or **Disabled**. | All levels |
| **Flow control** | Flow control status: **Enabled** or **Disabled**. | All levels |
| **Minimum links needed** | Number of child links that must be operational for the aggregate interface to be operational. | All levels |
| **Device flags** | Information about the physical device. For descriptions of possible values, see the "Common Output Fields" chapter in the Junos OS Operational Mode Commands. | All levels |
| **Interface flags** | Information about the interface. For descriptions of possible values, see the "Common Output Fields" chapter in the Junos OS Operational Mode Commands. | All levels |
| **Current address** | Configured MAC address. | **detail extensive** |
| **Hardware address** | Hardware MAC address. | **detail extensive** |
| **Last flapped** | Date, time, and how long ago the interface went from down to up or up to down. The format is **Last flapped: *year-month-day hours:minutes:seconds timezone* (*hours:minutes:seconds* ago)**. For example, **Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).** | **detail extensive** |
| **Input Rate** | Input rate in bits per second (bps) and packets per second (pps). | None specified |
| **Output Rate** | Output rate in bps and pps. | None specified |
| **Statistics last cleared** | Time when the statistics for the interface were last set to zero. | **detail extensive** |
| **Traffic statistics** | Number and rate of bytes and packets received and transmitted on the physical interface.<br>• **Input bytes**—Number of bytes received on the interface.<br>• **Output bytes**—Number of bytes transmitted on the interface.<br>• **Input packets**—Number of packets received on the interface<br>• **Output packets**—Number of packets transmitted on the interface. | **detail extensive** |

Copyright © 2013, Juniper Networks, Inc.

Table 46: Aggregated Ethernet show interfaces Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **IPv6 transit statistics** | Number of IPv6 transit bytes and packets received and transmitted on the physical interface if IPv6 statistics tracking is enabled.<br>• **Input bytes**—Number of bytes received on the interface.<br>• **Output bytes**—Number of bytes transmitted on the interface.<br>• **Input packets**—Number of packets received on the interface.<br>• **Output packets**—Number of packets transmitted on the interface. | **detail extensive** |
| **Input errors** | Input errors on the interface:<br>• **Errors**—Sum of incoming frame aborts and frame check sequence (FCS) errors.<br>• **Drops**—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism.<br>• **Framing errors**—Number of packets received with an invalid FCS.<br>• **Runts**—Number of frames received that are smaller than the runt threshold.<br>• **Giants**—Number of frames received that are larger than the giant threshold.<br>• **Policed discards**—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.<br>• **Resource errors**—Sum of transmit drops. | **detail extensive** |
| **Output errors** | Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:<br>• **Carrier transitions** —Number of times the interface has gone from **down** to **up**. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC is malfunctioning.<br>• **Errors**—Sum of the outgoing frame aborts and FCS errors.<br>• **Drops**—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism.<br>• **MTU errors**—Number of packets whose size exceeded the MTU of the interface.<br>• **Resource errors**—Sum of transmit drops. | **detail extensive** |
| **Egress queues** | Total number of egress queues supported on the specified interface | **detail extensive** |
| **Queue counters** | CoS queue number and its associated user-configured forwarding class name.<br>• **Queued packets**—Number of queued packets.<br>• **Transmitted packets**—Number of transmitted packets.<br>• **Dropped packets**—Number of packets dropped by the ASIC's RED mechanism. | **detail extensive** |
| Logical Interface | | |
| **Logical interface** | Name of the logical interface. | All levels |


Copyright © 2013, Juniper Networks, Inc.

Table 46: Aggregated Ethernet show interfaces Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **Index** | Index number of the logical interface (which reflects its initialization sequence). | **detail extensive** none |
| **SNMP ifIndex** | SNMP interface index number of the logical interface. | **detail extensive** none |
| **Generation** | Unique number for use by Juniper Networks technical support only. | **detail extensive** |
| **Flags** | Information about the logical interface. For descriptions of possible values, see the "Common Output Fields" chapter in the Junos OS Operational Mode Commands. | All levels |
| **VLAN-Tag** | Tag Protocol Identifier (TPID) and VLAN identifier. | All levels |
| **Demux** | IP demultiplexing (demux) value that appears if this interface is used as the demux underlying interface. The output is one of the following:<br>• Source Family Inet<br>• Destination Family Inet | **detail extensive** none |
| **Encapsulation** | Encapsulation on the logical interface. | All levels |
| **Statistics** | Information about the number of packets, packets per second, number of bytes, and bytes per second on this aggregate interface.<br>• **Bundle**—Information about input and output bundle rates.<br>• **Link**—(**detail** and **extensive** only) Information about specific links in the aggregate, including link state and input and output rates. | **detail extensive** none |
| **LACP info** | Link Aggregation Control Protocol (LACP) information for each aggregated interface.<br>• **Role** can be one of the following:<br>  ◦ **Actor**—Local device participating in LACP negotiation.<br>  ◦ **Partner**—Remote device participating in LACP negotiation.<br>• **System priority**—Priority assigned to the system (by management or administrative policy), encoded as an unsigned integer.<br>• **System identifier**—Actor or partner system ID, encoded as a MAC address.<br>• **Port priority**—Priority assigned to the port by the actor or partner (by management or administrative policy), encoded as an unsigned integer.<br>• **Port number**—Port number assigned to the port by the actor or partner, encoded as an unsigned integer.<br>• **Port key**—Operational key value assigned to the port by the actor or partner, encoded as an unsigned integer. | **detail extensive** none |
| **LACP Statistics** | LACP statistics for each aggregated interface.<br>• **LACP Rx**—LACP received counter that increments for each normal hello.<br>• **LACP Tx**—Number of LACP transmit packet errors logged.<br>• **Unknown Rx**—Number of unrecognized packet errors logged.<br>• **Illegal Rx**—Number of invalid packets received. | **detail extensive** none |

Copyright © 2013, Juniper Networks, Inc.

Table 46: Aggregated Ethernet show interfaces Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **Marker Statistic** | (**detail** and **extensive** only) Information about 802.3ad marker protocol statistics on the specified links.<br>• **Marker Rx**—Number of valid marker PDUs received on this aggregation port.<br>• **Resp Tx**—Number of marker response PDUs transmitted on this aggregation port.<br>• **Unknown Rx**—Number of frames received that either carry the slow protocols Ethernet type value (43B.4) but contain an unknown protocol data unit (PDU), or are addressed to the slow protocols group MAC address (43B.3) but do not carry the slow protocols Ethernet type.<br>• **Illegal Rx**—Number of frames received that carry the slow protocols Ethernet type value (43B.4) but contain a badly formed PDU or an illegal value of protocol subtype (43B.4). | **detail extensive** none |
| **Flow Statistics** | Flow statistics for each aggregated interface. | **detail extensive** none |
| **Flow Input statistics** | Statistics for packets received by the flow module. | **detail extensive** none |
| **Flow Output statistics** | Statistics for packets sent by the flow module. | **detail extensive** none |


Copyright © 2013, Juniper Networks, Inc.

Table 46: Aggregated Ethernet show interfaces Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **Flow error statistics (Packets dropped due to)** | | **detail extensive** none |

Copyright © 2013, Juniper Networks, Inc.

Table 46: Aggregated Ethernet show interfaces Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| | Packet drop statistics for the flow module.<br>• **Address spoofing**—Packet dropped when the screen module detected address spoofing.<br>• **Authentication failed**—Packet dropped because the IPsec Encapsulating Security Payload (ESP) or Authentication Header (AH) authentication failed.<br>• **Incoming NAT errors**—Packet dropped because the source NAT rule search failed, an invalid source NAT binding was found, or the NAT allocation failed.<br>• **Invalid zone received packet**—This counter is not currently in use.<br>• **Multiple user authentications**—Packet dropped if it matches more than one policy that specifies user authentication. (Sometimes packets are looped through the system more than once. Each time a packet passes through the system, that packet must be permitted by a policy.)<br>• **Multiple incoming NAT**—Packet dropped if source NATing is specified more than once. (Sometimes packets are looped through the system more than once.)<br>• **No parent for a gate**—This counter is not currently in use.<br>• **No one interested in self packets**—This counter is incremented for one of the following reasons:<br>◦ The outbound interface is a self interface, but the packet is not marked as a to-self packet and the destination address is in a source NAT pool.<br>◦ No service is interested in the to-self packet<br>◦ When a zone has ident-reset service enabled, the TCP RST to IDENT request for port 113 is sent back and this counter is incremented.<br>• **No minor session**—Packet dropped because no minor sessions are available and a minor session was requested. Minor sessions are allocated for storing additional TCP state information.<br>• **No more sessions**—Packet dropped because there were no more free sessions available.<br>• **No NAT gate**—This counter is not currently in use.<br>• **No route present**—Packet dropped because a valid route was not available to forward the packet.<br>• **No SA for incoming SPI**—Packet dropped because the incoming IPsec packet's security parameter index (SPI) does not match any known SPI.<br>• **No tunnel found**—Packet dropped because a valid tunnel could not be found.<br>• **No session for a gate**—Packet dropped by an ALG.<br>• **No zone or NULL zone binding**—Packet dropped because its incoming interface was not bound to any zone.<br>• **Policy denied**—The error counter is incremented for one of the following reasons:<br>◦ Source or destination NAT (or both) has occurred and policy says to drop the packet.<br>◦ Policy specifies user authentication, which failed.<br>◦ Policy was configured to deny this packet.<br>• **Security association not active**—Packet dropped because an IPsec packet was received for an inactive SA.<br>• **TCP sequence number out of window**—TCP packet with a sequence number failed the TCP sequence number check that was received. | |


Copyright © 2013, Juniper Networks, Inc.

Table 46: Aggregated Ethernet show interfaces Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| | • **Syn-attack protection**—Packet dropped because of SYN attack protection or SYN cookie protection.<br>• **User authentication errors**—Packet dropped because policy requires authentication; however:<br>  ◦ Only Telnet, FTP, and HTTP traffic can be authenticated.<br>  ◦ The corresponding authentication entry could not be found, if web-auth is specified.<br>  ◦ The maximum number of authenticated sessions per user was exceeded. | |
| *protocol-family* | Protocol family configured on the logical interface. For descriptions of possible values, see the "Common Output Fields" chapter in the Junos OS Operational Mode Commands. | **brief** |
| **Protocol** | Protocol family configured on the logical interface. For descriptions of possible values, see the "Common Output Fields" chapter in the Junos OS Operational Mode Commands. | **detail extensive** none |
| **MTU** | Maximum transmission unit size on the logical interface. | **detail extensive** none |
| **Maximum labels** | Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface. | **detail extensive** none |
| **Generation** | Unique number for use by Juniper Networks technical support only. | **detail extensive** |
| **Route Table** | Routing table in which the logical interface address is located. For example, **0** refers to the routing table inet.0. | **detail extensive** |
| **Flags** | Information about protocol family flags. For descriptions of possible values, see the "Common Output Fields" chapter in the Junos OS Operational Mode Commands. | **detail extensive** none |
| **Mac-Validate Failures** | Number of MAC address validation failures for packets and bytes. This field is displayed when MAC address validation is enabled for the logical interface. | **detail extensive** none |
| **Addresses, Flags** | Information about address flags. For descriptions of possible values, see the "Common Output Fields" chapter in the Junos OS Operational Mode Commands. | **detail extensive** none |
| **Destination** | IP address of the remote side of the connection. | **detail extensive** none |
| **Local** | IP address of the logical interface. | **detail extensive** none |
| **Broadcast** | Broadcast address of the logical interface. | **detail extensive** none |
| **Policer** | Policer to be evaluated when packets are received or transmitted on the interface. | **detail extensive** none |
| **Generation** | Unique number for use by Juniper Networks technical support only. | **detail extensive** |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show interfaces extensive (Aggregated Ethernet)

```
user@host> show interfaces ae0 extensive

Physical interface: ae0, Enabled, Physical link is Up
  Interface index: 1973, SNMP ifIndex: 501, Generation: 2176
  Link-level type: Ethernet, MTU: 1518, Speed: 3Gbps, BPDU Error: None, MAC-REWRITE
 Error: None, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Disabled, Minimum links needed: 1,
Minimum bandwidth needed: 0
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Current address: 00:1f:12:8c:af:c0, Hardware address: 00:1f:12:8c:af:c0
  Last flapped   : 2010-04-16 14:25:36 PDT (00:02:50 ago)
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :                  64                    0 bps
   Output bytes  :          9816525824            463779840 bps
   Input  packets:                   1                    0 pps
   Output packets:            38345804               226455 pps
   IPv6 transit statistics:
    Input  bytes  :                  0
    Output bytes  :                  0
    Input  packets:                  0
    Output packets:                  0
  Dropped traffic statistics due to STP State:
   Input  bytes  :                   0
   Output bytes  :                   0
   Input  packets:                   0
   Output packets:                   0
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
 0, Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
 0
  Egress queues: 8 supported, 4 in use
  Queue counters:       Queued packets  Transmitted packets      Dropped packets

    0 best-effort             38270790             38270790                   0

    1 expedited-fo                   0                    0                   0

    2 assured-forw                   0                    0                   0

    3 network-cont                 526                  526                   0

  Logical interface ae0.0 (Index 69) (SNMP ifIndex 502) (Generation 692)
    Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.11 ]  Encapsulation: ENET2
    Statistics        Packets        pps         Bytes          bps
    Bundle:
        Input :             1          0            64            0
        Output:      38572259     226453    9874497884    463775744
    Link:
      ge-5/0/1.0
        Input :             0          0             0            0
        Output:      12743866      75484    3262429696    154591232
      ge-5/2/0.0
        Input :             1          0            64            0
        Output:      13043256      75484    3339073116    154591232
```


Copyright © 2013, Juniper Networks, Inc.

```
      ge-5/2/1.0
        Input :             0          0             0            0
        Output:      12785137      75485    3272995072    154593280
    Marker Statistics:   Marker Rx     Resp Tx   Unknown Rx   Illegal Rx
      ge-5/0/1.0                0           0            0            0
      ge-5/2/0.0                0           0            0            0
      ge-5/2/1.0                0           0            0            0
    Security: Zone: HOST
    Allowed host-inbound traffic : bootp bfd bgp dns dvmrp igmp ldp msdp nhrp
ospf pgm pim rip router-discovery rsvp sap vrrp dhcp
    finger ftp tftp ident-reset http https ike netconf ping reverse-telnet
reverse-ssh rlogin rpm rsh snmp snmp-trap ssh telnet
    traceroute xnm-clear-text xnm-ssl lsping ntp sip
    Flow Statistics :
    Flow Input statistics :
      Self packets :                    0
      ICMP packets :                    0
      VPN packets :                     0
      Multicast packets :               0
      Bytes permitted by policy :       0
      Connections established :         0
    Flow Output statistics:
      Multicast packets :               0
      Bytes permitted by policy :       8976842784
    Flow error statistics (Packets dropped due to):
      Address spoofing:                 0
      Authentication failed:            0
      Incoming NAT errors:              0
      Invalid zone received packet:     0
      Multiple user authentications:    0
      Multiple incoming NAT:            0
      No parent for a gate:             0
      No one interested in self packets: 0
      No minor session:                 0
      No more sessions:                 0
      No NAT gate:                      0
      No route present:                 0
      No SA for incoming SPI:           0
      No tunnel found:                  0
      No session for a gate:            0
      No zone or NULL zone binding      0
      Policy denied:                    0
      Security association not active:  0
      TCP sequence number out of window: 0
      Syn-attack protection:            0
      User authentication errors:       0
    Protocol inet, MTU: 1500, Generation: 841, Route table: 0
      Flags: Sendbcast-pkt-to-re
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 100.1.1/24, Local: 100.1.1.2, Broadcast: 100.1.1.255,
Generation: 422
    Protocol multiservice, MTU: Unlimited, Generation: 842, Route table: 0
      Flags: Is-Primary
      Policer: Input: __default_arp_policer__
   Logical interface ae0.32767 (Index 83) (SNMP ifIndex 503) (Generation 693)
    Flags: SNMP-Traps 0x4004000 VLAN-Tag [ 0x0000.0 ]  Encapsulation: ENET2
    Statistics        Packets        pps         Bytes          bps
    Bundle:
        Input :             0          0             0            0
        Output:             0          0             0            0
    Link:
```

```
      ge-5/0/1.32767
        Input :             0          0             0           0
        Output:             0          0             0           0
      ge-5/2/0.32767
        Input :             0          0             0           0
        Output:             0          0             0           0
      ge-5/2/1.32767
        Input :             0          0             0           0
        Output:             0          0             0           0
    LACP info:        Role     System             System      Port    Port  Port

                              priority          identifier  priority  number   key

      ge-5/0/1.32767    Actor      127 00:1f:12:8c:af:c0       127     833     1

      ge-5/0/1.32767  Partner      127 00:1f:12:8f:d7:c0       127     641     1

      ge-5/2/0.32767    Actor      127 00:1f:12:8c:af:c0       127     848     1

      ge-5/2/0.32767  Partner      127 00:1f:12:8f:d7:c0       127     656     1

      ge-5/2/1.32767    Actor      127 00:1f:12:8c:af:c0       127     849     1

      ge-5/2/1.32767  Partner      127 00:1f:12:8f:d7:c0       127     657     1

    LACP Statistics:       LACP Rx     LACP Tx   Unknown Rx   Illegal Rx
      ge-5/0/1.32767           342         511            0            0
      ge-5/2/0.32767           344         498            0            0
      ge-5/2/1.32767           344         500            0            0
    Marker Statistics:   Marker Rx     Resp Tx   Unknown Rx   Illegal Rx
      ge-5/0/1.32767             0           0            0            0
      ge-5/2/0.32767             0           0            0            0
      ge-5/2/1.32767             0           0            0            0
    Security: Zone: HOST
    Allowed host-inbound traffic : bootp bfd bgp dns dvmrp igmp ldp msdp nhrp
ospf pgm pim rip router-discovery rsvp sap vrrp dhcp
    finger ftp tftp ident-reset http https ike netconf ping reverse-telnet
reverse-ssh rlogin rpm rsh snmp snmp-trap ssh telnet
    traceroute xnm-clear-text xnm-ssl lsping ntp sip
    Flow Statistics :
    Flow Input statistics :
      Self packets :                    0
      ICMP packets :                    0
      VPN packets :                     0
      Multicast packets :               0
      Bytes permitted by policy :       0
      Connections established :         0
    Flow Output statistics:
      Multicast packets :               0
      Bytes permitted by policy :       0
    Flow error statistics (Packets dropped due to):
      Address spoofing:                 0
      Authentication failed:            0
      Incoming NAT errors:              0
      Invalid zone received packet:     0
      Multiple user authentications:    0
      Multiple incoming NAT:            0
      No parent for a gate:             0
      No one interested in self packets: 0
      No minor session:                 0
      No more sessions:                 0
```


Copyright © 2013, Juniper Networks, Inc.

```
  No NAT gate:                        0
  No route present:                   0
  No SA for incoming SPI:             0
  No tunnel found:                    0
  No session for a gate:              0
  No zone or NULL zone binding        0
  Policy denied:                      0
  Security association not active:    0
  TCP sequence number out of window: 0
  Syn-attack protection:              0
  User authentication errors:         0
Protocol multiservice, MTU: Unlimited, Generation: 843, Route table: 0
  Flags: None
  Policer: Input: __default_arp_policer__
```

Copyright © 2013, Juniper Networks, Inc.

## show interfaces flow-statistics

**Syntax** **show interfaces flow-statistics** *<interface-name>*

**Release Information** Command introduced in Release 8.5 of Junos OS.

**Description** Display interfaces flow statistics.

**Options** *Interface-name*—(Optional) Display flow statistics about the specified interface. Following is a list of typical interface names. Replace *pim* with the PIM slot and *port* with the port number. For a complete list, see the *Junos OS Interfaces Configuration Guide for Security Devices*.

- **at-*pim*/0/*port***—ATM-over-ADSL or ATM-over-SHDSL interface.
- **br-*pim*/0/*port***—Basic Rate Interface for establishing ISDN connections.
- **ce1-*pim*/0/*port***—Channelized E1 interface.
- **ct1-*pim*/0/*port***—Channelized T1 interface.
- **dl0**—Dialer Interface for initiating ISDN and USB modem connections.
- **e1-*pim*/0/*port***—E1 interface.
- **e3-*pim*/0/*port***—E3 interface.
- **fe-*pim*/0/ *port***—Fast Ethernet interface.
- **ge-*pim*/0/*port***—Gigabit Ethernet interface.
- **se-*pim*/0/*port***—Serial interface.
- **t1-*pim*/0/*port***—T1 (also called DS1) interface.
- **t3-*pim*/0/ *port***—T3 (also called DS3) interface.
- **wx-*slot*/0/0**—WAN acceleration interface, for the WXC Integrated Services Module (ISM 200).

**Required Privilege Level** view

**Related Documentation**
- Interfaces for Security Devices
- MPLS for Security Devices

**List of Sample Output** show interfaces flow-statistics (Gigabit Ethernet) on page 1692

**Output Fields** Table 47 on page 1689 lists the output fields for the **show interfaces flow-statistics** command. Output fields are listed in the approximate order in which they appear.

 Copyright © 2013, Juniper Networks, Inc.

### Table 47: show interfaces flow-statistics Output Fields

| Field Name | Field Description |
|---|---|
| **Traffic statistics** | Number of packets and bytes transmitted and received on the physical interface. |
| **Local statistics** | Number of packets and bytes transmitted and received on the physical interface. |
| **Transit statistics** | Number of packets and bytes transiting the physical interface. |
| **Flow input statistics** | Statistics on packets received by flow module. |
| **Flow output statistics** | Statistics on packets sent by flow module. |
| **Flow error statistics** | Packet drop statistics for the flow module.<br><br>For further detail, see Table 48 on page 1689 |

### Table 48: Flow Error Statistics (packet drop statistics for the flow module)

| Error | Error Description |
|---|---|
| Screen: | |
| Address spoofing | The packet was dropped when the screen module detected address spoofing. |
| Syn-attack protection | The packet was dropped because of SYN attack protection or SYN cookie protection. |
| VPN: | |
| Authentication failed | The packet was dropped because the IPsec Encapsulating Security Payload (ESP) or Authentication Header (AH) authentication failed. |
| No SA for incoming SPI | The packet was dropped because the incoming IPsec packet's security parameter index (SPI) does not match any known SPI. |
| Security association not active | The packet was dropped because an IPsec packet was received for an inactive SA. |
| NAT: | |
| Incoming NAT errors | The source NAT rule search failed, an invalid source NAT binding was found, or the NAT allocation failed. |
| Multiple incoming NAT | Sometimes packets are looped through the system more than once; if source NATing is specified more than once, the packet will be dropped. |
| Auth: | |
| Multiple user authentications | Sometimes packets are looped through the system more than once. Each time a packet passes through the system, that packet must be permitted by a policy. If the packet matches more than one policy that specifies user authentication, then it will be dropped. |

Copyright © 2013, Juniper Networks, Inc.

Table 48: Flow Error Statistics (packet drop statistics for the flow module) *(continued)*

| | |
|---|---|
| User authentication errors | Packet was dropped because policy requires authentication; however:<br>• Only Telnet, FTP, and HTTP traffic can be authenticated.<br>• The corresponding authentication entry could not be found, if web-auth is specified.<br>• The maximum number of authenticated sessions per user was exceeded. |
| Flow: | |
| No one interested in self packets | This counter is incremented for one of the following reasons:<br>• The outbound interface is a self interface, but the packet is not marked as a to-self packet and the destination address is in a source NAT pool.<br>• No service is interested in the to-self packet<br>• When a zone has ident-reset service enabled, the TCP RST to IDENT request for port 113 is sent back and this counter is incremented. |
| No minor session | The packet was dropped because no minor sessions are available and a minor session was requested. Minor sessions are allocated for storing additional TCP state information. |
| No more sessions | The packet was dropped because there were no more free sessions available. |
| No route present | The packet was dropped because a valid route was not available to forward the packet.<br>For new sessions, the counter is incremented for one of the following reasons:<br>• No valid route was found to forward the packet.<br>• A discard or reject route was found.<br>• The route could not be added due to lack of memory.<br>• The reverse path forwarding check failed for an incoming multicast packet.<br>For existing sessions, the prior route was changed or deleted, or a more specific route was added. The session is rerouted, and this reroute could fail because:<br>• A new route could not be found; either the previous route was removed, or the route was changed to discard or reject.<br>• Multiple packets may concurrently force rerouting to occur, and only one packet can successfully complete the rerouting process. Other packets will be dropped.<br>• The route table was locked for updates by the routing engine. Packets that match a new session are retried, whereas packets that match an existing session are not. |
| No tunnel found | The packet was dropped because a valid tunnel could not be found |
| No session for a gate | This counter is incremented when a packet is destined for an ALG, and the ALG decides to drop this packet. |
| No zone or NULL zone binding | The packet was dropped because its incoming interface was not bound to any zone. |
| Policy denied | The error counter is incremented for one of the following reasons:<br>• Source and/or destination NAT has occurred and policy says to drop the packet.<br>• Policy specifies user authentication, which failed.<br>• Policy was configured to deny this packet. |


Copyright © 2013, Juniper Networks, Inc.

Table 48: Flow Error Statistics (packet drop statistics for the flow module) *(continued)*

| | |
|---|---|
| TCP sequence number out of window | A TCP packet with a sequence number failed the TCP sequence number check that was received. |
| **Counters Not Currently in Use** | |
| No parent for a gate | - |
| Invalid zone received packet | - |
| No NAT gate | - |

## Sample Output

### show interfaces flow-statistics (Gigabit Ethernet)

```
user@host> show interfaces flow-statistics ge-0/0/1.0
  Logical interface ge-0/0/1.0 (Index 70) (SNMP ifIndex 49)
    Flags: SNMP-Traps Encapsulation: ENET2
    Input packets : 5161
    Output packets: 83
    Security: Zone: zone2
    Allowed host-inbound traffic : bootp bfd bgp  dns dvmrp igmp ldp msdp nhrp
ospf pgm
    pim rip router-discovery rsvp sap vrrp dhcp finger ftp tftp ident-reset http
 https ike
   netconf ping rlogin rpm rsh snmp snmp-trap ssh telnet traceroute xnm-clear-text
 xnm-ssl
    lsping
    Flow Statistics :
    Flow Input statistics :
      Self packets :                    0
      ICMP packets :                    0
      VPN packets :                     2564
      Bytes permitted by policy :       3478
      Connections established :         1
    Flow Output statistics:
      Multicast packets :               0
      Bytes permitted by policy :       16994
    Flow error statistics (Packets dropped due to):
      Address spoofing:                 0
      Authentication failed:            0
      Incoming NAT errors:              0
      Invalid zone received packet:     0
      Multiple user authentications:    0
      Multiple incoming NAT:            0
      No parent for a gate:             0
      No one interested in self packets: 0
      No minor session:                 0
      No more sessions:                 0
      No NAT gate:                      0
      No route present:                 0
      No SA for incoming SPI:           0
      No tunnel found:                  0
      No session for a gate:            0
      No zone or NULL zone binding      0
      Policy denied:                    0
      Security association not active:  0
      TCP sequence number out of window: 0
      Syn-attack protection:            0
      User authentication errors:       0
    Protocol inet, MTU: 1500
      Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 2.2.2/24, Local: 2.2.2.2, Broadcast: 2.2.2.255
```


Copyright © 2013, Juniper Networks, Inc.

## show interfaces diagnostics optics

**Syntax** show interfaces diagnostics optics *interface-name*

**Release Information** Command introduced in Release 10.1 of Junos OS.

**Description** Display diagnostics data and alarms for Gigabit Ethernet optical transceivers (SFP) installed in SRX Series Services Gateways. The information provided by this command is known as digital optical monitoring (DOM) information.

Thresholds that trigger a high alarm, low alarm, high warning, or low warning are set by the transponder vendors. Generally, a high alarm or low alarm indicates that the optics module is not operating properly. This information can be used to diagnose why a transceiver is not working.

**Options** *interface-name*—Name of the interface associated with the port in which the transceiver is installed: **ge-*fpc/pic/port*** .

**Required Privilege Level** view

**Related Documentation**
- Interfaces for Security Devices

**List of Sample Output** show interfaces diagnostics optics on page 1697

**Output Fields** Table 49 on page 1693 the output fields for the show interfaces diagnostics optics command. Output fields are listed in the general order in which they appear.

### Table 49: show interfaces diagnostics optics Output Fields

| Field Name | Field Description |
|---|---|
| **Physical interface** | Displays the name of the physical interface. |
| **Laser bias current** | Displays the magnitude of the laser bias power setting current, in milliamperes. The laser bias provides direct modulation of laser diodes and modulates currents. |
| **Laser output power** | Displays the laser output power, in milliwatts (mW) and decibels referred to 1.0 mW (dBm). |
| **Module temperature** | Displays the temperature, in Celsius and Fahrenheit. |
| **Module voltage** | Displays the voltage, in Volts. |
| **Receiver signal average optical power** | Displays the receiver signal average optical power, in milliwatts (mW) and decibels referred to 1.0 mW (dBm). |
| **Laser bias current high alarm** | Displays whether the laser bias power setting high alarm is **On** or **Off**. |

Copyright © 2013, Juniper Networks, Inc.

Table 49: show interfaces diagnostics optics Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Laser bias current low alarm** | Displays whether the laser bias power setting low alarm is **On** or **Off**. |
| **Laser bias current high warning** | Displays whether the laser bias power setting high warning is **On** or **Off**. |
| **Laser bias current low warning** | Displays whether the laser bias power setting low warning is **On** or **Off**. |
| **Laser output power high alarm** | Displays whether the laser output power high alarm is **On** or **Off**. |
| **Laser output power low alarm** | Displays whether the laser output power low alarm is **On** or **Off**. |
| **Laser output power high warning** | Displays whether the laser output power high warning is **On** or **Off**. |
| **Laser output power low warning** | Displays whether the laser output power low warning is **On** or **Off**. |
| **Module temperature high alarm** | Displays whether the module temperature high alarm is **On** or **Off**. |
| **Module temperature low alarm** | Displays whether the module temperature low alarm is **On** or **Off**. |
| **Module temperature high warning** | Displays whether the module temperature high warning is **On** or **Off**. |
| **Module temperature low warning** | Displays whether the module temperature low warning is **On** or **Off**. |
| **Module voltage high alarm** | Displays whether the module voltage high alarm is **On** or **Off**. |
| **Module voltage low alarm** | Displays whether the module voltage low alarm is **On** or **Off**. |
| **Module voltage high warning** | Displays whether the module voltage high warning is **On** or **Off**. |
| **Module voltage low warning** | Displays whether the module voltage low warning is **On** or **Off**. |
| **Laser rx power high alarm** | Displays whether the receive laser power high alarm is **On** or **Off**. |
| **Laser rx power low alarm** | Displays whether the receive laser power low alarm is **On** or **Off**. |


Copyright © 2013, Juniper Networks, Inc.

Table 49: show interfaces diagnostics optics Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Laser rx power high warning** | Displays whether the receive laser power high warning is **On** or **Off**. |
| **Laser rx power low warning** | Displays whether the receive laser power low warning is **On** or **Off**. |
| **Laser bias current high alarm threshold** | Displays the vendor-specified threshold for the laser bias current high alarm. |
| **Laser bias current low alarm threshold** | Displays the vendor-specified threshold for the laser bias current low alarm. |
| **Laser bias current high warning threshold** | Displays the vendor-specified threshold for the laser bias current high warning. |
| **Laser bias current low warning threshold** | Displays the vendor-specified threshold for the laser bias current low warning. |
| **Laser output power high alarm threshold** | Displays the vendor-specified threshold for the laser output power high alarm. |
| **Laser output power low alarm threshold** | Displays the vendor-specified threshold for the laser output power low alarm. |
| **Laser output power high warning threshold** | Displays the vendor-specified threshold for the laser output power high warning. |
| **Laser output power low warning threshold** | Displays the vendor-specified threshold for the laser output power low warning. |
| **Module temperature high alarm threshold** | Displays the vendor-specified threshold for the module temperature high alarm. |
| **Module temperature low alarm threshold** | Displays the vendor-specified threshold for the module temperature low alarm. |
| **Module temperature high warning threshold** | Displays the vendor-specified threshold for the module temperature high warning. |
| **Module temperature low warning threshold** | Displays the vendor-specified threshold for the module temperature low warning. |
| **Module voltage high alarm threshold** | Displays the vendor-specified threshold for the module voltage high alarm. |
| **Module voltage low alarm threshold** | Displays the vendor-specified threshold for the module voltage low alarm. |
| **Module voltage high warning threshold** | Displays the vendor-specified threshold for the module voltage high warning. |

Copyright © 2013, Juniper Networks, Inc.

Table 49: show interfaces diagnostics optics Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Module voltage low warning threshold** | Displays the vendor-specified threshold for the module voltage low warning. |
| **Laser rx power high alarm threshold** | Displays the vendor-specified threshold for the laser rx power high alarm. |
| **Laser rx power low alarm threshold** | Displays the vendor-specified threshold for the laser rx power low alarm. |
| **Laser rx power high warning threshold** | Displays the vendor-specified threshold for the laser rx power high warning. |
| **Laser rx power low warning threshold** | Displays the vendor-specified threshold for the laser rx power low warning. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show interfaces diagnostics optics

```
user@host> show interfaces diagnostics optics ge-2/0/0
Physical interface: ge-2/0/0
    Laser bias current                          :  7.408 mA
    Laser output power                          :  0.3500 mW / -4.56 dBm
    Module temperature                          :  23 degrees C / 73 degrees F
    Module voltage                              :  3.3450 V
    Receiver signal average optical power       :  0.0002 mW / -36.99 dBm
    Laser bias current high alarm               :  Off
    Laser bias current low alarm                :  Off
    Laser bias current high warning             :  Off
    Laser bias current low warning              :  Off
    Laser output power high alarm               :  Off
    Laser output power low alarm                :  Off
    Laser output power high warning             :  Off
    Laser output power low warning              :  Off
    Module temperature high alarm               :  Off
    Module temperature low alarm                :  Off
    Module temperature high warning             :  Off
    Module temperature low warning              :  Off
    Module voltage high alarm                   :  Off
    Module voltage low alarm                    :  Off
    Module voltage high warning                 :  Off
    Module voltage low warning                  :  Off
    Laser rx power high alarm                   :  Off
    Laser rx power low alarm                    :  On
    Laser rx power high warning                 :  Off
    Laser rx power low warning                  :  On
    Laser bias current high alarm threshold     :  17.000 mA
    Laser bias current low alarm threshold      :  1.000 mA
    Laser bias current high warning threshold   :  14.000 mA
    Laser bias current low warning threshold    :  2.000 mA
    Laser output power high alarm threshold     :  0.6310 mW / -2.00 dBm
    Laser output power low alarm threshold      :  0.0670 mW / -11.74 dBm
    Laser output power high warning threshold   :  0.6310 mW / -2.00 dBm
    Laser output power low warning threshold    :  0.0790 mW / -11.02 dBm
    Module temperature high alarm threshold     :  95 degrees C / 203 degrees F
    Module temperature low alarm threshold      :  -25 degrees C / -13 degrees F
    Module temperature high warning threshold   :  90 degrees C / 194 degrees F
    Module temperature low warning threshold    :  -20 degrees C / -4 degrees F
    Module voltage high alarm threshold         :  3.900 V
    Module voltage low alarm threshold          :  2.700 V
    Module voltage high warning threshold       :  3.700 V
    Module voltage low warning threshold        :  2.900 V
    Laser rx power high alarm threshold         :  1.2590 mW / 1.00 dBm
    Laser rx power low alarm threshold          :  0.0100 mW / -20.00 dBm
    Laser rx power high warning threshold       :  0.7940 mW / -1.00 dBm
    Laser rx power low warning threshold        :  0.0158 mW / -18.01 dBm
```

Copyright © 2013, Juniper Networks, Inc.

## show interfaces swfabx

**Syntax** show interfaces <swfab0 | swfab1>

**Release Information** Command introduced in Release 11.1 of Junos OS.

**Description** List the configured interfaces for each swfab interface. The swfab interface can contain one or more members because it is an aggregated interface.

**Required Privilege Level** view

**Related Documentation**
- clear interfaces statistics swfabx on page 1376

**List of Sample Output** show interfaces <swfab0 | swfab1> on page 1698

**Output Fields** Table 50 on page 1698 lists the output fields for the **show interfaces <swfab0 | swfab1>** command. Output fields are listed in the approximate order in which they appear.

### Table 50: show interfaces <swfab0 | swfab1> Output Fields

| Field Name | Field Description |
|---|---|
| **fabric-options** | The fabric-options hierarchy is made to be in sync with the fab interfaces. |
| **member-interfaces** | Interfaces specified under member-interfaces are single logical aggregate-Ethernet interfaces.<br><br>This interface carries internode switching traffic. |

## Sample Output

### show interfaces <swfab0 | swfab1>

```
user@host> show interfaces <swfab0 | swfab1>
fabric-options {
       member-interfaces {
           ge-0/0/6;
           ge-0/0/7;
       }
  }
```


Copyright © 2013, Juniper Networks, Inc.

## show interfaces statistics (View)

**Syntax** show interfaces statistics *interface-name*

**Release Information** Command introduced in Release 10.1 of Junos OS.

**Description** Displays the interface input and output statistics for physical and logical interface.

**Required Privilege Level** view

**Related Documentation**
- Interfaces for Security Devices
- MPLS for Security Devices

**List of Sample Output** show interfaces statistics on page 1699

### Sample Output

show interfaces statistics

```
user@host> show interfaces statistics st0.1
Logical interface st0.1 (Index 91) (SNMP ifIndex 268)
     Flags: Point-To-Point SNMP-Traps Encapsulation: Secure-Tunnel
     Input packets : 2743333
     Output packets: 6790470992
     Security: Zone: untrust
     Allowed host-inbound traffic : bootp bfd bgp dns dvmrp igmp ldp msdp nhrp
ospf pgm pim rip router-discovery rsvp sap vrrp dhcp finger ftp tftp ident-reset
 http https ike netconf ping reverse-telnet
    reverse-ssh rlogin rpm rsh snmp snmp-trap ssh telnet traceroute xnm-clear-text
 xnm-ssl lsping ntp sip
     Protocol inet, MTU: 9192
       Addresses, Flags: Is-Preferred Is-Primary
         Destination: 192.167.1.0/30, Local: 192.167.1.1
```

Copyright © 2013, Juniper Networks, Inc.

## show lacp interfaces (View)

**Syntax** **show lacp interfaces** <*interface-name*>

**Release Information** Command modified in Release 10.2 of Junos OS.

**Description** Display Link Aggregation Control Protocol (LACP) information about the specified aggregated Ethernet interface, redundant Ethernet interface, Gigabit Ethernet interface, or 10-Gigabit Ethernet interface. If you do not specify an interface name, LACP information for all interfaces is displayed.

**Options** ***interface-name***—(Optional) Display LACP information for the specified interface:

- Aggregated Ethernet—**ae*number***
- Redundant Ethernet—**reth*number***
- Gigabit Ethernet—**ge-*fpc/pic/port***
- 10-Gigabit Ethernet—**xe*number***

**Required Privilege Level** view

**List of Sample Output**
show lacp interfaces (Aggregated Ethernet) on page 1703
show lacp interfaces (Redundant Ethernet) on page 1703
show lacp interfaces (Gigabit Ethernet) on page 1703

**Output Fields** Table 51 on page 1700 lists the output fields for the **show lacp interfaces** command. Output fields are listed in the approximate order in which they appear.

### Table 51: show lacp interfaces Output Fields

| Field Name | Field Description |
|---|---|
| **Aggregated interface** | Aggregated interface value. |


Copyright © 2013, Juniper Networks, Inc.

Table 51: show lacp interfaces Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **LACP State** | LACP state information for each aggregated interface:<br>• **Role**—Role played by the interface. It can be one of the following:<br>  ◦ **Actor**—Local device participating in LACP negotiation.<br>  ◦ **Partner**—Remote device participating in LACP negotiation.<br>• **Exp**—Expired state. **Yes** indicates the actor or partner is in an expired state. **No** indicates the actor or partner is not in an expired state.<br>• **Def**—Default. **Yes** indicates that the actor's receive machine is using the default operational partner information, administratively configured for the partner. **No** indicates the operational partner information in use has been received in a link aggregation control protocol data unit (PDU).<br>• **Dist**—Distribution of outgoing frames. **No** indicates distribution of outgoing frames on the link is currently disabled and is not expected to be enabled. Otherwise, the value is **Yes**.<br>• **Col**—Collection of incoming frames. **Yes** indicates collection of incoming frames on the link is currently enabled and is not expected to be disabled. Otherwise, the value is **No**.<br>• **Syn**—Synchronization. If the value is **Yes**, the link is considered synchronized. It has been allocated to the correct link aggregation group, the group has been associated with a compatible aggregator, and the identity of the link aggregation group is consistent with the system ID and operational key information transmitted. If the value is **No**, the link is not synchronized. It is currently not in the right aggregation.<br>• **Aggr**—Ability of aggregation port to aggregate (**Yes**) or to operate only as an individual link (**No**).<br>• **Timeout**—LACP timeout preference. Periodic transmissions of link aggregation control PDUs occur at either a slow or fast transmission rate, depending upon the expressed LACP timeout preference (**Long Timeout** or **Short Timeout**).<br>• **Activity**—Actor or partner's port activity. **Passive** indicates the port's preference for not transmitting link aggregation control PDUs unless its partner's control value is **Active**. **Active** indicates the port's preference to participate in the protocol regardless of the partner's control value. |

Copyright © 2013, Juniper Networks, Inc.

Table 51: show lacp interfaces Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **LACP Protocol** | LACP protocol information for each aggregated interface:<br>• Link state (active or standby) indicated in parentheses next to the interface when link protection is configured.<br>• **Receive State**—One of the following values:<br>  • **Current**—The state machine receives a link aggregation control PDU and enters the **Current** state.<br>  • **Defaulted**—If no link aggregation control PDU is received before the timer for the **Current** state expires a second time, the state machine enters the **Defaulted** state.<br>  • **Expired**—If no link aggregation control PDU is received before the timer for the **Current** state expires once, the state machine enters the **Expired** state.<br>  • **Initialize**—When the physical connectivity of a link changes or a Begin event occurs, the state machine enters the **Initialize** state.<br>  • **LACP Disabled**—If the port is operating in half duplex, the operation of LACP is disabled on the port, forcing the state to **LACP Disabled**. This state is similar to the **Defaulted** state, except that the port is forced to operate as an individual port.<br>  • **Port Disabled**—If the port becomes inoperable and a Begin event has not occurred, the state machine enters the **Port Disabled** state.<br>• **Transmit State**—Transmit state of state machine. One of the following values:<br>  • **Fast Periodic**—Periodic transmissions are enabled at a fast transmission rate.<br>  • **No Periodic**—Periodic transmissions are disabled.<br>  • **Periodic Timer**—Transitory state entered when the periodic timer expires.<br>  • **Slow Periodic**—Periodic transmissions are enabled at a slow transmission rate.<br>• **Mux State**—State of the multiplexer state machine for the aggregation port. The state is one of the following values:<br>  • **Attached**—Multiplexer state machine initiates the process of attaching the port to the selected aggregator.<br>  • **Collecting Distributing**—Collecting and distributing states are merged together to form a combined state (coupled control). Because independent control is not possible, the coupled control state machine does not wait for the partner to signal that collection has started before enabling both collection and distribution.<br>  • **Detached**—Process of detaching the port from the aggregator is in progress.<br>  • **Waiting**—Multiplexer state machine is in a holding process, awaiting an outcome. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show lacp interfaces (Aggregated Ethernet)

```
user@host> show lacp interfaces ae0
Aggregated interface: ae0
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-2/0/0       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-2/0/0     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-2/0/1       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-2/0/1     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-2/2/0       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-2/2/0     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-2/2/1       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-2/2/1     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      ge-2/0/0                  Current   Fast periodic Collecting distributing
      ge-2/0/1                  Current   Fast periodic Collecting distributing
      ge-2/2/0                  Current   Fast periodic Collecting distributing
      ge-2/2/1                  Current   Fast periodic Collecting distributing
```

### show lacp interfaces (Redundant Ethernet)

```
user@host> show lacp interfaces reth0
Aggregated interface: reth0
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-11/0/0      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-11/0/0    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-11/0/1      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-11/0/1    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-11/0/2      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-11/0/2    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-11/0/3      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-11/0/3    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-3/0/0       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-3/0/0     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-3/0/1       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-3/0/1     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-3/0/2       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-3/0/2     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-3/0/3       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-3/0/3     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      ge-11/0/0                 Current   Fast periodic Collecting distributing
      ge-11/0/1                 Current   Fast periodic Collecting distributing
      ge-11/0/2                 Current   Fast periodic Collecting distributing
      ge-11/0/3                 Current   Fast periodic Collecting distributing
      ge-3/0/0                  Current   Fast periodic Collecting distributing
      ge-3/0/1                  Current   Fast periodic Collecting distributing
      ge-3/0/2                  Current   Fast periodic Collecting distributing
      ge-3/0/3                  Current   Fast periodic Collecting distributing
{primary:node1}
```

### show lacp interfaces (Gigabit Ethernet)

```
user@host> show lacp interfaces ge-0/3/0
Aggregated interface: ae0
    LACP State:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-0/3/0       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/3/0     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP Protocol:   Receive State    Transmit State          Mux State
      ge-0/3/0             Current     Fast periodic  Collecting distributing
```

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

## show lacp statistics interfaces (View)

**Syntax** **show lacp statistics interfaces** *interface-name*

**Release Information** Command modified in Release 10.2 of Junos OS.
Command introduced in Release 11.1 of Junos OS for the QFX Series.

**Description** Display Link Aggregation Control Protocol (LACP) statistics about the specified aggregated Ethernet interface or redundant Ethernet interface. If you do not specify an interface name, LACP statistics for all interfaces are displayed.

**Options** ***interface-name***—(Optional) Name of an interface.

**Required Privilege Level** view

**Related Documentation**

- Configuring Link Aggregation
- Verifying the Status of a LAG Interface
- Verifying That LACP Is Configured Correctly and Bundle Members Are Exchanging LACP Protocol Packets
- Example: Configuring Link Aggregation Between a QFX Series Product and an Aggregation Switch
- Example: Configuring Link Aggregation with LACP Between a QFX Series Product and an Aggregation Switch

**List of Sample Output**
show lacp statistics interfaces on page 1706
show lacp statistics interfaces (QFX Series) on page 1706
show lacp statistics interfaces (QFabric Switches) on page 1706

**Output Fields** Table 52 on page 1705 lists the output fields for the **show lacp statistics interfaces** command. Output fields are listed in the approximate order in which they appear.

### Table 52: show lacp statistics interfaces Output Fields

| Field Name | Field Description |
|---|---|
| **Aggregated interface** | Aggregated interface value. |
| **LACP Statistics** | LACP statistics provide the following information:<br>• **LACP Rx**—LACP received counter that increments for each normal hello.<br>• **LACP Tx**—Number of LACP transmit packet errors logged.<br>• **Unknown Rx**—Number of unrecognized packet errors logged.<br>• **Illegal Rx**—Number of invalid packets received. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show lacp statistics interfaces

```
user@host> show lacp statistics interfaces ae0
Aggregated interface: ae0
    LACP Statistics:       LACP Rx     LACP Tx   Unknown Rx   Illegal Rx
      ge-2/0/0                1352        2035            0            0
      ge-2/0/1                1352        2056            0            0
      ge-2/2/0                1352        2045            0            0
      ge-2/2/1                1352        2043            0            0
```

### show lacp statistics interfaces (QFX Series)

```
user@host> show lacp statistics interfaces ae0
Aggregated interface: ae0
    LACP Statistics:       LACP Rx     LACP Tx   Unknown Rx   Illegal Rx
      xe-0/0/2                1352        2035            0            0
      xe-0/0/3                1352        2056            0            0
```

### show lacp statistics interfaces (QFabric Switches)

```
user@host> show lacp statistics interfaces nodegroup1:ae0
Aggregated interface: nodegroup1:ae0
    LACP Statistics:       LACP Rx     LACP Tx   Unknown Rx   Illegal Rx
      node1:xe-0/0/2              1352        2035            0            0
      node2:xe-0/0/3              1352        2056            0            0
```


Copyright © 2013, Juniper Networks, Inc.

## show modem wireless interface

**Syntax** **show modem wireless interface *interface-name***

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** Display information about 3G wireless modem interface.

**Options** **interface *interface-name***—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.

**Required Privilege Level** view

**Related Documentation**
- Modem Interfaces
- Interfaces for Security Devices

**List of Sample Output** show modem wireless interface cl-0/0/8 on page 1708

**Output Fields** Table 53 on page 1707 lists the output fields for the **show modem wireless interface** command.

### Table 53: show modem wireless interface Output Fields

| Field Name | Field Description |
|---|---|
| **Wireless modem firmware details** | Display firmware information about the 3G wireless modem. See show modem wireless interface firmware. |
| **Wireless Modem Network Info** | Display network statistics for the 3G wireless modem interface. See show modem wireless interface network. |
| **Radio statistics** | Display received signal strength indication (RSSI) for the 3G wireless modem. See show modem wireless interface rssi. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show modem wireless interface cl-0/0/8

```
user@host> show modem wireless interface cl-0/0/8
Wireless modem firmware details
  Modem firmware version: F1_2_3_15AP C:/WS/FW/F1_2_3_15AP/MSM7200R3/SRC/AMSS
2008/07/09 12:22:16
  Modem Firmware build date: 07/09/08
  Card type: Aircard 880E
  Modem manufacturer: Sierra Wireless, Inc
  Hardware version: 1.0
  Factory serial number (FSN): D46031822831022W
  Modem PIN security status: Disabled.
  SIM Status: SIM Okay
  SIM lock: Unlocked
  SIM user operation needed: No Op
  Retries remaining: 3
  Current modem temperature: 25 deg C
Wireless Modem Network Info
  Current Modem Status: Online
  Current Service Status: Offline
  Current Service Type: Combo(CS,PS)
  Current Service Mode: HSPA
  Current Band: 257.
  Roaming Status: No
  Network Selection Mode: Automatic
  Network:
  Mobile Country Code (MCC): 1
  Mobile Network Code (MNC): 1
  Location Area Code (LAC): 128
  Routing Area Code (RAC): 0
  Cell Identification: 0
  Scrambling Code: 9
Radio statistics
  Current radio signal strength: -95 dB
```


Copyright © 2013, Juniper Networks, Inc.

## show modem wireless interface firmware

**Syntax** **show modem wireless interface *interface-name* firmware**

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** Display firmware details for 3G wireless modem interface.

**Options** **interface *interface-name***—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.

**Required Privilege Level** view

**Related Documentation**
- Modem Interfaces
- Interfaces for Security Devices

**List of Sample Output**
show modem wireless interface firmware (CDMA EV-DO modem) on page 1710
show modem wireless interface firmware (GSM modem) on page 1710

**Output Fields** Table 54 on page 1709 lists some of the output fields for the **show modem wireless interface firmware** command. Output fields are listed in the approximate order in which they appear.

### Table 54: show modem wireless interface firmware Output Fields

| Field Name | Field Description |
|---|---|
| **SIM Status** | Status of the subscriber identity module (SIM) in the GSM 3G wireless modem card. The status can be one of the following states:<br>• **SIM Okay**<br>• **SIM not inserted**<br>• **SIM removed**<br>• **SIM init failure**—There is a problem with the SIM; the SIM may need to be replaced.<br>• **SIM locked**<br>• **PIN1 blocked**—Obtain a PIN unblocking key (PUK) to unblock the SIM.<br>• **PIN1 rejected**—The wrong PIN was entered.<br>• **PIN2 rejected**—The wrong PIN was entered.<br>• **Network rejected** |
| **SIM lock** | Whether the SIM is locked or unlocked. See **SIM user operation needed** to determine if any action is required. |
| **SIM user operation needed** | Action required by the user. This can be one of the following:<br>• **No op**—No user operation required.<br>• **Enter PIN**—Enter the personal identification number (PIN) to unlock the SIM. See request modem wireless gsm sim-unlock.<br>• **Enter PUK**—Enter the PIN unblocking key (PUK) to unblock the SIM. See request modem wireless gsm sim-unblock. |

Copyright © 2013, Juniper Networks, Inc.

Table 54: show modem wireless interface firmware Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Retries remaining** | If the value of **SIM user operation needed** is **Enter PIN**, the number of PIN unlock attempts remaining before the modem is blocked. If the PIN is entered incorrectly three consecutive times, the SIM is blocked.<br><br>If the value of **SIM user operation needed** is **Enter PUK**, the number of unblock attempts remaining before the modem is unusable. If the PUK is entered incorrectly ten times, the SIM must be returned to the service provider for reactivation. |

## Sample Output

### show modem wireless interface firmware (CDMA EV-DO modem)

```
user@host> show modem wireless interface cl-0/0/8 firmware
Modem Firmware Version : p2005600
    Modem Firmware built date : 12-09-07
    Card type : Aircard 597E - CDMA EV-DO revA
    Manufacturer : Sierra Wireless, Inc.
    Hardware Version : 1.0
    Electronic Serial Number (ESN) : 0x6032688F
    Preferred Roaming List (PRL) Version : 20224
    Supported Mode : 1xev-do rev-a, 1x
    Current Modem Temperature : 32 C
    Modem Activated : YES
    Activation Date: 2-06-08
    Modem PIN Security : Unlocked
    Power-up lock : Disabled
```

## Sample Output

### show modem wireless interface firmware (GSM modem)

```
user@host> show modem wireless interface cl-0/0/8 firmware
  Wireless modem firmware details
   Modem firmware version: F1_2_3_15AP C:/WS/FW/F1_2_3_15AP/MSM7200R3/SRC/AMSS
2008/07/09 12:22:16
   Modem Firmware build date: 07/09/08
   Card type: Aircard 881E
   Modem manufacturer: Sierra Wireless, Inc
   Hardware version: 1.0
   Factory serial number (FSN): D46031813941022W
   Modem PIN security status: Disabled
   SIM status: Low Power
   SIM lock: Unlocked
   SIM user operation needed: No Op
   Retries remaining: 3
   Current modem temperature: 25 degrees Celsius
```


Copyright © 2013, Juniper Networks, Inc.

## show modem wireless interface network

**Syntax** **show modem wireless interface *interface-name* network**

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** Display wireless network statistics for 3G wireless modem interface.

**Options** **interface *interface-name***—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.

**Required Privilege Level** view

**Related Documentation**
- Modem Interfaces
- Interfaces for Security Devices

**List of Sample Output**
show modem wireless interface network (CDMA EV-DO modem) on page 1712
show modem wireless interface network (GSM modem) on page 1712

**Output Fields** Table 55 on page 1711 lists some of the output fields for the **show modem wireless interface network** command.

### Table 55: show modem wireless interface network Output Fields

| Field Name | Field Description |
|---|---|
| **System Identifier (SID)** | Current SID of the network providing service. |
| **Network Identifier (SID)** | Current NID of the station providing service. |
| **Roaming Status** | Roaming state. |
| **Current Modem Status** | Status of the 3G wireless modem card. The status can be one of the following states:<br>• **Offline**—Modem is not usable<br>• **Online**—Modem booted properly<br>• **Low Power**—Modem booted and in low power mode |
| **Current Service Status** | Status of the 3G wireless modem connection. The status can be one of the following states:<br>• **Offline**—Modem is not connected<br>• **Online**—Modem is connected |
| **Current Service Type** | One of the following:<br>• Circuit switched (CS)<br>• Packet switched (PS<br>• Combo (CS,PS) |

Copyright © 2013, Juniper Networks, Inc.

Table 55: show modem wireless interface network Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Current Service Mode** | One of the following:<br>• High-Speed Packet Access (HSPA)<br>• High-Speed Downlink Packet Access (HSDPA)<br>• High-Speed Uplink Packet Access (HSUPA) |
| **Current Band** | Current radio band in use. |
| **Mobile country Code (MCC)** | Number that uniquely identifies the country. |
| **Mobile Network Code** | Number that uniquely identifies a network within a country. |
| **System Identifier (SID)** | Current SID of the network providing service. |

## Sample Output

### show modem wireless interface network (CDMA EV-DO modem)

```
user@host> show modem wireless interface cl-0/0/8 network
Running Operating mode : 1xEV-DO (Rev A) and 1xRTT
 Call Setup Mode : Mobile IP only
 System Identifier (SID) : 3421
 Network Identifier (NID) : 91
 Roaming Status(1xRTT) : Home
 Idle Digital Mode : HDR
 System Time : Wed Jun6 15:16:9 2008
```

## Sample Output

### show modem wireless interface network (GSM modem)

```
user@host> show modem wireless interface cl-0/0/8 network
Wireless Modem Network Info
   Current Modem Status: Online
   Current Service Status: Offline
   Current Service Type: Combo(CS,PS)
   Current Service Mode: HSPA
   Current Band: 257
   Roaming Status: No
   Network Selection Mode: Automatic
   Network:
   Mobile Country Code (MCC): 1
   Mobile Network Code (MNC): 1
   Location Area Code (LAC): 128
   Routing Area Code (RAC): 0
   Cell Identification: 0
   Scrambling Code: 9
```


Copyright © 2013, Juniper Networks, Inc.

## show modem wireless interface rssi

**Syntax** **show modem wireless interface *interface-name* rssi**

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** Display received signal strength indication (RSSI) for 3G wireless modem interface.

**Options** **interface *interface-name***—The 3G wireless modem interface on the SRX210 device is **cl-0/0/8**.

**Required Privilege Level** view

**Related Documentation**
- Modem Interfaces
- Interfaces for Security Devices

**List of Sample Output** show modem wireless interface cl-0/0/8 rssi on page 1713

**Output Fields** Table 56 on page 1713 lists the output fields for the **show modem wireless interface rssi** command.

Table 56: show modem wireless interface rssi Output Fields

| Field Name | Field Description |
|---|---|
| **rssi** | Current RSSI, in decibels (dB). |

### Sample Output

show modem wireless interface cl-0/0/8 rssi

```
user@host> show modem wireless interface cl-0/0/8 rssi
Radio statistics
  Current radio signal strength: -95 dB
```

Copyright © 2013, Juniper Networks, Inc.

## show network-access address-assignment pool (View)

**Syntax** show network-access address-assignment pool *name*

**Release Information** Command introduced in Release 10.4 of Junos OS.

**Description** Display information summary about a specific pool.

**Required Privilege Level** view

**Output Fields** Table 57 on page 1714 lists the output fields for the **show network-access address-assignment pool** command. Output fields are listed in the approximate order in which they appear.

### Table 57: show network-access address-assignment pool Output Fields

| Field Name | Field Description |
|---|---|
| **IP address** | IP address assigned to a client. |
| **Hardware address** | MAC address of the client. For XAuth clients, the value is NA. |
| **Host/User** | For static IP address assignment, the user name and profile are displayed in the format *username*@*profile*. If the client is assigned an IP address from an address pool and a user name exists, the user name is displayed. For DHCP applications, if the host name is configured the host name is displayed; otherwise NA is displayed. |
| **Type** | Either XAuth or DHCP attributes are configured. |

### Sample Output

```
user@host> show network-access address-assignment pool xauth1
IP address       Hardware address       Host/User              Type
40.0.0.1         NA                     jason@dvpn-auth        XAUTH
40.0.0.2         NA                     jacky                  XAUTH
40.0.0.3         00:05:1b:00:b9:01      host1                  DHCP
40.0.0.4         00:05:1b:00:b9:02      NA                     DHCP
```


Copyright © 2013, Juniper Networks, Inc.

## show network-access requests pending

**Syntax**
**show** network-access requests pending
<**detail**>
<**index** *number* >

**Release Information** Command introduced in Release 8.5 of Junos OS.

**Description** Display the status of pending authentication requests.

**Options**
- none—Show pending authentication requests.
- **detail**—Display detailed information about all pending requests.
- **index** ***number*** —(Optional) Display detailed information about the request specified by this index number. Use the command without options to obtain a list of requests and index numbers.

**Required Privilege Level** view

**Related Documentation**
- clear network-access requests pending on page 1378

**List of Sample Output**
show network-access requests pending on page 1716
show network-access requests pending detail on page 1716
show network-access requests pending index 1 on page 1716

**Output Fields** Table 58 on page 1715 lists the output fields for the show network-access requests pending command. Output fields are listed in the approximate order in which they appear.

### Table 58: show network-access requests pending Output Fields

| Field Name | Field Description |
|---|---|
| **Index** | Internal number identifying the pending request. Use this number to obtain more information on the record. |
| **User** | Originator of authentication request. |
| **Status** | The pending requests are requests and responses that are not yet sent back to the respective clients. The pending requests can be in one of the following states:<br>• **Processing**: This request is being processed by the device. The authentication process has started but is not complete.<br>• **Waiting on Auth Server**: The request is sent to an external authentication server, and the device is waiting for the response.<br>• **Processed:** This request has completed authentication (success or failure). The results are not yet forwarded back to the client.<br>• **Request cancelled by Admin**: This request was cancelled by the Admin. The reply with cancel code is not yet sent back to the client. |

Copyright © 2013, Juniper Networks, Inc.

Table 58: show network-access requests pending Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Profile** | The profile determines how the user is authenticated.<br><br>Local clients defined with the statement **access profile client** are authenticated with the password authentication. Clients configured external to the device, on a RADIUS or LDAP server are authenticated with RADIUS or LDAP authentication. |

## Sample Output

show network-access requests pending

```
user@host> show network-access requests pending
Information about pending authentication entries
  Total pending authentication requests: 2
Index User                 Status
1     Sun                  Processing
2     Sam                  Processed
```

## Sample Output

show network-access requests pending detail

```
user@host> show network-access requests pending detail
Information about pending authentication entries
  Total pending authentication requests: 2
Index: 1  User: Sun
  Status: Processing
  Profile: Sunnyvale-firewall-users
Index: 2  User: Sam
  Status: Processed
  Profile: Westford-profile
```

## Sample Output

show network-access requests pending index 1

```
user@host> show network-access requests pending index 1
Index: 1  User: Sun
  Status: Processing
  Profile: Sunnyvale-firewall-users
```


Copyright © 2013, Juniper Networks, Inc.

## show network-access requests statistics

**Syntax** **show network-access requests statistics**

**Release Information** Command modified in Release 9.1 of Junos OS.

**Description** Display authentication statistics for the configured authentication type.

**Required Privilege Level** view

**Related Documentation**
- authentication-order (Access Profile) on page 12
- clear network-access requests statistics on page 1379

**Output Fields** Table 59 on page 1717 lists the output fields for the network-access requests statistics command. Output fields are listed in the approximate order in which they appear.

### Table 59: show network-access requests statistics Output Fields

| Field Name | Field Description |
|---|---|
| **Total requests received** | Total number of authentication requests that the device received from clients. |
| **Total responses sent** | Total number of authentication responses that the device sent to the clients. |
| **Success responses** | Total number of clients that authenticated successfully. |
| **Failure responses** | Total number of clients that failed to authenticate. |

## show network-access requests statistics

```
user@host> show network-access requests statistics
General authentication statistics
  Total requests received: 100
  Total responses sent: 70
Radius authentication statistics
  Total requests received: 40
  Success responses: 20
  Failure responses: 20
LDAP authentication statistics
  Total requests received: 30
  Success responses: 15
  Failure responses: 15
Local authentication statistics
  Total requests received: 5
  Success responses: 2
  Failure responses: 3
Securid authentication statistics
  Total requests received: 15
  Success responses: 3
  Failure responses: 12
```

Copyright © 2013, Juniper Networks, Inc.

## show network-access securid-node-secret-file

**Syntax** **show network-access securid-node-secret-file**

**Release Information** Command introduced in Release 9.1 of Junos OS.

**Description** Display the path to the node secret file for the SecurID authentication type.

**Required Privilege Level** view

**Related Documentation**
- configuration-file on page 17
- securid-server on page 44
- clear network-access securid-node-secret-file on page 1380

**List of Sample Output** show network-access securid-node-secret-file on page 1718

**Output Fields** Table 60 on page 1718 lists the output fields for the network-access securid-node-secret-file command. Output fields are listed in the approximate order in which they appear.

Table 60: show network-access securid-node-secret-file Output Fields

| Field Name | Field Description |
|---|---|
| **SecurID Server** | Name of the SecurID authentication server. |
| **Node Secret File** | Path to the node secret file. |

### Sample Output

show network-access securid-node-secret-file

```
user@host> show network-access securid-node-secret-file
SecurID server node secret file:
SecurID Server       Node Secret File
ace-server1          /var/db/securid/ace-server1/node-secret
```


Copyright © 2013, Juniper Networks, Inc.

## show oam ethernet connectivity-fault-management adjacencies

**Syntax** show oam ethernet connectivity-fault-management adjacencies <interface-name>

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Display connectivity-fault-management adjacencies.

**Options** **interface-name**—Dispalys the name of the interface.

**Required Privilege Level** view

**Related Documentation**
- Ethernet Port Switching for Security Devices

**List of Sample Output** show oam ethernet connectivity-fault- management adjacencies on page 1719

**Output Fields** Table 61 on page 1719 lists the output fields for the **show oam ethernet connectivity-fault-management adjacencies** command. Output fields are listed in the approximate order in which they appear

Table 61: show oam ethernet connectivity-fault-management adjacencies Output Fields

| Field Name | Field Description |
|---|---|
| Mep-id | Maintenance association end point (MEP) identifier. |
| Interface | Interface identifier. |
| State | Indicates if the connectivity check protocol is up. |
| Timer to Expire | Indicates the expiration time. |

### Sample Output

show oam ethernet connectivity-fault-management adjacencies

```
user@host> show oam ethernet connectivity-fault-management adjacencies
Mep-id     Interface        State        Timer to Expire
         101     fe-0/0/4.0         ok                 29
```

Copyright © 2013, Juniper Networks, Inc.

## show oam ethernet connectivity-fault-management forwarding-state

**Syntax** show oam ethernet connectivity-fault-management forwarding-state <interface>

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Display the Ethernet OAM forwarding state for received packets.

**Options** **<interface>**—Displays the Ethernet OAM state for an interface.

**Required Privilege Level** view

**Related Documentation**
- Ethernet Port Switching for Security Devices

**List of Sample Output** show oam ethernet connectivity-fault- management forwarding-state on page 1720

**Output Fields** Table 62 on page 1720 lists the output fields for the **show oam ethernet connectivity-fault-management forwarding-state** command. Output fields are listed in the approximate order in which they appear.

Table 62: show oam ethernet connectivity-fault-management forwarding-state Output Fields

| Field Name | Field Description |
|---|---|
| Interface name | Interface identifier. |
| Level | Maintenance domain level. |
| Direction | MEP direction configured. |
| Filter action | Filter action for messages at the level. |
| Nexthop type | Next-hop type. |
| Nexthop index | Next-hop index number. |

### Sample Output

show oam ethernet connectivity-fault-

```
user@host> show oam ethernet connectivity-fault-management forwarding-state interface
Interface name: ge-0/0/1.0 vlan:100
Instance name: INSTANCE_0 bd_vlan_100
```


Copyright © 2013, Juniper Networks, Inc.

### management forwarding-state

```
Maintenance domain forwarding state:

Level    Direction      Filter action     Nexthop       Nexthop
                                          type          index
0                       Drop              Discard
1                       Drop              Discard
2                       Drop              Discard
3                       Drop              Discard
4                       Drop              Discard
5                       Drop              Discard
6                       Drop              Discard
7        down           Receive           Receive
```

Copyright © 2013, Juniper Networks, Inc.

## show oam ethernet connectivity-fault-management interfaces

**Syntax** show oam ethernet connectivity-fault-management interfaces <interface name>

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Display Ethernet OAM information for the specified interface.

**Options** **<interface name>**—Displays connectivity fault management information for the specified interface.

**Required Privilege Level** view

**Related Documentation**
- Ethernet Port Switching for Security Devices

**List of Sample Output** show oam ethernet connectivity-fault- management interfaces on page 1722

**Output Fields** Table 63 on page 1722 lists the output fields for the **show oam ethernet connectivity-fault-management interfaces** command. Output fields are listed in the approximate order in which they appear.

Table 63: show oam ethernet connectivity-fault-management interfaces Output Fields

| Field Name | Field Description |
|---|---|
| Interfaces | Interface identifier. |
| Link | The local link status is Up, down, or oam-down. |
| Status | The status is active or inactive. |
| Level | Maintenance domain level configured. |
| MEP Identifier | Maintenance association end point (MEP) identifier. |
| Neighbors | Number of MEP neighbors. |

### Sample Output

**show oam ethernet connectivity-fault-management interfaces**

```
user@host> show oam ethernet connectivity-fault-management interfaces
Interfaces      Link      Status      Level      MEP         Neighbours
                                                Identifier

                ge-0/0/1.0      Up        Active       7           1000            0
```


Copyright © 2013, Juniper Networks, Inc.

## show oam ethernet connectivity-fault-management mep-database

**Syntax** show oam ethernet connectivity-fault-management mep-database

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Displays Ethernet OAM maintenance endpoint database information.

**Options** **<local-mep>**—Identifier for local maintenance endpoint (1 through 8191).

**maintenance-association** —Name of the maintenance association.

**maintenance-domain** —Name of the maintenance domain.

**remote-mep** —Identifier for remote maintenance endpoint (1 through 8191).

**Required Privilege Level** View

**Related Documentation**
- Ethernet Port Switching for Security Devices

**List of Sample Output** show oam ethernet connectivity-fault- management mep-database on page 1725

**Output Fields** Table 64 on page 1723 lists the output fields for the **show oam ethernet connectivity-fault-management mep-database** command. Output fields are listed in the approximate order in which they appear.

### Table 64: show oam ethernet connectivity-fault-management mep-database Output Fields

| Field Name | Field Description |
|---|---|
| Maintenance domain name | Maintenance domain name. |
| Format (Maintenance domain) | Maintenance domain name format configured. |
| Level | Maintenance domain level configured. |
| Maintenance association name | Maintenance association name. |
| Format (Maintenance association) | Maintenance association name format configured. |
| Continuity-check status | Continuity check status. |
| Interval | Continuity check message interval. |
| MEP identifier | Maintenance association end point (MEP) identifier. |
| Direction | MEP direction configured. |
| MAC address | MAC address configured for the MEP. |

Copyright © 2013, Juniper Networks, Inc.

Table 64: show oam ethernet connectivity-fault-management mep-database Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| Auto-discovery | Indicates whether automatic discovery is enabled or disabled. |
| Priority | Priority used for CCMs and linktrace messages transmitted by the MEP. |
| Interface name | Interface identifier. |
| Interface status | Local interface status. |
| Link status | Local link status. |
| Remote MEP not receiving CCM | Indicates that the remote MEP is not receiving CCMs. |
| Erroneous CCM received | Indicates that erroneous CCMs have been received. |
| Cross-connect CCM received | Indicates that cross-connect CCMs have been received. |
| RDI sent by some MEP | Indicates that the remote defect indication (RDI) bit is set in messages that have been received. The absence of the RDI bit in a CCM indicates that the transmitting MEP is receiving CCMs from all configured MEPs. |
| CCMs sent | Number of CCMs transmitted. |
| CCMs received out of sequence | Number of CCMs received out of sequence. |
| LBMs sent | Number of loopback messages (LBMs) sent. |
| Valid in-order LBRs received | Number of loopback response messages (LBRs) received that were valid messages and in sequence. |
| Valid out-of-order LBRs received | Number of LBRs received that were valid messages and not in sequence. |
| LBRs received with corrupted data | Number of LBRs received that were corrupted. |
| LBRs sent | Number of LBRs transmitted. |
| LTMs sent | Linktrace messages (LTMs) transmitted. |
| LTMs received | Linktrace messages received. |
| LTRs sent | Linktrace responses (LTRs) transmitted. |
| LTRs received | Linktrace responses received. |
| Sequence number of next LTM request | Sequence number of the next linktrace message request to be transmitted. |


Copyright © 2013, Juniper Networks, Inc.

Table 64: show oam ethernet connectivity-fault-management mep-database Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| 1DMs sent | If the MEP is an initiator for a one-way ETH-DM session, then this is the number of one-way delay measurement (1DM) PDU frames sent to the peer MEP in this session.<br><br>For all other cases, this field displays 0. |
| Valid 1DMs received | If the MEP is a receiver for a one-way ETH-DM session, then this is the number of valid 1DM frames received.<br><br>For all other cases, this field displays 0. |
| Invalid 1DMs received | If the MEP is a receiver for a one-way ETH-DM session, then this is the number of invalid 1DM frames received.<br><br>For all other cases, this field displays 0. |
| DMMs sent | If the MEP is an initiator for a two-way ETH-DM session, then this is the number of Delay Measurement Message (DMM) PDU frames sent to the peer MEP in this session. For all other cases, this field displays 0. |
| DMRs sent | If the MEP is a responder for a ETH-DM session, then this is the number of Delay Measurement Reply (DMR) frames sent.<br><br>For all other cases, this field displays 0. |
| Valid DMRs received | If the MEP is an initiator for a two-way ETH-DM session, then this is the number of valid DMRs received.<br><br>For all other cases, this field displays 0. |
| Invalid DMRs received | If the MEP is an initiator for a two-way ETH-DM session, then this is the number of invalid DMRs received.<br><br>For all other cases, this field displays 0. |

## Sample Output

### show oam ethernet connectivity-fault-

```
user@host> show oam ethernet connectivity-fault-management mep-database
maintenance-domain Customer1
Maintenance domain name: Customer1, Format: string, Level: 7
  Maintenance association name: Track_vlan_100, Format: string
```

management mep-database

```
Continuity-check status: enabled, Interval: 1s
MEP identifier: 1000, Direction: down, MAC address: 80:71:1f:ad:53:81
Auto-discovery: disabled, Priority: 0
Interface name: ge-0/0/1.0, Interface status: Active, Link status: Up
Defects:
  Remote MEP not receiving CCM                 : no
  Erroneous CCM received                       : no
  Cross-connect CCM received                   : no
  RDI sent by some MEP                         : no
Statistics:
  CCMs sent                                    : 170114
  CCMs received out of sequence                : 0
  LBMs sent                                    : 0
  Valid in-order LBRs received                 : 0
  Valid out-of-order LBRs received             : 0
  LBRs received with corrupted data            : 0
  LBRs sent                                    : 0
  LTMs sent                                    : 0
  LTMs received                                : 1
  LTRs sent                                    : 1
  LTRs received                                : 0
  Sequence number of next LTM request          : 0
  1DMs sent                                    : 0
  Valid 1DMs received                          : 0
  Invalid 1DMs received                        : 0
  DMMs sent                                    : 0
  DMRs sent                                    : 0
  Valid DMRs received                          : 0
  Invalid DMRs received                        : 0
```


Copyright © 2013, Juniper Networks, Inc.

## show oam ethernet connectivity-fault-management mep-statistics

**Syntax**

show oam ethernet connectivity-fault-management mep-statistics
count
local-mep
maintenance-association
maintenance-domain
remote-mep

**Release Information**

Statement introduced in Junos OS Release 12.1X44-D10.

**Description**

Display Ethernet OAM maintenance endpoint statistics.



NOTE: The delay measurement (DM) statistics are not valid for SRX Series devices, which supports only the IEEE 802.1ag standard.

**Options**

**count** —Number of statistics per maintenance endpoint (1 through 100).

**local-mep** —Identifier for local maintenance endpoint (1 through 8191).

**maintenance-association**—Name of maintenance association.

**maintenance-domain**—Name of maintenance domain.

**remote-mep** —Identifier for remote maintenance endpoint (1 through 8191).

**Required Privilege Level**

view

**Related Documentation**

- Ethernet Port Switching for Security Devices

**List of Sample Output**

show oam ethernet connectivity-fault- management mep-statistics on page 1729

**Output Fields**

Table 65 on page 1727 lists the output fields for the **show oam ethernet connectivity-fault-management mep-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 65: show oam ethernet connectivity-fault-management mep-statistics Output Fields

| Field Name | Field Description |
|---|---|
| MEP identifier | Maintenance association end point (MEP) identifier. |
| CCMs sent | Number of CCMs transmitted. |
| CCMs received out of sequence | Number of CCMs received out of sequence. |
| LBMs sent | Number of loopback messages (LBMs) sent. |

Copyright © 2013, Juniper Networks, Inc.

Table 65: show oam ethernet connectivity-fault-management mep-statistics Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| Valid in-order LBRs received | Number of loopback response messages (LBRs) received that were valid messages and in sequence. |
| Valid out-of-order LBRs received | Number of LBRs received that were valid messages and not in sequence. |
| LBRs received with corrupted data | Number of LBRs received that were corrupted. |
| LBRs sent | Number of LBRs transmitted. |
| LTMs sent | Linktrace messages (LTMs) transmitted. |
| LTMs received | Linktrace messages received. |
| LTRs sent | Linktrace responses (LTRs) transmitted. |
| LTRs received | Linktrace responses received. |
| Sequence number of next LTM request | Sequence number of the next linktracemessage request to be transmitted. |
| 1DMs sent | If the MEP is an initiator in a one-way ETH-DM session, then this is the number of one-way delay measurement (1DM) PDU frames sent to the peer MEP in this session.<br><br>For all other cases, this field displays 0. |
| Valid 1DMs received | If the MEP is a receiver for a one-way ETH-DM session, then this is the number of valid 1DM frames received.<br><br>For all other cases, this field displays 0. |
| Invalid 1DMs received | If the MEP is a receiver for a one-way ETH-DM session, then this is the number of invalid 1DM frames received.<br><br>For all other cases, this field displays 0. |
| DMMs sent | If the MEP is an initiator for a two-way ETH-DM session, then this is the number of Delay Measurement Message (DMM) PDU frames sent to the peer MEP in this session. For all other cases, this field displays 0. |
| DMRs sent | If the MEP is a responder for a ETH-DM session, then this is the number of Delay Measurement Reply (DMR) frames sent. For all other cases, this field displays 0. |
| Valid DMRs received | If the MEP is an initiator for a two-way ETH-DM session, then this is the number of valid DMRs received.<br><br>For all other cases, this field displays 0. |
| Invalid DMRs received | If the MEP is an initiator for a two-way ETH-DM session, then this is the number of invalid DMRs received.<br><br>For all other cases, this field displays 0. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show oam ethernet connectivity-fault-management mep-statistics

```
user@host> show oam ethernet connectivity-fault-management mep-statistics
maintenance-domain private maintenance-association private-ma remote-mep 100
MEP identifier: 101, MAC address: 80:71:1f:ad:53:81
  CCMs sent                                       : 83
  CCMs received out of sequence                   : 0
  LBMs sent                                       : 0
  Valid in-order LBRs received                    : 0
  Valid out-of-order LBRs received                : 0
  LBRs received with corrupted data               : 0
  LBRs sent                                       : 0
  LTMs sent                                       : 0
  LTMs received                                   : 0
  LTRs sent                                       : 0
  LTRs received                                   : 0
  Sequence number of next LTM request             : 0
  1DMs sent                                       : 0
  Valid 1DMs received                             : 0
  Invalid 1DMs received                           : 0
  DMMs sent                                       : 0
  DMRs sent                                       : 0
  Valid DMRs received                             : 0
  Invalid DMRs received                           : 0
```

Copyright © 2013, Juniper Networks, Inc.

## show oam ethernet connectivity-fault-management mip

**Syntax** show oam ethernet connectivity-fault-management mip
interface-name
vlan

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Display MIP information.

**Options** **interface-name** —Displays information of the specified logical interface.

**vlan**—Displays information about the specified VLAN (1 through 4094).

**Required Privilege Level** view

**Related Documentation**
- Ethernet Port Switching for Security Devices

**List of Sample Output** show oam ethernet connectivity-fault- management mip on page 1730

**Output Fields** Table 66 on page 1730 lists the output fields for the **show oam ethernet connectivity-fault-management mip** command. Output fields are listed in the approximate order in which they appear.

Table 66: show oam ethernet connectivity-fault-management mip Output Fields

| Field Name | Field Description |
|---|---|
| Default Maintenance-domain | The default maintenance domain name. |
| Interface | Interface identifier. |
| Level | Maintenance domain level configured. |

## Sample Output

show oam ethernet connectivity-fault-management mip

```
user@host> show oam ethernet connectivity-fault-management mip vlan 100
default maintenance-domain mhf    : default

  Interface       Level
  ge-0/0/1.0          5
  fe-0/0/4.0          5
```


Copyright © 2013, Juniper Networks, Inc.

## show oam ethernet connectivity-fault-management path-database

**Syntax**

show oam ethernet connectivity-fault-management path-database
<host>
maintenance-association
maintenance-domain

**Release Information**

Statement introduced in Junos OS Release 12.1X44-D10.

**Description**

Display the linktrace path-database for a remote host.

**Options**

**<host>**—MAC address of the remote host in xx:xx:xx:xx:xx:xx format.

**maintenance-association** —Name of the maintenance association.

**maintenance-domain** —Name of the maintenance domain.

**Required Privilege Level**

view

**Related Documentation**

- Ethernet Port Switching for Security Devices

**List of Sample Output**

show oam ethernet connectivity-fault- management path-database on page 1732

**Output Fields**

Table 67 on page 1731 lists the output fields for the **show oam ethernet connectivity-fault-management path-database** command. Output fields are listed in the approximate order in which they appear.

Table 67: show oam ethernet connectivity-fault-management path-database Output Fields

| Field Name | Field Description |
|---|---|
| Interface | Interface Identifier. |
| Maintenance Domain | Maintenance domain name. |
| Maintenance Association | Maintenance association name. |
| Level | Maintenance domain level configured for the maintenance domain. |
| Hop | Sequential hop count of the linktrace path. |
| TTL | Number of hops remaining in the linktrace message (LTM). The time to live (TTL) is decremented at each hop. |
| Source MAC Address | MAC address of the 802.1ag maintenance association intermediate point (MIP) that is forwarding the LTM. |
| Next-hop MAC Address | MAC address of the 802.1ag node that is the next hop in the LTM path. |

Copyright © 2013, Juniper Networks, Inc.

Table 67: show oam ethernet connectivity-fault-management path-database Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| Transaction Identifier | Identifier maintained by the MEP. Each LTM uses a transaction identifier. The transaction identifier is maintained globally across all maintenance domains. Use the transaction identifier to match an incoming linktrace response (LTR) with a previously sent LTM. |

## Sample Output

### show oam ethernet connectivity-fault-management path-database

```
user@host> show oam ethernet connectivity-fault-management path-database
Interface : fe-0/0/4
      Maintenance Domain: private, Level: 5
      Maintenance Association: private-ma, Local Mep: 100

    Hop   TTL    Source MAC address        Next-hop MAC address
    Transaction Identifier:0
    1     63     80:71:1f:ad:50:04         80:71:1f:ad:50:01
    2     62     80:71:1f:ad:53:81         00:00:00:00:00:00
    Transaction Identifier:1
    1     63     80:71:1f:ad:50:04         80:71:1f:ad:50:01
    2     62     80:71:1f:ad:53:81         00:00:00:00:00:00
    Transaction Identifier:2
    1     63     80:71:1f:ad:50:04         80:71:1f:ad:50:01
    2     62     80:71:1f:ad:53:81         00:00:00:00:00:00
    Transaction Identifier:3
    1     63     80:71:1f:ad:50:04         80:71:1f:ad:50:01
    2     62     80:71:1f:ad:53:81         00:00:00:00:00:00
```


Copyright © 2013, Juniper Networks, Inc.

## show oam ethernet connectivity-fault-management routes

**Syntax** show oam ethernet connectivity-fault-management routes

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Display connectivity-fault-management bridge routes.

**Required Privilege Level** view

**Related Documentation**
- Ethernet Port Switching for Security Devices

**List of Sample Output** show oam ethernet connectivity-fault- management routes on page 1734

**Output Fields** Table 68 on page 1733 lists the output fields for the **show oam ethernet connectivity-fault-management routes** command. Output fields are listed in the approximate order in which they appear.

Table 68: show oam ethernet connectivity-fault-management routes Output Fields

| Field Name | Field Description |
|---|---|
| VLAN | The configured VLAN interface. |
| MAC | MAC address configured for the route. |
| Next-hop index | Software index of the next hop that is used to route the traffic for a given prefix. |
| Action | The next-hop action. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show oam ethernet connectivity-fault-management routes

```
user@host> show oam ethernet connectivity-fault-management routes
VLAN                MAC                 Next-hop index  Action
vlan1               00:00:00:00:00:00           563             Flood
vlan1               01:80:c2:00:00:30                           Discard
vlan1               01:80:c2:00:00:31                           Discard
vlan1               01:80:c2:00:00:32                           Discard
vlan1               01:80:c2:00:00:33                           Discard
vlan1               01:80:c2:00:00:34                           Discard
vlan1               01:80:c2:00:00:35                           Receive
vlan1               01:80:c2:00:00:36           563             Flood
vlan1               01:80:c2:00:00:37           563             Flood
vlan1               01:80:c2:00:00:38                           Discard
vlan1               01:80:c2:00:00:39                           Discard
vlan1               01:80:c2:00:00:3a                           Discard
vlan1               01:80:c2:00:00:3b                           Discard
vlan1               01:80:c2:00:00:3c                           Discard
vlan1               01:80:c2:00:00:3d                           Receive
vlan1               01:80:c2:00:00:3e            563            Flood
vlan1               01:80:c2:00:00:3f            563            Flood
vlan2               00:00:00:00:00:00            563            Flood
```


Copyright © 2013, Juniper Networks, Inc.

## show oam ethernet link-fault-management

**Syntax**
show oam ethernet link-fault-management
<brief | detail>
*<interface-name>*

**Release Information**
Statement for branch SRX Series devices introduced in Junos OS Release 9.5.

**Description**
Display Operation, Administration, and Maintenance (OAM) link fault management (LFM) information for Ethernet interfaces.

**Options**
**brief | detail**—(Optional) Display the specified level of output.

***interface-name*** —(Optional) Display link fault management information for the specified Ethernet interface only.

**Required Privilege Level**
view

**Related Documentation**
- Ethernet Port Switching for Security Devices
- Understanding Ethernet OAM Link Fault Management for SRX Series Services Gateways
- Example: Configuring Ethernet OAM Link Fault Management

**List of Sample Output**
show oam ethernet link-fault-management brief on page 1739
show oam ethernet link-fault-management detail on page 1739

**Output Fields**
Table 69 on page 1735 lists the output fields for the **show oam ethernet link-fault-management** command. Output fields are listed in the approximate order in which they appear.

### Table 69: show oam ethernet link-fault-management Output Fields

| Field Name | Field Description | Level of Output |
|---|---|---|
| **Status** | Status of the established link.<br>• **Fail**—A link fault condition exists.<br>• **Running**—A link fault condition does not exist. | All levels |
| **Discovery state** | State of the discovery mechanism:<br>• **Passive Wait**<br>• **Send Any**<br>• **Send Local Remote**<br>• **Send Local Remote Ok** | All levels |
| **Peer address** | Address of the OAM peer. | All levels |

Copyright © 2013, Juniper Networks, Inc.

Table 69: show oam ethernet link-fault-management Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **Flags** | Information about the interface.<br>• **Remote-Stable**—Indicates remote OAM client acknowledgment of, and satisfaction with, local OAM state information. **False** indicates that remote DTE has either not seen or is unsatisfied with local state information. **True** indicates that remote DTE has seen and is satisfied with local state information.<br>• **Local-Stable**—Indicates local OAM client acknowledgment of, and satisfaction with, remote OAM state information. **False** indicates that local DTE either has not seen or is unsatisfied with remote state information. **True** indicates that local DTE has seen and is satisfied with remote state information.<br>• **Remote-State-Valid**—Indicates the OAM client has received remote state information found within local information TLVs (type, length, values) of received Information OAM PDUs. **False** indicates that the OAM client has not seen remote state information. **True** indicates that the OAM client has seen remote state information. | All levels |
| **Remote loopback status** | An OAM entity can put its remote peer into loopback mode using the Loopback control OAM PDU. In loopback mode, every frame received is transmitted back on the same port (except for OAM PDUs, which are needed to maintain the OAM session). | All levels |
| **Remote entity information** | Remote entity information.<br>• **Remote MUX action**—Indicates the state of the multiplexer functions of the OAM sublayer. Device is forwarding non-OAM PDUs to the lower sublayer or discarding non-OAM PDUs.<br>• **Remote parser action**—Indicates the state of the parser function of the OAM sublayer. Device is forwarding non-OAM PDUs to the higher sublayer, looping back non-OAM PDUs to the lower sublayer, or discarding non-OAM PDUs.<br>• **Discovery mode**—Indicates whether discovery mode is active or inactive.<br>• **Unidirectional mode**—Indicates the ability to operate a link in unidirectional mode for diagnostic purposes.<br>• **Remote loopback mode**—Indicates whether remote loopback is supported or not supported.<br>• **Link events**—Indicates whether interpreting link events is supported or not supported on the remote peer.<br>• **Variable requests**—Indicates whether variable requests are supported or not supported. The Variable Request OAM PDU, is used to request one or more MIB variables from the remote peer. | All levels |
| OAM Receive Statistics | | |
| **Information** | Number of information PDUs received. | **detail** |
| **Event** | Number of loopback control PDUs received. | **detail** |
| **Variable request** | Number of variable request PDUs received. | **detail** |
| **Variable response** | Number of variable response PDUs received. | **detail** |
| **Loopback control** | Number of loopback control PDUs received. | **detail** |


Copyright © 2013, Juniper Networks, Inc.

Table 69: show oam ethernet link-fault-management Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **Organization specific** | Number of vendor organization specific PDUs received. | **detail** |
| OAM Transmit Statistics | | |
| **Information** | Number of information PDUs transmitted. | **detail** |
| **Event** | Number of event notification PDUs transmitted. | **detail** |
| **Variable request** | Number of variable request PDUs transmitted. | **detail** |
| **Variable response** | Number of variable response PDUs transmitted. | **detail** |
| **Loopback control** | Number of loopback control PDUs transmitted. | **detail** |
| **Organization specific** | Number of vendor organization specific PDUs transmitted. | **detail** |
| OAM Received Symbol Error Event information | | |
| **Events** | Number of symbol error event TLVs that have been received after the OAM sublayer was reset. | **detail** |
| **Window** | Symbol error event window in the received PDU.<br><br>The protocol default value is the number of symbols that can be received in one second on the underlying physical layer. | **detail** |
| **Threshold** | Number of errored symbols in the period required for the event to be generated. | **detail** |
| **Errors in period** | Number of symbol errors in the period reported in the received event PDU. | **detail** |
| **Total errors** | Number of errored symbols that have been reported in received event TLVs after the OAM sublayer was reset.<br><br>Symbol errors are coding symbol errors. | **detail** |
| OAM Received Frame Error Event Information | | |
| **Events** | Number of errored frame event TLVs that have been received after the OAM sublayer was reset. | **detail** |
| **Window** | Duration of the window in terms of the number of 100 ms period intervals. | **detail** |
| **Threshold** | Number of detected errored frames required for the event to be generated. | **detail** |
| **Errors in period** | Number of detected errored frames in the period. | **detail** |

Copyright © 2013, Juniper Networks, Inc.

Table 69: show oam ethernet link-fault-management Output Fields *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **Total errors** | Number of errored frames that have been reported in received event TLVs after the OAM sublayer was reset.<br><br>A frame error is any frame error on the underlying physical layer. | **detail** |
| OAM Received Frame Period Error Event Information | | |
| **Events** | Number of frame seconds errors event TLVs that have been received after the OAM sublayer was reset. | **detail** |
| **Window** | Duration of the frame seconds window. | **detail** |
| **Threshold** | Number of frame seconds errors in the period. | **detail** |
| **Errors in period** | Number of frame seconds errors in the period. | **detail** |
| **Total errors** | Number of frame seconds errors that have been reported in received event TLVs after the OAM sublayer was reset. | **detail** |
| OAM Transmitted Symbol Error Event Information | | |
| **Events** | Number of symbol error event TLVs that have been transmitted after the OAM sublayer was reset. | **detail** |
| **Window** | The symbol error event window in the transmitted PDU. | **detail** |
| **Threshold** | Number of errored symbols in the period required for the event to be generated. | **detail** |
| **Errors in period** | Number of symbol errors in the period reported in the transmitted event PDU. | **detail** |
| **Total errors** | Number of errored symbols reported in event TLVs that have been transmitted after the OAM sublayer was reset. | **detail** |
| OAM Transmitted Frame Error Event Information | | |
| **Events** | Number of errored frame event TLVs that have been transmitted after the OAM sublayer was reset. | **detail** |
| **Window** | Duration of the window in terms of the number of 100-ms period intervals. | **detail** |
| **Threshold** | Number of detected errored frames required for the event to be generated. | **detail** |
| **Errors in period** | Number of detected errored frames in the period. | **detail** |
| **Total errors** | Number of errored frames that have been detected after the OAM sublayer was reset. | **detail** |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show oam ethernet link-fault-management brief

```
user@host> show oam ethernet link-fault-management brief
Interface: ge-0/0/1
  Status: Running, Discovery state: Send Any
  Peer address: 00:90:69:72:2c:83
  Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
  Remote loopback status: Disabled on local port, Enabled on peer port
  Remote entity information:
    Remote MUX action: discarding, Remote parser action: loopback
    Discovery mode: active, Unidirectional mode: unsupported
    Remote loopback mode: supported, Link events: supported
    Variable requests: unsupported
```

### show oam ethernet link-fault-management detail

```
user@host> show oam ethernet link-fault-management detail
  Interface: ge-0/0/1
    Status: Running, Discovery state: Send Any
    Peer address: 00:90:69:0a:07:14
    Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
    OAM receive statistics:
      Information: 186365, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 0, Organization specific: 0
    OAM transmit statistics:
      Information: 186347, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 0, Organization specific: 0
    OAM received symbol error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame period error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM transmitted symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM transmitted frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    Remote entity information:
      Remote MUX action: forwarding, Remote parser action: forwarding
      Discovery mode: active, Unidirectional mode: unsupported
      Remote loopback mode: supported, Link events: supported
      Variable requests: unsupported
```

Copyright © 2013, Juniper Networks, Inc.

## show poe controller (View)

**Syntax** show poe controller

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** Display the status of the Power over Ethernet (PoE) controller.

**Options** **none**—Display general parameters of the PoE software module controller.

**Required Privilege Level** View

**Related Documentation**
- Ethernet Interfaces
- Interfaces for Security Devices

**Output Fields** Table 70 on page 1740 lists the output fields for the **show poe controller** command. Output fields are listed in the approximate order in which they appear.

### Table 70: show poe controller Output Fields

| Field name | Field Description |
|---|---|
| Controller-index | Identifies the controller. |
| Maximum-power | Specifies the maximum power that can be provided by the SRX Series device to PoE ports. |
| Power-consumption | Specifies the total amount of power allocated to the PoE ports. |
| Guard-band | Shows the guard band configured on the controller. |
| Management | Shows the power management mode. |

## Sample Output

### show poe controller

**user@host>show poe controller**

```
Controller  Maximum   Power              Guard band  Management
index       power     consumption
   0        150.0 W    0.0 W               0 W         Static
```


Copyright © 2013, Juniper Networks, Inc.

## show poe interface (View)

**Syntax** show poe interface <ge-fpc/pic/port>

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** Display the status of Power over Ethernet (PoE) ports.

**Options**
- **none**—Display the status of all PoE ports on the SRX Series device.
- **ge-fpc/pic/port**— (Optional) Display the status of a specific PoE port on the SRX Series device.

**Required Privilege Level** View

**Related Documentation**
- Device and Routing Operations Monitoring

**Output Fields** Table 71 on page 1741 lists the output fields for the **show poe interface** command. Output fields are listed in the approximate order in which they appear.

### Table 71: show poe interface Output Fields

| Field name | Field Description |
|---|---|
| PoE Interface | Specifies the interface name. |
| Admin Status | Specifies whether PoE capabilities are enabled or disabled. |
| Oper status | Specifies the operational status of the port. |
| Max-power | Specifies the maximum power configured on the port. |
| Priority | Specifies whether the port is high priority or low priority. |
| Power-consumption | Specifies how much power is being used by the port. |
| Class | Indicates the class of the powered device as defined by the IEEE 802 AF standard. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show poe interface

user@host>show poe interface

```
Interface Admin status Oper status Max power Priority Power consumption Class
    ge-0/0/0 Enabled      Searching   15.4W     Low      0.0W                0
    ge-0/0/1 Enabled      Powered-up  15.4W     High     6.6W                0
    ge-0/0/2 Disabled     Disabled    15.4W     Low      0.0W                0
    ge-0/0/3 Disabled     Disabled    15.4W     Low      0.0W                0
```

user@host>show poe interface ge-0/0/1

```
PoE interface status :
PoE interface                :  ge-0/0/1
Administrative status        : Enabled
Operational status           : Powered-up
Power limit on the interface : 15.4 W
Priority                     : High
Power consumed               : 6.6 W
Class of power device        :   0
```


Copyright © 2013, Juniper Networks, Inc.

## show poe telemetries interface (View)

**Syntax** show poe telemetries interface ge-fpc/pic/port all | x

**Release Information** Command introduced in Release 9.5 of Junos OS.

**Description** Display a history of power consumption on the specified interface.

**Options**
- **ge-fpc/pic/port**—Display telemetries for the specified PoE interface.
- **all**—Display all telemetries records for the specified PoE interface.
- **x**—Display the specified number of telemetries records for the specified PoE interface.

**Required Privilege Level** View

**Related Documentation**
- Device and Routing Operations Monitoring

**Output Fields** Table 72 on page 1743 lists the output fields for the **show poe telemetries interface** command. Output fields are listed in the approximate order in which they appear.

### Table 72: show poe telemetries interface Output Fields

| Field name | Field Description |
|---|---|
| S1 No | Number of the record for the specified port. The last record is the most is the most recent. |
| Timestamp | Time that the power-consumption data was gathered. |
| Power | Amount of power provided by the specified port at the time the data was gathered. |
| Voltage | Voltage on the specified port at the time the data was gathered. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show poe telemetries interface

user@host>show poe telemetries interface ge-0/0/1 all

```
Sl No    Timestamp                Power    Voltage
   1     Fri Jan 04 11:41:15 2009 6.6 W    47.2 V
   2     Fri Jan 04 11:40:15 2009 6.6 W    47.2 V
   3     Fri Jan 04 11:39:15 2009 6.6 W    47.2 V
   4     Fri Jan 04 11:38:15 2009 6.6 W    47.2 V
   5     Fri Jan 04 11:37:15 2009 6.6 W    47.2 V
   6     Fri Jan 04 11:36:15 2009 6.6 W    47.2 V
   7     Fri Jan 04 11:35:15 2009 6.6 W    47.2 V
   8     Fri Jan 04 11:34:15 2009 6.6 W    47.2 V
```

user@host>show poe telemetries interface ge-0/0/1 5

```
Sl No    Timestamp                Power    Voltage
   1     Fri Jan 04 11:47:15 2009 6.6 W    47.2 V
   2     Fri Jan 04 11:38:15 2009 6.6 W    47.2 V
   3     Fri Jan 04 11:29:15 2009 6.6 W    47.2 V
   4     Fri Jan 04 11:11:15 2009 6.6 W    47.2 V
   5     Fri Jan 04 11:10:15 2009 6.6 W    47.2 V
```


Copyright © 2013, Juniper Networks, Inc.

## show pppoe interfaces

**Syntax**

show pppoe interfaces
<brief | detail | extensive>
<pp0.*logical*>

**Release Information**

For SRX100, SRX110, SRX210, SRX220, SRX240, and SRX650 devices, statement introduced in Release 9.5 of Junos OS.

**Description**

Display session-specific information about PPPoE interfaces.

**Options**

**none**—Display interface information for all PPPoE interfaces.

**brief | detail**—(Optional) Display the specified level of output.

**extensive**—(Optional) Display information about the number of packets sent and received and the number of timeouts during a PPPoE session.

**pp0.*logical***—(Optional) Name of an interface. The logical unit number for static interfaces can be a value from 0 through 16385. The logical unit number for dynamic interfaces can be a value from 1073741824 through the maximum number of logical interfaces supported on your SRX100, SRX110, SRX210, SRX220, SRX240, and SRX650 devices.

**Required Privilege Level**

view

**Related Documentation**

- Interfaces for Security Devices
- Device and Routing Operations Monitoring

**List of Sample Output**

show pppoe interfaces on page 1747
show pppoe interfaces brief on page 1747
show pppoe interfaces detail on page 1747
show pppoe interfaces extensive on page 1747

**Output Fields**

Table 73 on page 1745 lists the output fields for the **show pppoe interfaces** command. Output fields are listed in the approximate order in which they appear.

### Table 73: show pppoe interfaces Output Fields

| Field Name | Field Description |
|---|---|
| **Index** | Index number of the logical interface, which reflects its initialization sequence. |
| **State** | State of the logical interface: **up** or **down**. |
| **Session ID** | Session ID. |
| **Service name** | Type of service required (can be used to indicate an ISP name, a class, or quality of service). |

Copyright © 2013, Juniper Networks, Inc.

Table 73: show pppoe interfaces Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Configured AC name** | Configured access concentrator name. |
| **Session AC name** | Name of the access concentrator. |
| **Remote MAC address** or **Remote MAC** | MAC address of the remote side of the connection, either the access concentrator or the PPPoE client. |
| **Auto-reconnect timeout** | Timeout value for reconnecting after a PPPoE session is terminated (in seconds). |
| **Idle timeout** | Length of time (in seconds) that a connection can be idle before disconnecting. |
| **Session uptime** | Length of time the session has been up, in *hh:mm:ss*. |
| **Underlying interface** | Interface on which PPPoE is running. |
| **Packet Type** | Number of packets sent and received during the PPPoE session, categorized by packet type and packet errors:<br>• **PADI**—PPPoE Active Discovery Initiation packets.<br>• **PADO**—PPPoE Active Discovery Offer packets.<br>• **PADR**—PPPoE Active Discovery Request packets.<br>• **PADS**—PPPoE Active Discovery Session-Confirmation packets.<br>• **PADT**—PPPoE Active Discovery Termination packets.<br>• **Service name error**—Packets for which the Service-Name request could not be honored.<br>• **AC system error**—Packets for which the access concentrator experienced an error in performing the host request. For example, the host had insufficient resources to create a virtual circuit.<br>• **Generic error**—Packets that indicate an unrecoverable error occurred.<br>• **Malformed packets**—Malformed or short packets that caused the packet handler to discard the frame as unreadable.<br>• **Unknown packets**—Unrecognized packets. |
| **Timeout** | Timeouts that occur during the PPPoE session:<br>• **PADI**—No PADI packets received within the timeout period.<br>• **PADO**—No PADO packets received within the timeout period. (This value is always zero and is not supported.)<br>• **PADR**—No PADR packets received within the timeout period. |
| **Receive Error Counters** | Error counters received during the PPPoE session:<br>• **PADI**—No PADI error counters received during the session.<br>• **PADO**—No PADO error counters received during the session.<br>• **PADR**—No PADR error counters received during the session.<br>• **PADS**—No PADS error counters received during the session. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show pppoe interfaces

```
user@host> show pppoe interfaces
pp0.0 Index 71
  State: Session up, Session ID: 4,
  Service name: None,
  Session AC name: srx-pppoe-ac, Configured AC name: None,
  Remote MAC address: b0:c6:9a:74:5e:c1,
  Session uptime: 5d 15:21 ago,
  Auto-reconnect timeout: Never, Idle timeout: Never,
  Underlying interface: ge-0/0/1.0 Index 70
```

### show pppoe interfaces brief

```
user@host> show pppoe interfaces brief
Interface       Underlying            State       Session    Remote
                interface                         ID         MAC
pp0.0           ge-0/0/1.0            Session up  4          b0:c6:9a:74:5e:c1
```

### show pppoe interfaces detail

```
user@host> show pppoe interfaces detail
pp0.0 Index 71
  State: Session up, Session ID: 4,
  Service name: None,
  Session AC name: srx-pppoe-ac, Configured AC name: None,
  Remote MAC address: b0:c6:9a:74:5e:c1,
  Session uptime: 5d 15:21 ago,
  Auto-reconnect timeout: Never, Idle timeout: Never,
  Underlying interface: ge-0/0/1.0 Index 70
```

### show pppoe interfaces extensive

```
user@host> show pppoe interfaces extensive
pp0.0 Index 71
  State: Session up, Session ID: 4,
  Service name: None,
  Session AC name: srx-pppoe-ac, Configured AC name: None,
  Remote MAC address: b0:c6:9a:74:5e:c1,
  Session uptime: 5d 15:22 ago,
  Auto-reconnect timeout: Never, Idle timeout: Never,
  Underlying interface: ge-0/0/1.0 Index 70
  PacketType                      Sent         Received
    PADI                             1                0
    PADO                             0                1
    PADR                             1                0
    PADS                             0                1
    PADT                             0                0
    Service name error               0                0
    AC system error                  0                0
    Generic error                    0                0
    Malformed packets                0                0
    Unknown packets                  0                0
  Timeout
    PADI                             0
    PADO                             0
    PADR                             0
  Receive Error Counters
    PADI                             0
    PADO                             0
    PADR                             0
    PADS                             0
```

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

## show pppoe statistics

**Syntax**
show pppoe statistics
<*logical-interface-name*>

**Release Information**
For SRX100, SRX110, SRX210, SRX220, SRX240, and SRX650 devices, statement introduced in Release 9.5 of Junos OS.

**Description**
Display statistics information about PPPoE interfaces.

**Options**
**none**—Display PPPoE statistics for all interfaces.

***logical-interface-name***—(Optional) Name of an underlying PPPoE logical interface.

**Required Privilege Level**
view

**Related Documentation**
- show pppoe interfaces on page 1745
- Interfaces for Security Devices
- Device and Routing Operations Monitoring

**List of Sample Output**
show pppoe statistics on page 1750

**Output Fields**
Table 74 on page 1749 lists the output fields for the **show pppoe statistics** command. Output fields are listed in the approximate order in which they appear.

### Table 74: show pppoe statistics Output Fields

| Field Name | Field Description |
|---|---|
| **Active PPPoE sessions** | Total number of active PPPoE sessions. |
| **Packet Type** | Number of packets sent and received during the PPPoE session, categorized by packet type and packet errors:<br>• **PADI**—PPPoE Active Discovery Initiation packets.<br>• **PADO**—PPPoE Active Discovery Offer packets.<br>• **PADR**—PPPoE Active Discovery Request packets.<br>• **PADS**—PPPoE Active Discovery Session-Confirmation packets.<br>• **PADT**—PPPoE Active Discovery Termination packets.<br>• **Service name error**—Packets for which the Service-Name request could not be honored.<br>• **AC system error**—Packets for which the access concentrator experienced an error in performing the host request. For example, the host had insufficient resources to create a virtual circuit.<br>• **Generic error**—Packets that indicate an unrecoverable error occurred.<br>• **Malformed packets**—Malformed or short packets that caused the packet handler to discard the frame as unreadable.<br>• **Unknown packets**—Unrecognized packets. |

Copyright © 2013, Juniper Networks, Inc.

Table 74: show pppoe statistics Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Timeout** | Timeouts that occur during the PPPoE session:<br>• **PADI**—No PADI packets received within the timeout period.<br>• **PADO**—No PADO packets received within the timeout period. (This value is always zero and is not supported.)<br>• **PADR**—No PADR packets received within the timeout period. |
| **Receive Error Counters** | Error counters received during the PPPoE session:<br>• **PADI**—No PADI error counters received during the session.<br>• **PADO**—No PADO error counters received during the session.<br>• **PADR**—No PADR error counters received during the session.<br>• **PADS**—No PADS error counters received during the session. |

## Sample Output

### show pppoe statistics

```
user@host> show pppoe statistics
Active PPPoE sessions: 0

  PacketType                       Sent         Received
    PADI                              0                0
    PADO                              0                0
    PADR                              0                0
    PADS                              0                0
    PADT                              0                0
    Service name error                0                0
    AC system error                   0                0
    Generic error                     0                0
    Malformed packets                 0                0
    Unknown packets                   0                0
  Timeout
    PADI                              0
    PADO                              0
    PADR                              0
  Receive Error Counters
    PADI                              0
    PADO                              0
    PADR                              0
    PADS                              0
```


Copyright © 2013, Juniper Networks, Inc.

## show schedulers

**Syntax**
**show schedulers**
**< scheduler-name** ***scheduler-name*** **>**

**Release Information**
Command introduced in Release 8.5 of Junos OS. **Description** output field added in Release 12.1 of Junos OS.

**Description**
Display information about security policy schedulers configured on the system. If a specific scheduler is identified, detailed information is displayed for that scheduler only.

**Options**
- none—Display information for all configured schedulers.
- **scheduler-name** ***scheduler-name*** —(Optional) Display information for a particular scheduler.

**Required Privilege Level**
view

**Related Documentation**
- schedulers (Security Policies) on page 306

**List of Sample Output**
show schedulers on page 1752
show schedulers scheduler-name sch20 on page 1752

**Output Fields**
Table 75 on page 1751 lists the output fields for the **show schedulers** command. Output fields are listed in the approximate order in which they appear.

### Table 75: show schedulers Output Fields

| Field Name | Field Description |
|---|---|
| **Scheduler name** | Name of the scheduler. |
| **State** | Status of the scheduler:<br>• **active**—The scheduler is associated with one or more policies. If active:<br>  ◦ **Next deactivation**—Date and time when the policies with which the scheduler is associated are to be deactivated.<br>• **inactive**—The scheduler is associated with one or more policies. If inactive:<br>  ◦ **Next activation**—Date and time when the associated policies are to be activated.<br>• **unused**—The scheduler is not associated with any policy, or it is past the stop date and no future activity is required. |
| **Description** | Description of the scheduler. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show schedulers

```
user@host> show schedulers
Scheduler name: s1, State: unused
  Description: The scheduler s1 is for the sales team
  Scheduler name: sch1, State: inactive
  Description: The scheduler sch1 is for the sales team
  Next activation: Thu Feb 15 00:00:00 2007
  Scheduler name: sch10, State: unused
  Description: The scheduler sch10 is for the sales team
  Scheduler name: sch20, State: active
  Description: The scheduler sch20 is for the sales team
  Next deactivation: Thu Feb 15 00:00:00 2007
```

## Sample Output

show schedulers scheduler-name sch20

```
user@host> show schedulers scheduler-name sch20
Scheduler name: sch20, State: active
  Description: The scheduler sch20 is for the sales team
  Next deactivation: Thu Feb 15 00:00:00 2007
```


Copyright © 2013, Juniper Networks, Inc.

## show security alarms

**Syntax** show security alarms
<detail>
<alarm-id *id-number*>
<alarm-type [ *types* ]>
<newer-than *YYYY-MM-DD.HH:MM:SS*>
<older-than *YYYY-MM-DD.HH:MM:SS*>
<process *process*>
<severity *severity*>

**Release Information** Command introduced in Junos OS Release 11.2.

**Description** Display the alarms that are active on the device. Run this command when the CLI prompt indicates that a security alarm has been raised, as shown here:

```
[1 SECURITY ALARM] user@host#
```

**Options** **none**—Display all active alarms.

**detail**—(Optional) Display detailed output.

**alarm-id *id-number***—(Optional) Display the specified alarm.

**alarm-type [ *types* ]**—(Optional) Display the specified alarm type or a set of types. You can specify one or more of the following alarm types:

- **authentication**
- **cryptographic-self-test**
- **decryption-failures**
- **encryption-failures**
- **ike-phase1-failures**
- **ike-phase2-failures**
- **key-generation-self-test**
- **non-cryptographic-self-test**
- **policy**
- **replay-attacks**

**newer-than *YYYY-MM-DD.HH:MM:SS***—(Optional) Display active alarms that were raised after the specified date and time.

**older-than *YYYY-MM-DD.HH:MM:SS***—(Optional) Display active alarms that were raised before the specified date and time.

**process *process***—(Optional) Display active alarms that were raised by the specified system process.

Copyright © 2013, Juniper Networks, Inc.

**severity *severity***—(Optional) Display active alarms of the specified severity.

You can specify the following severity levels:

- **alert**
- **crit**
- **debug**
- **emerg**
- **err**
- **info**
- **notice**
- **warning**

**Required Privilege Level**

security—To view this statement in the configuration.

**Related Documentation**

- clear security alarms on page 1383
- Security Policies for Security Devices
- Device and Routing Operations Monitoring
- Troubleshooting for Security Devices

**List of Sample Output**

show security alarms on page 1756
show security alarms detail on page 1756
show security alarms alarm-id on page 1756
show security alarms alarm-type authentication on page 1756
show security alarms newer-than <time> on page 1756
show security alarms older-than <time> on page 1757
show security alarms process <process> on page 1757
show security alarms severity <severity> on page 1757

**Output Fields**

Table 76 on page 1754 lists the output fields for the **show security alarms** command. Output fields are listed in the approximate order in which they appear. Field names might be abbreviated (as shown in parentheses) when no level of output is specified or when the **detail** keyword is used.

Table 76: show security alarms

| Field Name | Field Description | Level of Output |
|---|---|---|
| **ID** | Identification number of the alarm. | All levels |
| **Alarm time** | Date and time the alarm was raised.. | All levels |
| **Message** | Information about the alarm, including the alarm type, username, IP address, and port number. | All levels |


Copyright © 2013, Juniper Networks, Inc.

Table 76: show security alarms *(continued)*

| Field Name | Field Description | Level of Output |
|---|---|---|
| **Process** | System process (For example, login or sshd) and process identification number associated with the alarm. | **detail** |
| **Severity** | Severity level of the alarm. | **detail** |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security alarms

```
[3 SECURITY ALARMS] user@router> show security alarms

ID    Alarm time               Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
2     2010-01-19 13:41:52 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
3     2010-01-19 13:42:13 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
```

### show security alarms detail

```
[3 SECURITY ALARMS] user@router> show security alarms detail

Alarm ID   : 1
Alarm Type : authentication
Time       : 2010-01-19 13:41:36 PST
Message    : SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for
 user 'user' reached from '10.17.0.1'
Process    : sshd (pid 1414)
Severity   : notice

Alarm ID   : 2
Alarm Type : authentication
Time       : 2010-01-19 13:41:52 PST
Message    : SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for
 user 'user' reached from '10.17.0.1'
Process    : sshd (pid 1414)
Severity   : notice

Alarm ID   : 3
Alarm Type : authentication
Time       : 2010-01-19 13:42:13 PST
Message    : SSHD_LOGIN_FAILED_LIMIT: Specified number of login failures (1) for
 user 'user' reached from '10.17.0.1'
Process    : sshd (pid 1414)
Severity   : notice
```

### show security alarms alarm-id

```
[3 SECURITY ALARMS] user@router> show security alarms alarm-id 1

ID    Alarm time               Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
```

### show security alarms alarm-type authentication

```
[3 SECURITY ALARMS] user@router> show security alarms alarm-type authentication

ID    Alarm time               Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
2     2010-01-19 13:41:52 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
3     2010-01-19 13:42:13 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
```

### show security alarms

```
[3 SECURITY ALARMS] user@router> show security alarms newer-than 2010-01-19.13:41:59
```


Copyright © 2013, Juniper Networks, Inc.

newer-than <time>

```
3     2010-01-19 13:42:13 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
```

show security alarms older-than <time>

```
[3 SECURITY ALARMS] user@router> show security alarms older-than 2010-01-19.13:41:59

ID    Alarm time               Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
2     2010-01-19 13:41:52 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
```

show security alarms process <process>

```
[3 SECURITY ALARMS] user@router> show security alarms process sshd

ID    Alarm time               Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
2     2010-01-19 13:41:52 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
3     2010-01-19 13:42:13 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
```

show security alarms severity <severity>

```
[3 SECURITY ALARMS] user@router> show security alarms severity notice

ID    Alarm time               Message
1     2010-01-19 13:41:36 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
2     2010-01-19 13:41:52 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
3     2010-01-19 13:42:13 PST  SSHD_LOGIN_FAILED_LIMIT: Specified number of login
 failures (1) for user 'user' reached from '10.17.0.1'
```

Copyright © 2013, Juniper Networks, Inc.

## show security alg h323 counters

**Syntax** **show security alg h323 counters**
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Display H.323 Application Layer Gateway (ALG) counters information.

**Options**

- none—Display H.323 ALG counters. information.
- **node**—(Optional) For chassis cluster configurations, display H.323 counters on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**

- h323 on page 631
- clear security alg h323 counters on page 1386
- H.323 ALGs for Security Devices

**List of Sample Output** show security alg h323 counters on page 1759

**Output Fields** Table 77 on page 1758 lists the output fields for the **show security alg h323 counters** command. Output fields are listed in the approximate order in which they appear.

### Table 77: show security alg h323 counters Output Fields

| Field Name | Field Description |
|---|---|
| **Packets received** | Number of H.323 ALG packets received. |
| **Packets dropped** | Number of H.323 ALG packets dropped. |
| **RAS message received** | Number of incoming RAS (Endpoint Registration, Admission, and Status) messages per second per gatekeeper received and processed. |
| **Q.931 message received** | Counter for Q.931 message received. |
| **H.245 message received** | Counter for H.245 message received. |


Copyright © 2013, Juniper Networks, Inc.

Table 77: show security alg h323 counters Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Number of calls** | Total number of H.323 ALG calls.<br>NOTE:<br>This counter displays the number of call legs and may not display the exact number of voice calls that are active. For instance, for a single active voice call between two endpoints, this counter might display a value of **2**. |
| **Number of active calls** | Number of active H.323 ALG calls. |
| **Decoding errors** | Number of decoding errors. |
| **Message flood dropped** | Error counter for message flood dropped. |
| **NAT errors** | H.323 ALG Network Address Translation (NAT) errors. |
| **Resource manager errors** | H.323 ALG resource manager errors. |

## Sample Output

### show security alg h323 counters

```
user@host> show security alg h323 counters
H.323 counters summary:
Packets received           :4060
Packets dropped            :24
RAS message received       :3690
Q.931 message received       :202
H.245 message received       :145
Number of calls        :25
Number of active calls       :0
H.323 Error Counters:
Decoding errors            :24
Message flood dropped       :0
NAT errors           :0
Resource manager errors       :0
H.323 Message Counters:
RRQ      : 431   RCF      :  49 ARQ  : 60  ACF      : 33
URQ      : 34   UCF      : 25 DRQ  : 55  DCF      : 44
oth RAS  : 2942  Setup    : 28 Alert    : 9 Connect    : 25
CallPrcd  : 18  Info    : 0  RelCmpl  : 39  Facility   : 14
Progress  : 0  Empty    : 65  OLC      : 20 OLC-ACK  :   20
oth H245  : 16
```

Copyright © 2013, Juniper Networks, Inc.

## show security alg ike-esp-nat summary

**Syntax** **show security alg ike-esp-nat summary**

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display Application Layer Gateway (ALG) for IKE and ESP information summary.

**Required Privilege Level** view

**Related Documentation**
- clear security alg ike-esp-nat on page 1387

**List of Sample Output** show security alg ike-esp-nat summary on page 1760

### Sample Output

show security alg ike-esp-nat summary

```
user@host> security alg ike-esp-nat summary
Initiator cookie: d5732d9b4114de1a
Responder cookie: 4776fe31164ef
Session-ID:       13
ALG state :       1
Timeout:          6292
Used IKE cookies: 0
Maximum IKE cookies: 2400
```


Copyright © 2013, Juniper Networks, Inc.

## show security alg mgcp calls

**Syntax**

**show security alg mgcp calls**
<endpoint *endpoint-name* | node ( *node-id* | all | local | primary)>

**Release Information**

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description**

Display information about Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG) calls.

**Options**

- none—Display all MGCP ALG calls.
- **endpoint** ***endpoint-name*** —(Optional) Display information about the endpoints of each MGCP ALG call.
- **node**—(Optional) For chassis cluster configurations, display MGCP calls on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level**

view

**Related Documentation**

- mgcp on page 757
- clear security alg mgcp calls on page 1388
- MGCP ALGs for Security Devices
- Device and Routing Operations Monitoring

**List of Sample Output**

show security alg mgcp calls on page 1762
show security alg mgcp calls endpoint on page 1762

**Output Fields**

Table 78 on page 1761 lists the output fields for the **show security alg mgcp calls** command. Output fields are listed in the approximate order in which they appear.

### Table 78: show security alg mgcp calls Output Fields

| Field Name | Field Description |
|---|---|
| **Connection ID** | Connection identifier for MGCP ALG calls. |
| **Local SDP** | MGCP ALG call local owner IP address as per the Session Description Protocol (SDP). |
| **Remote SDP** | MGCP ALG call remote owner IP address as per the Session Description Protocol (SDP). |

Copyright © 2013, Juniper Networks, Inc.

Table 78: show security alg mgcp calls Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **RM Group** | Resource manager group ID. |
| **Notified entity** | The certificate authority (CA) currently controlling the gateway. |

## Sample Output

### show security alg mgcp calls

```
user@host> show security alg mgcp calls
Endpoint@GW        Zone         Call ID                   RM Group
d001@101.50.10.1        Trust        10d55b81140e0f76          512
Connection Id> 0
Local SDP>   o: 101.50.10.1               x_o: 101.50.10.1
c: 101.50.10.1/32206          x_c: 101.50.10.1/32206
Remote SDP>  c: 3.3.3.5/16928             x_c: 3.3.3.5/16928
Endpoint@GW        Zone         Call ID                   RM Group
d001@3.3.3.5        Untrust      3a104e9b41a7c4c9          511
Connection Id> 0
Local SDP>   o: 3.3.3.5                   x_o: 3.3.3.5
c: 3.3.3.5/16928              x_c: 3.3.3.5/16928
Remote SDP>  c: 101.50.10.1/32206         x_c: 101.50.10.1/32206
```

## Sample Output

### show security alg mgcp calls endpoint

```
user@host> show security alg mgcp calls endpoint
Gateway: 101.50.10.1     Zone: Trust       IP: 101.50.10.1 -> 101.50.10.1
   Endpoint             Trans #  Call #   Notified Entity
   d001                 1        1        0.0.0.0/0->0.0.0.0/0
Gateway: 3.3.3.5      Zone: Untrust      IP: 3.3.3.5 -> 3.3.3.5
   Endpoint             Trans #  Call #   Notified Entity
   d001                 1        1        0.0.0.0/0->0.0.0.0/0
```


Copyright © 2013, Juniper Networks, Inc.

## show security alg mgcp counters

**Syntax** **show security alg mgcp counters**
<node ( *node-id* | all | local | primary)>

**Release Information** Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Display Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG) counters information.

**Options**
- none—Display MGCP ALG counters information.
- **node**—(Optional) For chassis cluster configurations, display MGCP counters on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**
- mgcp on page 757
- clear security alg mgcp counters on page 1389
- MGCP ALGs for Security Devices
- Device and Routing Operations Monitoring

**List of Sample Output** show security alg mgcp counters on page 1765

**Output Fields** Table 79 on page 1763 lists the output fields for the **show security alg mgcp counters** command. Output fields are listed in the approximate order in which they appear.

### Table 79: show security alg mgcp counters Output Fields

| Field Name | Field Description |
|---|---|
| **Packets received** | Number of MGCP ALG packets received. |
| **Packets dropped** | Number of MGCP ALG packets dropped. |
| **Message received** | Number of MGCP ALG messages received. |
| **Number of connections** | Number of MGCP ALG connections. |
| **Number of active connections** | Number of active MGCP ALG connections. |

Copyright © 2013, Juniper Networks, Inc.

Table 79: show security alg mgcp counters Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Number of calls** | Number of MGCP ALG calls. |
| **Number of active calls** | Number of MGCP ALG active calls. |
| **Number of active transactions** | Number of active transactions. |
| **Number of re-transmission** | Number of MGCP ALG retransmissions. |
| **Unknown-method** | MGCP ALG unknown method errors. |
| **Decoding error** | MGCP ALG decoding errors. |
| **Transaction error** | MGCP ALG transaction errors. |
| **Call error** | MGCP ALG counter errors. |
| **Connection error** | MGCP ALG connection errors. |
| **Connection flood drop** | MGCP ALG connection flood drop errors. |
| **Message flood drop** | MGCP ALG message flood drop error. |
| **IP resolve error** | MGCP ALG IP address resolution errors. |
| **NAT error** | MGCP ALG Network Address Translation (NAT) errors. |
| **Resource manager error** | MGCP ALG resource manager errors. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security alg mgcp counters

```
user@host> show security alg mgcp counters
MGCP counters summary:
Packets received            :284
Packets dropped             :0
Message received            :284
Number of connections           :4
Number of active connections :3
Number of calls            :4
Number of active calls            :3
Number of transactions            :121
Number of active transactions:52
Number of re-transmission    :68
MGCP Error Counters:
Unknown-method            :0
Decoding error            :0
Transaction error            :0
Call error            :0
Connection error            :0
Connection flood drop            :0
Message flood drop            :0
IP resolve error            :0
NAT error            :0
Resource manager error            :0
MGCP Packet Counters:
CRCX   :4   MDCX     :9   DLCX     :2
AUEP   :1    AUCX     :0   NTFY     :43
RSIP   :79    EPCF     :0   RQNT     :51
000-199  :0     200-299  :95    300-999  :0
```

Copyright © 2013, Juniper Networks, Inc.

## show security alg mgcp endpoints

**Syntax**

**show security alg mgcp endpoints**
< *endpoint name* >
<node ( *node-id* | all | local | primary)>

**Release Information**

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description**

Display information about Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG) endpoints.

**Options**

- none—Display MGCP ALG endpoints information.
- ***endpoint-name*** —(Optional) Display information about the specified MGCP ALG endpoint.
- **node**—(Optional) For chassis cluster configurations, display MGCP endpoints on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level**

view

**Related Documentation**

- mgcp on page 757
- MGCP ALGs for Security Devices
- Device and Routing Operations Monitoring

**List of Sample Output**

show security alg mgcp endpoints on page 1767
show security alg mgcp endpoints d001@100.100.100.152 on page 1767

**Output Fields**

Table 80 on page 1766 lists the output fields for the **show security alg mgcp endpoints** command. Output fields are listed in the approximate order in which they appear.

### Table 80: show security alg mgcp endpoints Output Fields

| Field Name | Field Description |
|---|---|
| **Gateway** | IP address of the gateway. |
| **Zone** | Gateway zone ID. |
| **Endpoint** | Endpoint name. |
| **Trans #** | Transaction ID. |


Copyright © 2013, Juniper Networks, Inc.

Table 80: show security alg mgcp endpoints Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Call #** | Call ID. |
| **Notified entity** | The certificate authority (CA) currently controlling the gateway. |

## Sample Output

### show security alg mgcp endpoints

```
user@host> show security alg mgcp endpoints
Gateway: 100.100.100.152     Zone: z0             IP: 100.100.100.152 ->
100.100.100.152
  Endpoint          Trans #   Call #   Notified entity
  d001              3         1        0.0.0.0:0 -> 0.0.0.0:0
```

## Sample Output

### show security alg mgcp endpoints d001@100.100.100.152

```
user@host> show security alg mgcp endpoints d001@100.100.100.152
Gateway: 100.100.100.152     Zone: z0             IP: 100.100.100.152 ->
100.100.100.152
  Endpoint          Trans #   Call #   Notified entity
  d001              12        2        0.0.0.0:0 -> 0.0.0.0:0
```

Copyright © 2013, Juniper Networks, Inc.

## show security alg msrpc

**Syntax** **show security alg msrpc**
**<object-id-map> <node ( *node-id* | all | local | primary)>**

**Release Information** Command updated in Release 10.1 of Junos OS.

**Description** Display Microsoft (MS) remote procedure call (RPC) Application Layer Gateway (ALG) information.

**Options**

- none—Display all MSRPC ID (UUID) to object ID (OID) table information.
- **object-id-map**—(Optional) Display information from the MSRPC ID (UUID) to object ID (OID) table.
- **node**—(Optional) For chassis cluster configurations, display MSRPC UUID-to-object-ID mapping information on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**

- msrpc on page 765
- RPC ALGs for Security Devices

**List of Sample Output** show security alg msrpc object-id-map on page 1769

**Output Fields** Table 81 on page 1768 lists the output fields for the **show security alg msrpc** command. Output fields are listed in the approximate order in which they appear.

### Table 81: show security alg msrpc Output Fields

| Field Name | Field Description |
|---|---|
| UUID | MS RPC ID. |
| OID | MS RPC object ID. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security alg msrpc object-id-map

```
user@host> show security alg msrpc object-id-map
UUID                                 OID
1be617c0-31a5-11cf-a7d8-00805f48a135 0x80000020
e3514235-4b06-11d1-ab04-00c04fc2dcd2 0x80000002
67df7c70-0f04-11ce-b13f-00aa003bac6c 0x80000014
```

## show security alg sccp calls

**Syntax**

**show security alg sccp calls**
< **brief** | **detail** | node ( *node-id* | all | local | primary) >

**Release Information**

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description**

Display information about Skinny Client Control Protocol (SCCP) Application Layer Gateway (ALG) calls.

**Options**

- none | **brief**—Display brief call information.
- **detail**—(Optional) Display detailed call information.
- **node**—(Optional) For chassis cluster configurations, display SCCP calls on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level**

view

**Related Documentation**

- sccp on page 914
- clear security alg sccp calls on page 1390
- SCCP ALGs for Security Devices
- Device and Routing Operations Monitoring

**List of Sample Output**

show security alg sccp calls on page 1771
show security alg sccp calls detail on page 1771

**Output Fields**

Table 82 on page 1770 lists the output fields for the **show security alg sccp calls** command. Output fields are listed in the approximate order in which they appear.

### Table 82: show security alg sccp calls Output Fields

| Field Name | Field Description |
|---|---|
| **Client IP address** | IP address of the client. |
| **Client zone** | Client zone ID. |
| **Call manager** | IP address of the call manager. |
| **Resource manager group** | Resource manager group ID. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security alg sccp calls

```
user@host> show security alg sccp calls
Client IP          Zone      CallManager       Conference ID  RM group
11.0.102.91        7         13.0.99.226       16789504       2047
12.0.102.96        8         13.0.99.226       16789505       2048
```

## Sample Output

### show security alg sccp calls detail

```
user@host> show security alg sccp calls detail
Client IP address: 11.0.102.91
Client zone: 7
CallManager IP: 13.0.99.226
Conference ID: 16789504
Resource manager group: 2048
SCCP channel information:
    Media transmit channel address (IP address/Port): 0.0.0.0:0
    Media transmit channel translated address (IP address/Port): 0.0.0.0:0
    Media transmit channel pass-through party ID (PPID): 0
    Media transmit channel resource ID: 0
    Media receive channel address (IP address/Port): 11.0.102.91:20060
    Media receive channel translated address (IP address/Port): 25.0.0.1:1032
    Media receive channel pass-through party ID (PPID): 16934451
    Media receive channel resource ID: 8185
    Multimedia transmit channel address (IP address/Port): 0.0.0.0:0
    Multimedia transmit channel translated address (IP address/Port): 0.0.0.0:0
    Multimedia transmit channel pass-through party ID (PPID): 0
    Multimedia transmit channel resource ID: 0
    Multimedia receive channel address (IP address/Port): 0.0.0.0:0
    Multimedia receive channel translated address (IP address/Port): 0.0.0.0:0
    Multimedia receive channel pass-through party ID (PPID): 0
    Multimedia receive channel resource ID: 0
Total number of calls = 1
```

Copyright © 2013, Juniper Networks, Inc.

## show security alg sccp counters

**Syntax** **show security alg sccp counters**
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Display information about Skinny Client Control Protocol (SCCP) Application Layer Gateway (ALG) counters.

**Options**
- none—Display all SCCP ALG counters.
- **node**—(Optional) For chassis cluster configurations, display SCCP counters on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**
- sccp on page 914
- clear security alg sccp counters on page 1391
- SCCP ALGs for Security Devices
- Device and Routing Operations Monitoring

**List of Sample Output** show security alg sccp counters on page 1773

**Output Fields** Table 83 on page 1772 lists the output fields for the **show security alg sccp counters** command. Output fields are listed in the approximate order in which they appear.

### Table 83: show security alg sccp counters Output Fields

| Field Name | Field Description |
|---|---|
| **Active client sessions** | Number of active SCCP ALG client sessions. |
| **Active calls** | Number of active SCCP ALG calls. |
| **Total calls** | Total number of SCCP ALG calls. |
| **Packets received** | Number of SCCP ALG packets received. |
| **PDUs processed** | Number of SCCP ALG protocol data units (PDU) processed. |


Copyright © 2013, Juniper Networks, Inc.

Table 83: show security alg sccp counters Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Current call rate** | Number of calls per second. |
| **Packets dropped** | Number of packets dropped by the SCCP ALG. |
| **Decode errors** | Number of decoding errors. |
| **Protocol errors** | Number of protocol errors. |
| **Address translation errors** | Number of NAT errors. |
| **Policy lookup errors** | Number of errors occurring during policy lookups. |
| **Unknown PDUs** | Number of unknown protocol data units (PDUs). |
| **Maximum calls exceed** | Number of times the maximum number of calls was exceeded. |
| **Maximum call rate exceed** | Number of times the maximum call rate was exceeded. |
| **Initialization errors** | Number of call initialization errors. |
| **Internal errors** | Number of internal errors. |
| **Nonspecific error** | Number of nonspecific errors. |

## Sample Output

### show security alg sccp counters

```
user@host> show security alg sccp counters
SCCP call statistics:
  Active client sessions         : 4
  Active calls                   : 2
  Total calls                    : 3
  Packets received               : 232
  PDUs processed                 : 232
  Current call rate              : 0
Error counters:
  Packets dropped                : 0
  Decode errors                  : 0
  Protocol errors                : 0
  Address translation errors     : 0
  Policy lookup errors           : 0
  Unknown PDUs                   : 0
  Maximum calls exceeded         : 0
  Maximum call rate exceeded     : 0
  Initialization errors          : 0
  Internal errors                : 0
  Nonspecific error              : 0
```

Copyright © 2013, Juniper Networks, Inc.

## show security alg sip calls

**Syntax** **show security alg sip calls**
**<brief | detail | node ( *node-id* | all | local | primary) >**

**Release Information** Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Display information about Session Initiation Protocols (SIP) Application Layer Gateway (ALG) calls.

**Options**
- none | **brief**—Display brief call information.
- **detail**—(Optional) Display detailed information about SIP ALG calls.
- **node**—(Optional) For chassis cluster configurations, display SIP calls on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**
- sip (Security) on page 949
- clear security alg sip calls on page 1392
- SIP ALGs for Security Devices
- Device and Routing Operations Monitoring

**List of Sample Output**
show security alg sip calls on page 1775
show security alg sip calls detail on page 1775

**Output Fields** Table 84 on page 1774 lists the output fields for the **show security alg sip calls** command. Output fields are listed in the approximate order in which they appear.

### Table 84: show security alg sip calls Output Fields

| Field Name | Field Description |
|---|---|
| **UAS callid** | Call Identifier for the SIP ALG user agent server. |
| **State** | State of the SIP ALG user agent server. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security alg sip calls

```
user@host> show security alg sip calls
Total number of calls: 1
     Call ID  : 1-2468@20.0.0.174
   Method   : INVITE
```

## Sample Output

### show security alg sip calls detail

```
user@host> show security alg sip calls detail
Total number of calls: 1
       Call ID  : 1-2468@20.0.0.174
     Method   : INVITE
     State    : SETUP
     Group ID : 307
```

Copyright © 2013, Juniper Networks, Inc.

## show security alg sip counters

**Syntax** **show security alg sip counters**
<node ( *node-id* | all | local | primary)>

**Release Information** Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Display information about Session Initiation Protocol (SIP) Application Layer Gateway (ALG) counters.

**Options**
- none—Display all SIP ALG counters.
- **node**—(Optional) For chassis cluster configurations, display SIP counters on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**
- sip (Security) on page 949
- clear security alg sip counters on page 1393
- SIP ALGs for Security Devices
- Device and Routing Operations Monitoring

**List of Sample Output** show security alg sip counters on page 1779

**Output Fields** Table 85 on page 1776 lists the output fields for the **show security alg sip counters** command. Output fields are listed in the approximate order in which they appear.

### Table 85: show security alg sip counters Output Fields

| Field Name | Field Description |
|---|---|
| INVITE | Number of INVITE requests sent. An INVITE request is sent to invite another user to participate in a session. |
| CANCEL | Number of CANCEL requests sent. A user can send a CANCEL request to cancel a pending INVITE request. A CANCEL request has no effect if the SIP server processing the INVITE had sent a final response for the INVITE before it received the CANCEL |
| ACK | Number of ACK requests sent. The user from whom the INVITE originated sends an ACK request to confirm reception of the final response to the INVITE request. |


Copyright © 2013, Juniper Networks, Inc.

Table 85: show security alg sip counters Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| BYE | Number of BYE requests sent. A user sends a BYE request to abandon a session. A BYE request from either user automatically terminates the session. |
| RR header exceeded max | Number of times the SIP ALG RR (Record-Route) headers exceeded the maximum limit. |
| REGISTER | Number of REGISTER requests sent. A user sends a REGISTER request to a SIP registrar server to inform it of the current location of the user. A SIP registrar server records all the information it receives in REGISTER requests and makes this information available to any SIP server attempting to locate a user. |
| OPTIONS | Number of OPTIONS requests sent. An OPTION request is used by the User Agent (UA) to obtain information about the capabilities of the SIP proxy. A server responds with information about what methods, session description protocols, and message encoding it supports. |
| INFO | Number of INFO requests sent. AN INFO message is used to communicate mid-session signaling information along the signaling path for the call. |
| MESSAGE | Number of MESSAGE requests sent. SIP messages consist of requests from a client to a server and responses to the requests from a server to a client with the purpose of establishing a session (or a call). |
| NOTIFY | Number of NOTIFY requests sent. NOTIFY requests are sent to inform subscribers of changes in state to which the subscriber has a subscription. |
| PRACK | Number of PRACK requests sent. The PRACK request plays the same role as ACK, but for provisional responses. |
| PUBLISH | Number of PUBLISH requests sent. The PUBLISH request used for publishing event state. PUBLISH is similar to REGISTER in that it allows a user to create, modify, and remove state in another entity which manages this state on behalf of the user. |
| REFER | Number of REFER requests sent. A REFER request is used to refer the recipient (identified by the Request-URI) to a third party by the contact information provided in the request. |
| SUBSCRIBE | Number of SUBSCRIBE requests sent. A SUBCRIBE request is used to request current state and state updates from a remote node. |
| UPDATE | Number of UPDATE requests sent. AN UPDATE request is used to create a temporary opening in the firewall (pinhole) for new or updates Session Description Protocol (SDP) information. The following fields are modified: Via, From, To, Call-ID, Contact, Route, and Record-Route. |
| BENOTIFY | Number of BENOTIFY requests sent. A BENOTIFY request is used to reduce the unnecessary SIP signaling traffic on application servers. Applications that do not need a response for a NOTIFY request can enhance performance by enabling BENOTIFY. |
| SERVICE | Number of SERVICE requests sent. The SERVICE method used by a SIP client to request a service of a SIP server. It is a standard SIP message and will be forwarded until it reaches the server or end user which is performing the service. |

Copyright © 2013, Juniper Networks, Inc.

Table 85: show security alg sip counters Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **OTHER** | Number of OTHER requests sent. |
| **Total Pkt-in** | Number of SIP ALG total packets received. |
| **Total Pkt dropped on error** | Number of SIP ALG total packets dropped while transmission and retransmission of messages. |
| **Call error** | Number of SIP ALG call errors. |
| **IP resolve error** | Number of SIP ALG IP address resolution errors. |
| **NAT error** | Number of SIP ALG NAT errors. |
| **Resource manager error** | Number of SIP ALG resource manager errors. |
| **Contact header exceeded max** | Number of times the SIP ALG contact headers exceeded the maximum limit. |
| **Invite Dropped due to call limit** | Number of SIP ALG invite dropped due to call limits. |
| **SIP msg not processed by stack** | Number of SIP ALG stack errors. |
| **SIP msg not processed by alg** | Number of SIP ALG messages not processed by ALGs. |
| **SIP unknown method dropped** | Number of SIP ALG unknown method errors. |
| **Decoding error** | Number of SIP ALG decoding errors. |
| **Request for disconnected call** | Number of SIP ALG calls disconnected. |
| **Request out of state** | Number of SIP ALG messages out of state errors. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security alg sip counters

```
user@host> show security alg sip counters
SIP message counters(T:Transmit, RT:Retransmit):
   Method     T   1xx   2xx   3xx  4xx   5xx   6xx
              RT   RT    RT    RT   RT    RT    RT
   INVITE      4    4     3     0    0     0     0
               0    0     0     0    0     0     0
   CANCEL      0    0     0     0    0     0     0
               0    0     0     0    0     0     0
      ACK      3    0     0     0    0     0     0
               0    0     0     0    0     0     0
      BYE      3    0     3     0    0     0     0
               0    0     0     0    0     0     0
 REGISTER      7    0     7     0    0     0     0
               0    0     0     0    0     0     0
  OPTIONS      0    0     0     0    0     0     0
               0    0     0     0    0     0     0
     INFO      0    0     0     0    0     0     0
               0    0     0     0    0     0     0
  MESSAGE      0    0     0     0    0     0     0
               0    0     0     0    0     0     0
   NOTIFY      0    0     0     0    0     0     0
               0    0     0     0    0     0     0
    PRACK      0    0     0     0    0     0     0
               0    0     0     0    0     0     0
  PUBLISH      0    0     0     0    0     0     0
               0    0     0     0    0     0     0
    REFER      0    0     0     0    0     0     0
               0    0     0     0    0     0     0
SUBSCRIBE      0    0     0     0    0     0     0
               0    0     0     0    0     0     0
   UPDATE      0    0     0     0    0     0     0
               0    0     0     0    0     0     0
 BENOTIFY      0    0     0     0    0     0     0
               0    0     0     0    0     0     0
  SERVICE      0    0     0     0    0     0     0
               0    0     0     0    0     0     0
    OTHER      0    0     0     0    0     0     0
               0    0     0     0    0     0     0
SIP Error Counters:
Total Pkt-in                        :34
Total Pkt dropped on error          :0
Call error                          :0
IP resolve error                    :0
NAT error                           :0
Resource manager error              :0
RR header exceeded max              :0
Contact header exceeded max         :0
Call Dropped due to limit                 : 0
SIP stack error                                 : 0
SIP decode error                              : 0
SIP unknown method error                : 0
RTO message sent                            : 0
RTO message received                      : 0
RTO buffer allocation failure               : 0
RTO buffer transmit failure                 : 0
RTO send processing error               : 0
RTO receive processing error            : 0
RTO receive invalid length                  : 0
```

Copyright © 2013, Juniper Networks, Inc.

```
RTO receive call process error        : 0
RTO receive call allocation error     : 0
RTO receive call register error         : 0
RTO receive invalid status error      : 0
```


Copyright © 2013, Juniper Networks, Inc.

## show security alg sip rate

**Syntax**

**show security alg sip rate**
<node ( *node-id* | all | local | primary)>

**Release Information**

Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description**

Display rate information for Session Initiation Protocol (SIP) Application Layer Protocol (ALG) messages.

**Options**

- none—Display all SIP ALG rate information.
- **node**—(Optional) For chassis cluster configurations, display SIP rate on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level**

view

**Related Documentation**

- sip (Security) on page 949
- SIP ALGs for Security Devices
- Device and Routing Operations Monitoring

**List of Sample Output**

show security alg sip rate on page 1782

**Output Fields**

Table 86 on page 1781 lists the output fields for the **show security alg sip rate** command. Output fields are listed in the approximate order in which they appear.

### Table 86: show security alg sip rate Output Fields

| Field Name | Field Description |
|---|---|
| **CPU ticks** | SIP ALG CPU ticks per microsecond. |
| **Time taken** | Time, in microseconds, that the last SIP ALG message needed to transit the network. |
| **Total time** | Total time, in microseconds, during an interval of less than 10 minutes for the specified number of SIP ALG messages to transit the network. |
| **Rate** | Number of SIP ALG messages per second transiting the network. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

**show security alg sip rate**

```
user@host> show security alg sip rate
CPU ticks per us is 166
Time taken for the last message is 1103 us
Total time taken for 3124 messages is 6221482 us (in less than 10 minutes)
Rate: 502 messages/second
```


Copyright © 2013, Juniper Networks, Inc.

## show security alg sip transactions

**Syntax**
show security alg sip transactions
<node (*node-id* | all | local | primary)>

**Release Information**
Command modified in Release 9.2 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description**
Display information about Session Initiation Protocol (SIP) Application Layer Gateway (ALG) transactions.

**Options**
- none—Display all SIP ALG transactions.
- **node**—(Optional) For chassis cluster configurations, display SIP transactions on a specific node (device) in the cluster.
- ***node-id***—Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

**Required Privilege Level**
view

**Related Documentation**
- sip (Security) on page 949
- SIP ALGs for Security Devices
- Device and Routing Operations Monitoring

**List of Sample Output**
show security alg sip transactions on page 1784

**Output Fields**
Table 87 on page 1783 lists the output fields for the **show security alg sip transaction** command. Output fields are listed in the approximate order in which they appear.

### Table 87: show security alg sip transactions Output Fields

| Field Name | Field Description |
|---|---|
| UAS | SIP ALG User Agent Server transaction name. |
| UAC | ALG SIP User Agent Client transaction name. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security alg sip transactions

```
user@host> show security alg sip transactions
Total number of transactions: 1
Transaction Name       Method    CSeq       State         Timeout    VIA RSC ID
UAS:tsx0x4b06ddf4         BYE    101     Proceeding            -1       -
UAC:tsx0x4b06f610         BYE    101        Calling            27      8185
```


Copyright © 2013, Juniper Networks, Inc.

## show security alg status

**Syntax** **show security alg status**

**Release Information** Command modified in Release 9.5 of Junos OS

**Description** Display the status (enabled/disabled) of the supported Application Layer Gateway (ALG) transactions.

This command is supported on SRX Series and J Series devices. The following list describes the default status on each of these devices:

- SRX3000 and SRX5000 line devices—FTP, TFTP, DNS, MSRPC, PPTP, SUNRPC, RSH, SQL, and TALK ALGs are enabled by default. All other ALGs are disabled.
- SRX100, SRX210, SRX240, and SRX650 devices—All supported ALGs are enabled by default.
- J Series devices—All supported ALGs are enabled by default.

For complete information about which ALGs are supported on which devices, see Application Layer Gateways.

**Options** none—Display status of all supported ALGs.

**Required Privilege Level** view

**Related Documentation**

- Application Layer Gateways for Security Devices
- Device and Routing Operations Monitoring

**Output Fields** The following list describes the output fields for the **show security alg status** command. Output fields are listed in the approximate order in which they appear.

- **DNS**—Domain Name Server
- **FTP**—File Transfer Protocol
- **H323**—H.323 protocol
- **MGCP**—Media Gateway Control Protocol
- **MSRPC**—Microsoft remote procedure call
- **PPTP**—Point-to-Point Tunneling Protocol
- **RSH**—UNIX remote shell services
- **RTSP**—Real-Time Streaming Protocol
- **SCCP**—Skinny Client Control Protocol
- **SIP**—Session Initiation Protocol
- **SQL**—Oracle SQL

Copyright © 2013, Juniper Networks, Inc.

- **SUNRPC**—Sun Microsystems remote procedure call
- **TALK**—TALK program
- **TFTP**—Trivial File Transfer Protocol

## Sample Output

### show security alg status

```
user@host> show security alg status
ALG Status :

  DNS      : Enabled

  FTP      : Enabled

  H323     : Disabled

  MGCP     : Disabled

  MSRPC    : Enabled

  PPTP     : Enabled

  RSH      : Enabled

  RTSP     : Disabled

  SCCP     : Disabled

  SIP      : Disabled

  SQL      : Enabled

  SUNRPC   : Enabled

  TALK     : Enabled

  TFTP     : Enabled
```


Copyright © 2013, Juniper Networks, Inc.

## show security application-firewall rule-set

**Syntax** show security application-firewall rule-set (*<rule-set-name>* | all)

**Release Information** Command introduced in Junos OS Release 11.1. Updated in Junos OS Release 12.1X44-D10 with output format changes.

**Description** Display information about the specified rule set defined in the application firewall.

**Options** *rule-set-name*—Name of the rule set.

**all**—Display information about all the application firewall rule sets.

**Required Privilege Level** view

**Related Documentation**
- Application Firewall
- clear security application-firewall rule-set statistics on page 1394
- Logical Systems for Security Devices

**List of Sample Output**
show security application-firewall rule-set my_ruleset1 on page 1788
show security application-firewall rule-set all on page 1788

**Output Fields** Table 88 on page 1787 lists the output fields for the **show security application-firewall rule-set** command. Output fields are listed in the approximate order in which they appear.

### Table 88: show security application-firewall rule-set Output Fields

| Field Name | Field Description |
|---|---|
| **Rule-set** | Name of the rule set. |
| **Rule** | Name of the rule<br>• **Dynamic applications**—Name of the applications.<br>• **Dynamic application groups**—Name of the application groups.<br>• **SSL-Encryption**—The encryption setting for SSL traffic.<br>• **Action**—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following:<br>  ◦ **permit**<br>  ◦ **deny**<br>  ◦ **reject**<br>• **Number of sessions matched**—Number of sessions matched with the application firewall rule. |
| **Default rule** | The default rule applied when the identified application is not specified in any rules of the rule set.<br>• **Number of sessions matched**—Number of sessions matched with the application firewall default rule. |

Copyright © 2013, Juniper Networks, Inc.

Table 88: show security application-firewall rule-set Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Number of sessions with appid pending** | Number of sessions that are pending with the application ID processing |

## Sample Output

show security application-firewall rule-set my_ruleset1

```
user@host>show security application-firewall rule-set my_ruleset1
Rule-set: my_ruleset1
           Rule: rule1
               Dynamic Applications: junos:facebook, junos:messenger
               Dynamic Application Groups: junos:web, junos:chat
               SSL-Encryption: any
               Action: deny
               Number of sessions matched: 10
           Default rule: permit
               Number of sessions matched: 200
           Number of sessions with appid pending: 2
```

## Sample Output

show security application-firewall rule-set all

```
user@host> show security application-firewall rule-set all
Rule-set: my_ruleset1
           Rule: rule1
               Dynamic Applications: junos:facebook, junos:messenger
               Dynamic Application Groups: junos:web, junos:chat
               SSL-Encryption: no
               Action: deny
               Number of sessions matched: 10
           Default rule: permit
               Number of sessions matched: 200
           Number of sessions with appid pending: 5
         Rule-set: my_ruleset2
           Rule: rule2
               Dynamic Application Groups: junos: web
               SSL-Encryption: any
               Action: deny
               Number of sessions matched: 10
           Default rule: permit
               Number of sessions matched: 200
           Number of sessions with appid pending: 0
```


Copyright © 2013, Juniper Networks, Inc.

## show security application-firewall rule-set logical-system

**Syntax** The master, or root, administrator can issue the following statements:

show security application-firewall rule-set all
show security application-firewall rule-set *rule-set-name* | all | logical-system *logical-system-name* | all | root-logical-system [*logical-system-name* | all ]

The user logical system administrator can issue the following statement:

show security application-firewall rule-set all

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Display information about application firewall rule set(s) associated with a specific logical system, all logical systems, or the root logical system configured on a device.



NOTE: The master administrator can configure and view application firewall rule sets for the root logical system and all user logical systems configured on the device. User logical system administrators can configure and view application firewall rule set information only for the user logical systems for which they have access. For information about master and user administrator roles in logical systems, see Logical Systems for Security Devices.

**Options** ***rule-set-name***—Name of a specific rule set.

***logical-system-name***—Name of a specific logical system.

**all**—(default) Display all rule sets for all logical systems. The user logical system administrator can display all rule sets only for the logical system they can access.

**root-logical-system**—Display application firewall rule set information for the root logical system (master administrator only).

**Required Privilege Level** view

**Related Documentation**

- Application Firewall
- clear security application-firewall rule-set statistics logical-system on page 1395
- Master Administrator for Logical Systems on Security Devices

**List of Sample Output**

show security application-firewall rule-set logical-system all on page 1790
show security application-firewall rule-set all on page 1791

**Output Fields** Table 89 on page 1790 lists the output fields for the **show security application-firewall rule-set logical-system** command. Output fields are listed in the approximate order in which they appear.

Copyright © 2013, Juniper Networks, Inc.

Table 89: show security application-firewall rule-set logical-system Output Fields

| Field Name | Field Description |
|---|---|
| **Rule-set** | Name of the rule set. |
| **Logical system** | Name of the logical system. |
| **Rule** | Name of the rule.<br>• **Dynamic applications**—Name of the applications.<br>• **Dynamic application groups**—Name of the application groups.<br>• **Action**—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following:<br>  ◦ **permit**<br>  ◦ **deny**<br>• **Number of sessions matched**—Number of sessions matched with the application firewall rule. |
| **Default rule** | The default rule applied when the identified application is not specified in any rules of the rule set.<br>• **Number of sessions matched**—Number of sessions matched with the application firewall default rule. |
| **Number of sessions with appid pending** | Number of sessions that are pending with the application ID processing. |

## Sample Output

### show security application-firewall

```
root@host> show security application-firewall rule-set logical-system all

Rule-set: root_rs1
```


Copyright © 2013, Juniper Networks, Inc.

rule-set logical-system all

```
    Logical system: root-logical-system
    Rule: r1
        Dynamic Applications: junos:FTP
        Action:permit
        Number of sessions matched: 10
Default rule:deny
        Number of sessions matched: 100
Number of sessions with appid pending: 4

Rule-set: root-rs2
    Logical system: root-logical-system
    Rule: r1
        Dynamic Application Groups: junos:web
        Action:permit
        Number of sessions matched: 20
Default rule:deny
        Number of sessions matched: 100
Number of sessions with appid pending: 10
```

show security application-firewall rule-set all

```
root@host> show security application-firewall rule-set all

Rule-set: ls-product-design-rs1
    Logical system: ls-product-design
    Rule: r1
        Dynamic Applications: junos:TELNET
        Action:permit
        Number of sessions matched: 10
Default rule:deny
        Number of sessions matched: 100
Number of sessions with appid pending: 2

Rule-set: ls-product-design-rs1
    Logical system: ls-product-design
    Rule: r2
        Dynamic Application Groups: junos:web
        Action:permit
        Number of sessions matched: 20
Default rule:deny
        Number of sessions matched: 200
Number of sessions with appid pending: 4

Rule-set: ls-product-design-rs2
    Logical system: ls-product-design
    Rule: r1
        Dynamic Applications: junos:FACEBOOK
        Action:deny
        Number of sessions matched: 40
Default rule:permit
        Number of sessions matched: 400
Number of sessions with appid pending: 10
```

Copyright © 2013, Juniper Networks, Inc.

## show security application-tracking counters

**Syntax** show security application-tracking counters

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display the status of AppTrack counters.

**Required Privilege Level** view

**Related Documentation**
- Application Tracking
- Logical Systems for Security Devices

**Output Fields** Table 90 on page 1792 lists the output fields for the **show security application-tracking counters** command. Output fields are listed in the approximate order in which they appear.

### Table 90: show security application-tracking counters

| Field Name | Field Description |
|---|---|
| **Session create messages** | The number of log messages generated when a session was created. |
| **Session close messages** | The number of log messages generated when a session was closed. |
| **Session volume updates** | The number of log messages generated when an update interval was exceeded. |
| **Failed messages** | The number of messages that were not generated due to memory or session constraints. |

## Sample Output

### show security application-tracking counters

```
user@host> show security application-tracking counters
AVT counters:                          Value
 Session create messages                 0
 Session close messages                  0
 Session volume updates                  0
 Failed messages                         0
```


Copyright © 2013, Juniper Networks, Inc.

## show security datapath-debug capture

**Syntax** show security datapath-debug capture

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Display details of the data path debugging capture file.

**Required Privilege Level** view

**Related Documentation**
- show security datapath-debug counter on page 1794
- Master Administrator for Logical Systems on Security Devices
- Device and Routing Operations Monitoring
- Troubleshooting for Security Devices

**List of Sample Output** show security datapath—debug capture on page 1793

**Output Fields** Output fields are listed in the approximate order in which they appear.

### Sample Output

show security datapath—debug capture

```
user@host> show security datapath-debug capture
Packet 1, len 120: (C0/F0/P0/SEQ:71:lbt)
91 00 00 47 11 00 10 00 9a 14 00 19 03 00 00 00
00 00 00 00 00 01 00 47 10 00 00 00 00 00 00 00
00 1f 12 f8 dd 29 00 21 59 84 f4 01 81 00 02 1e
08 00 45 60 01 f4 00 00 00 00 3f 06 73 9f 01 01
01 02 03 01 01 02 d4 31 d4 31 00 00 00 00 00 00
00 00 50 02 00 00 ff ad 00 00 00 00
Packet 2, len 120: (C0/F0/P0/SEQ:71:lbt)
90 00 00 47 04 00 00 00 00 00 00 00 02 02 00 47
10 00 00 00 00 00 00 00 50 00 a6 1c 00 00 00 00
00 00 00 0a 00 00 00 00 00 00 09 d9 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 1f 12 f8
dd 29 00 21 59 84 f4 01 81 00 02 1e
```

Copyright © 2013, Juniper Networks, Inc.

## show security datapath-debug counter

**Syntax** show security datapath-debug counter

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Display details of the data path debugging counter.

**Required Privilege Level** view

**Related Documentation**
- show security datapath-debug capture on page 1793
- Master Administrator for Logical Systems on Security Devices
- Device and Routing Operations Monitoring
- Troubleshooting for Security Devices

**List of Sample Output** show security datapath-debug counter on page 1794

**Output Fields** Output fields are listed in the approximate order in which they appear.

### Sample Output

show security datapath-debug counter

```
user@host> show security datapath-debug counter
Datapath debug counters
Packet Filter 1:
np-ingress
Chassis 0 FPC 4 : 1
np-ingress
Chassis 0 FPC 3 : 0
np-egress
Chassis 0 FPC 4 : 1
np-egress
Chassis 0 FPC 3 : 0
jexec
Chassis 0 FPC 0 PIC 1: 0
jexec
Chassis 0 FPC 0 PIC 0: 1
lbt
Chassis 0 FPC 0 PIC 1: 0
lbt
Chassis 0 FPC 0 PIC 0: 2
pot
Chassis 0 FPC 0 PIC 1: 0
pot
```


Copyright © 2013, Juniper Networks, Inc.

## show security dns-cache

**Syntax** show security dns-cache <dns-name *dns-name*>

**Release Information** Command introduced in Junos OS Release 12.1X44-D10.

**Description** Display DNS cache information.



NOTE: This command is only available to the master administrator on devices that are configured for logical systems. This command is not available in user logical systems or on devices that are not configured for logical systems.

**Options**
- **dns-name**—Display DNS cache information for the specified name.

**Required Privilege Level** view

**Related Documentation**
- clear security dns-cache on page 1397
- Master Administrator for Logical Systems on Security Devices

**List of Sample Output**
show security dns-cache on page 1796
show security dns-cache dns-name dns2.test.com on page 1796

**Output Fields** Table 91 on page 1795 lists the output fields for the **show security dns-cache** command. Output fields are listed in the approximate order in which they appear.

### Table 91: show security dns-cache Output Fields

| Field Name | Field Description |
|---|---|
| **DNS Name** | DNS name. |
| **Address Family** | IPv4 or IPv6. |
| **TTL** | Time-to-live value. |
| **IP Address** | IP address for the DNS name. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security dns-cache

```
user@host> show security dns-cache
DNS Name: dns1.test.com:
  Address Family: IPv4, TTL: 10
    IP Address: 1.1.1.1
  Address Family: IPv6: TTL = 15
    IP Address: 2001:1.1.1.1
DNS Name: dns2.test.com:
  Address Family: IPv4, TTL: 20
    IP Address: 2.2.2.2
    IP Address: 2.2.2.3
```

## Sample Output

show security dns-cache dns-name dns2.test.com

```
user@host> show security dns-cache dns-name dns2.test.com
DNS Name: dns2.test.com:
  Address Family: IPv4, TTL: 20
    IP Address: 2.2.2.2
    IP Address: 2.2.2.3
```


Copyright © 2013, Juniper Networks, Inc.

## show security dynamic-policies

**Syntax** show security dynamic-policies [detail] [from-zone *zone*] [scope-id *id*] [to-zone *zone*]

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display dynamic policies downloaded on the group member.

**Options**

- none—Display basic information about all policies installed on the group member.
- **detail**—(Optional) Display a detailed view of all of the policies installed on the group member.
- **from-zone**—(Optional) Display information about the policies installed on the group member for the specified source zone.
- **scope-id**—(Optional) Display information about the policies installed on the group member for the specified policy identifier.
- **to-zone**—(Optional) Display information about the policies installed on the group member for the specified destination zone.

**Required Privilege Level** view

**Related Documentation**

- show security policies on page 2139

**List of Sample Output**

show security dynamic-policies on page 1799
show security dynamic-policies detail on page 1799
show security dynamic-policies from-zone Internal on page 1800
show security dynamic-policies scope-id 8 from-zone Internal on page 1800
show security dynamic-policies detail from-zone Internal on page 1801
show security dynamic-policies detail from-zone Internal to-zone Host on page 1801

**Output Fields** Table 92 on page 1797 lists the output fields for the **show security dynamic-policies** command. Output fields are listed in the approximate order in which they appear.

### Table 92: show security dynamic-policies Output Fields

| Field Name | Field Description |
|---|---|
| **Policy** | Name of the applicable Policy. |
| **State** | Status of the policy:<br>• **enabled**: The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it.<br>• **disabled**: The policy cannot be used in the policy lookup process, and therefore it is not available for access control. |
| **Index** | An internal number associated with the policy. |

Copyright © 2013, Juniper Networks, Inc.

Table 92: show security dynamic-policies Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Scope Policy** | Policy identifier. |
| **Sequence number** | Number of the policy within a given context. For example, three policies that are applicable in a from-zoneA-to-zoneB context might be ordered with sequence numbers 1, 2, and 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, and 4. |
| **Source addresses** | For standard display mode, the names of the source addresses for a policy. Address sets are resolved to their individual names. (In this case, only the names are given, not their IP addresses.)<br><br>For detail display mode, the names and corresponding IP addresses of the source addresses for a policy. Address sets are resolved to their individual address name-IP address pairs. |
| **Destination addresses** | Name of the destination address (or address set) as it was entered in the destination zone's address book. A packet's destination address must match this value for the policy to apply to it. |
| **Application** | Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time.<br><br>• **IP protocol**: The IP protocol used by the application—for example, TCP, UDP, ICMP.<br>• **ALG**: If an ALG is associated with the session, the name of the ALG. Otherwise, 0.<br>• **Inactivity timeout**: Elapse time without activity after which the application is terminated.<br>• **Source port range**: The low-high source port range for the session application.<br>• **Destination port range**: The low-high destination port range for the session application. |
| **action-type** | Must be permit. |
| **Policy Type** | Must be dynamic. |
| **From zone** | Name of the source zone. |
| **To zone** | Name of the destination zone. |
| **Tunnel** | Tunnel name, type (IPsec), and index number. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security dynamic-policies

```
user@host> show security dynamic-policies
Policy: policy_forward-0001, State: enabled, Index: 1048580, Scope Policy: 4
  Sequence number: 1
  Source addresses:10.10.10.0/16
  Destination addresses:20.20.20.0/16
    Applications: Unknown
action-type: permit, tunnel:
Policy: policy_forward-0002, State: enabled, Index: 2097156, Scope Policy: 4
  Sequence number: 2
  Source addresses:10.10.10.0/16
  Destination addresses:20.20.20.0/16
    Applications: Unknown
action-type: permit, tunnel:
```

## Sample Output

show security dynamic-policies detail

```
user@host> show security dynamic-policies detail
Policy: policy_forward-0001, action-type: permit, State: enabled, Index:
1048580,AI: disabled, Scope Policy: 4
  Policy Type: Dynamic
  Sequence number: 1
  From zone: Host, To zone: untrust
  Source addresses:10.10.10.0/16
  Destination addresses:20.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [23-23]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1001
Policy: policy_backward-0001, action-type: permit, State: enabled, Index:
1048582,AI: disabled, Scope Policy: 6
  Policy Type: Dynamic
  Sequence number: 1
  From zone: untrust, To zone: Host
  Source addresses:20.10.10.0/16
  Destination addresses:20.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [80-80]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1003
Policy: policy_internal-0001, action-type: permit, State: enabled, Index:
1048583,AI: disabled, Scope Policy: 7
  Policy Type: Dynamic
  Sequence number: 1
  From zone: Internal, To zone: Host
  Source addresses:192.168.1.0/24
  Destination addresses:10.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [80-80]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1005
Policy: policy_external-0001, action-type: permit, State: enabled, Index:
1048584,AI: disabled, Scope Policy: 8
  Policy Type: Dynamic
  Sequence number: 1
```

Copyright © 2013, Juniper Networks, Inc.

```
  From zone: Internal, To zone: untrust
  Source addresses:192.168.1.0/24
  Destination addresses:20.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [80-80]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1006
Policy: policy_forward-0002, action-type: permit, State: enabled, Index:
2097156,AI: disabled, Scope Policy: 4
  Policy Type: Dynamic
  Sequence number: 2
  From zone: Host, To zone: untrust
  Source addresses:10.10.10.0/16
  Destination addresses:20.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [80-80]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1002
Policy: policy_backward-0002, action-type: permit, State: enabled, Index:
2097158,AI: disabled, Scope Policy: 6
  Policy Type: Dynamic
  Sequence number: 2
  From zone: untrust, To zone: Host
  Source addresses:20.10.10.0/16
  Destination addresses:20.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [23-23]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1004
```

## Sample Output

### show security dynamic-policies from-zone Internal

```
user@host> show security dynamic-policies from-zone Internal
Policy: policy_internal-0001, State: enabled, Index: 1048583, Scope Policy: 7
  Sequence number: 1
    Applications: Unknown
action-type: permit, tunnel:
Policy: policy_external-0001, State: enabled, Index: 1048584, Scope Policy: 8
  Sequence number: 1
    Applications: Unknown
action-type: permit, tunnel:
```

## Sample Output

### show security dynamic-policies

```
user@host> show security dynamic-policies scope-id 8 from-zone Internal
Policy: policy_external-0001, State: enabled, Index: 1048584, Scope Policy: 8
  Sequence number: 1
```


Copyright © 2013, Juniper Networks, Inc.

scope-id 8 from-zone Internal

```
    Applications: Unknown
action-type: permit, tunnel:
```

## Sample Output

show security dynamic-policies detail from-zone Internal

```
user@host> show security dynamic-policies detail from-zone Internal
Policy: policy_internal-0001, action-type: permit, State: enabled, Index:
1048583,AI: disabled, Scope Policy: 7
  Policy Type: Dynamic
  Sequence number: 1
  From zone: Internal, To zone: Host
  Source addresses:192.168.1.0/24
  Destination addresses:10.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [80-80]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1005
Policy: policy_external-0001, action-type: permit, State: enabled, Index:
1048584,AI: disabled, Scope Policy: 8
  Policy Type: Dynamic
  Sequence number: 1
  From zone: Internal, To zone: untrust
  Source addresses:192.168.1.0/24
  Destination addresses:20.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [80-80]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1006
```

## Sample Output

show security dynamic-policies detail from-zone Internal to-zone Host

```
user@host> show security dynamic-policies detail from-zone Internal to-zone Host
Policy: policy_internal-0001, action-type: permit, State: enabled, Index:
1048583,AI: disabled, Scope Policy: 7
  Policy Type: Dynamic
  Sequence number: 1
  From zone: Internal, To zone: Host
  Source addresses:192.168.1.0/24
  Destination addresses:10.20.20.0/16
  Application: Unknown
    IP protocol: 6, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [80-80]
  Tunnel: Test Tunnel, Type: IPSec, Index: 1005
```

Copyright © 2013, Juniper Networks, Inc.

## show security dynamic-vpn client version

**Syntax** show security dynamic-vpn client version

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Display the client software version.

**Required Privilege Level** view

### Sample Output

```
user@host> show security dynamic-vpn client version
Juniper Access Manager version: 1.1.0.4165
```


Copyright © 2013, Juniper Networks, Inc.

## show security dynamic-vpn users

**Syntax** show security dynamic-vpn users

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Display all relevant user information.

**Required Privilege Level** view

**Output Fields** Table 93 on page 1803 lists the output fields for the **show security dynamic-vpn users** command. Output fields are listed in the approximate order in which they appear.

### Table 93: show security dynamic-vpn users Output Fields

| Field Name | Field Description |
|---|---|
| **User** | Username. |
| **User-groups** | Remote IPSec VPN usergroups |
| **Number of connections** | Number of connections currently active. |
| **Remote IP** | IP address of the client. |
| **IPsec VPN** | Name of the IPsec VPN. |
| **IKE gateway** | Name of the IKE gateway. |
| **IKE ID** | IKE ID configured for the client. |
| **Status** | Status of the connection. |

### Sample Output

```
user@host> show security dynamic-vpn users
User: alice , User group: group-one , Number of connections: 1
Remote IP: 2.2.2.10
    IPSEC VPN: dyn_vpn2
    IKE gateway: gw2
    IKE ID   : alicegw2.juniper.net
    IKE Lifetime: 72000
    IPSEC Lifetime: 3600
    Status: CONNECTED
```

Copyright © 2013, Juniper Networks, Inc.

## show security dynamic-vpn users terse

**Syntax** show security dynamic-vpn users terse

**Release Information** This command introduced in Release 10.0 of Junos OS.

**Description** Display all relevant user information.

**Required Privilege Level** view

**Output Fields** Table 94 on page 1804 lists the output fields for the **show security dynamic-vpn users terse** command. Output fields are listed in the approximate order in which they appear.

### Table 94: show security dynamic-vpn users terse Output Fields

| Field Name | Field Description |
|---|---|
| **User** | Username. |
| **User-groups** | Remote IPSec VPN usergroups |
| **Remote IP** | IP address of the client. |
| **IKE ID** | IKE ID configured for the client. |
| **Status** | Status of the connection. |
| **Client Config Name** | Name of the client configuration. |
| **Time Established** | Time that the user connection was established. |

## Sample Output

```
user@host> show security dynamic-vpn users terse

User   User      Remote   IKE       Status    IKE      IPSEC    Client Time
       Groups    IP       ID                  Lifetime Lifetime Config Established

                                                                Name
alice group-one 2.2.2.10 alicegw2.CONNECTED 72000    3600     group   Wed
                         juniper.                                   Aug 8 10:
                         net                                        26:39 2012
```


Copyright © 2013, Juniper Networks, Inc.

## show security firewall-authentication history

**Syntax** **show security firewall-authentication history**
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Display security firewall authentication history information.

**Options**
- none—Display history of firewall authentication information.
- **node**—(Optional) For chassis cluster configurations, display all firewall authentication history on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**
- firewall-authentication (Security) on page 590
- clear security firewall-authentication history on page 1400
- Logical Systems for Security Devices

**List of Sample Output**
show security firewall-authentication history on page 1806
show security firewall-authentication history node all on page 1806

**Output Fields** Table 95 on page 1805 lists the output fields for the **show security firewall-authentication history** command. Output fields are listed in the approximate order in which they appear.

### Table 95: show security firewall-authentication history Output Fields

| Field Name | Field Description |
|---|---|
| **Authentications** | Number of authentications. |
| **Id** | Identification number. |
| **Source IP** | IP address of the authentication source. |
| **Date** | Authentication date. |
| **Time** | Authentication time. |
| **Duration** | Authentication duration. |

Copyright © 2013, Juniper Networks, Inc.

Table 95: show security firewall-authentication history Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Status** | Authentication status success or failure. |
| **User** | Name of the user. |

## Sample Output

### show security firewall-authentication history

```
user@host> show security firewall-authentication history
History of firewall authentication data:
  Authentications: 1
          Id Source Ip       Date       Time     Duration   Status   User
           1 211.0.0.6       2007-04-03 11:43:06 00:00:45   Success  hello
```

## Sample Output

### show security firewall-authentication history node all

```
user@host> show security firewall-authentication history node all
node0:
--------------------------------------------------------------------------
History of firewall authentication data:
Authentications: 2
Id Source Ip       Date       Time     Duration   Status   User
1 100.0.0.1       2008-01-04 12:00:10 0:05:49    Success  local1
2 100.0.0.1       2008-01-04 14:36:52 0:01:03    Success  local1
node1:
--------------------------------------------------------------------------
History of firewall authentication data:
  Authentications: 1
          Id Source Ip       Date       Time     Duration   Status   User
           1 100.0.0.1       2008-01-04 14:59:43 1193046:06: Success local1
```


Copyright © 2013, Juniper Networks, Inc.

## show security firewall-authentication history address

**Syntax** **show security firewall-authentication history address** *ip-address*
**<node ( *node-id* | all | local | primary)>**

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Display security firewall authentication history for this source IP address.

**Options**

- **address** *ip-address* —IP address of the authentication source.
- none—Display all firewall authentication history for this address.
- **node**—(Optional) For chassis cluster configurations, display firewall authentication history for this address on a specific node.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**

- firewall-authentication (Security) on page 590
- clear security firewall-authentication history address on page 1401

**List of Sample Output**
show security firewall-authentication history address 4.4.4.2 on page 1808
show security firewall-authentication history address 100.0.0.1 node local on page 1808

**Output Fields** Table 96 on page 1807 lists the output fields for the **show security firewall-authentication history address** command. Output fields are listed in the approximate order in which they appear.

### Table 96: show security firewall-authentication history address Output Fields

| Field Name | Field Description |
|---|---|
| **Username** | User ID. |
| **Source IP** | IP address of the authentication source. |
| **Authentication state** | Status of authentication (success or failure). |
| **Authentication method** | Path chosen for authentication. |
| **Access start date** | Date when user authenticated. |

Copyright © 2013, Juniper Networks, Inc.

Table 96: show security firewall-authentication history address Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Access start time** | Time when user authenticated. |
| **Duration of user access** | Time duration of the accessing firewall. |
| **Policy name** | Name of the policy. |
| **Source zone** | User traffic received from the zone. |
| **Destination zone** | User traffic destined to the zone. |
| **Access profile** | Name of profile used for authentication. |
| **Bytes sent by this user** | Number of bytes sent by the user. |
| **Bytes received by this user** | Number of bytes received by the user. |

## Sample Output

### show security firewall-authentication history address 4.4.4.2

```
user@host> show security firewall-authentication history address 4.4.4.2
Username: u1
Source IP: 4.4.4.2
Authentication state: Success
Authentication method: Pass-through using HTTP
Access start date: 2007-09-12
Access start time: 15:33:29
Duration of user access: 0:00:48
Policy name: Z1-Z2
Source zone: Z1
Destination zone: Z2
Access profile: profile-local
Bytes sent by this user: 0
Bytes received by this user: 449
```

## Sample Output

### show security firewall-authentication

```
user@host> show security firewall-authentication history address 100.0.0.1 node local
node0:
--------------------------------------------------------------------------
```


Copyright © 2013, Juniper Networks, Inc.

history address 100.0.0.1 node local

```
Username: local1
Source IP: 100.0.0.1
Authentication state: Success
Authentication method: Pass-through using Telnet
Access start date: 2008-01-04
Access start time: 12:00:10
Duration of user access: 0:05:49
Policy name: POL1
Source zone: z1
Destination zone: z2
Access profile: p1
Bytes sent by this user: 0
Bytes received by this user: 0
Username: local1
Source IP: 100.0.0.1
Authentication state: Success
Authentication method: Pass-through using Telnet
Access start date: 2008-01-04
Access start time: 14:36:52
Duration of user access: 0:01:03
Policy name: POL1
Source zone: z1
Destination zone: z2
Access profile: p1
Bytes sent by this user: 2178
Bytes received by this user: 4172
```

Copyright © 2013, Juniper Networks, Inc.

## show security firewall-authentication history identifier

**Syntax** **show security firewall-authentication history identifier** *identifier*
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Display security firewall authentication history information for the authentication with this identifier.

**Options**

- **identifier** *identifier*—Identifying number of the authentication process.
- none—Display all firewall authentication history information for the authentication with this identifier.
- **node**—(Optional) For chassis cluster configurations, display firewall authentication history on a specific node for the authentication with this identifier.
  - *node-id* —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**

- firewall-authentication (Security) on page 590
- clear security firewall-authentication history identifier on page 1402

**List of Sample Output**
show security firewall-authentication history identifier 1 on page 1811
show security firewall-authentication identifier 1 node primary on page 1811

**Output Fields** Table 97 on page 1810 lists the output fields for the **show security firewall-authentication history identifier** command. Output fields are listed in the approximate order in which they appear.

Table 97: show security firewall-authentication history identifier Output Fields

| Field Name | Field Description |
|---|---|
| **Username** | User ID. |
| **Source IP** | IP address of the authentication source. |
| **Authentication state** | Status of authentication (success or failure). |
| **Authentication method** | Path chosen for authentication. |


Copyright © 2013, Juniper Networks, Inc.

Table 97: show security firewall-authentication history identifier Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Access start date** | Date when user authenticated. |
| **Access start time** | Time when user authenticated. |
| **Duration of user access** | Time duration of the accessing firewall. |
| **Policy index** | Identification number of the policy. |
| **Policy name** | Name of the policy. |
| **Source zone** | User traffic received from the zone. |
| **Destination zone** | User traffic destined to the zone. |
| **Access profile** | Name of profile used for authentication. |
| **Bytes sent by this user** | Number of bytes sent by the user. |
| **Bytes received by this user** | Number of bytes received by the user. |
| **Client-groups** | Name of the client group. |

## Sample Output

show security firewall-authentication history identifier 1

```
user@host> show security firewall-authentication history identifier 1
Username: hello
Source IP: 211.0.0.6
Authentication state: Success
Authentication method: Pass-through using Telnet
Access start date: 2007-04-03
Access start time: 11:43:06
Duration of user access: 00:00:45
Policy index: 4
Source zone: z2
Destination zone: z1
Access profile: profile1
Bytes sent by this user: 0
Bytes received by this user: 1050
Client-groups: Sunnyvale Bangalore
```

## Sample Output

show security firewall-authentication

```
user@host> show security firewall-authentication history identifier 1 node primary
node0:
--------------------------------------------------------------------------
```

Copyright © 2013, Juniper Networks, Inc.

identifier 1 node primary

```
Username: local1
Source IP: 100.0.0.1
Authentication state: Success
Authentication method: Pass-through using Telnet
Access start date: 2008-01-04
Access start time: 12:00:10
Duration of user access: 0:05:49
Policy name: POL1
Source zone: z1
Destination zone: z2
Access profile: p1
Bytes sent by this user: 0
Bytes received by this user: 0
```


Copyright © 2013, Juniper Networks, Inc.

## show security firewall-authentication users

**Syntax** **show security firewall-authentication users**
<node ( ***node-id*** | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Display firewall authentication details about all users.

**Options**
- none—Display details about all firewall authentication users.
- **node**—(Optional) For chassis cluster configurations, display firewall authentication details for all users on a specific node.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**
- firewall-authentication (Security) on page 590
- clear security firewall-authentication users on page 1403
- Logical Systems for Security Devices

**List of Sample Output**
show security firewall-authentication users on page 1814
show security firewall-authentication users node 0 on page 1814
show security firewall-authentication users node all on page 1814

**Output Fields** Table 98 on page 1813 lists the output fields for the **show security firewall-authentication users** command. Output fields are listed in the approximate order in which they appear.

Table 98: show security firewall-authentication users Output Fields

| Field Name | Field Description |
|---|---|
| **Total users in table** | Gives count of how many entries/users the command will display. |
| **Id** | Identification number. |
| **Source IP** | IP address of the authentication source. |
| **Src zone** | User traffic received from the zone. |
| **Dst zone** | User traffic destined to the zone. |

Copyright © 2013, Juniper Networks, Inc.

Table 98: show security firewall-authentication users Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Profile** | Name of profile used for authentication. |
| **Age** | Idle timeout for the user. |
| **Status** | Authentication status success or failure. |
| **User** | Name of the user. |

## Sample Output

show security firewall-authentication users

```
user@host> show security firewall-authentication users
Firewall authentication data:
  Total users in table: 1
          Id Source Ip       Src zone Dst zone Profile    Age Status   User
           1 1111:1212/64        z1       z2       p1       0 Success  local1
```

## Sample Output

show security firewall-authentication users node 0

```
user@host> show security firewall-authentication users node 0
node0:
--------------------------------------------------------------------------
Firewall authentication data:
  Total users in table: 1
          Id Source Ip       Src zone Dst zone Profile    Age Status   User

           3 100.0.0.1       z1       z2       p1           1 Success  local1
```

## Sample Output

show security firewall-authentication users node all

```
user@host> show security firewall-authentication users node all
node0:
--------------------------------------------------------------------------
Firewall authentication data:
  Total users in table: 1
          Id Source Ip       Src zone Dst zone Profile    Age Status   User
           3 100.0.0.1       z1       z2       p1           1 Success  local1

node1:
--------------------------------------------------------------------------
Firewall authentication data:
  Total users in table: 1
          Id Source Ip       Src zone Dst zone Profile    Age Status   User
           2 100.0.0.1       z1       z2       p1           1 Success  local1
```


Copyright © 2013, Juniper Networks, Inc.

## show security firewall-authentication users address

**Syntax** **show security firewall-authentication users address** *ip-address*
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Display information about the users at the specified IP address that are currently authenticated.

**Options**

- **address** *ip-address*—IP address of the authentication source.
- none—Display all the firewall authentication information for users at this IP address.
- **node**—(Optional) For chassis cluster configurations, display user firewall authentication entries on a specific node.
  - *node-id* —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**

- firewall-authentication (Security) on page 590
- clear security firewall-authentication users address on page 1404

**List of Sample Output**
show security firewall-authentication users address 211.0.0.6 on page 1816
show security firewall-authentication users address 100.0.0.1 node local on page 1816

**Output Fields** Table 99 on page 1815 lists the output fields for the **show security firewall-authentication users address** command. Output fields are listed in the approximate order in which they appear.

### Table 99: show security firewall-authentication users address Output Fields

| Field Name | Field Description |
|---|---|
| **Username** | User ID. |
| **Source IP** | IP address of the authentication source. |
| **Authentication state** | Status of authentication (success or failure). |
| **Authentication method** | Path chosen for authentication. |
| **Access time remaining** | Duration for which the connection exists. |

Copyright © 2013, Juniper Networks, Inc.

Table 99: show security firewall-authentication users address Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Source zone** | User traffic received from the zone. |
| **Destination zone** | User traffic destined to the zone. |
| **Policy index** | Identification number of the policy. |
| **Policy name** | Name of the policy. |
| **Access profile** | Name of profile used for authentication. |
| **Interface Name** | Name of the interface. |
| **Bytes sent by this user** | Number of bytes sent by the user. |
| **Bytes received by this user** | Number of bytes received by the user. |
| **Client-groups** | Name of the client group. |

## Sample Output

show security firewall-authentication users address 211.0.0.6

```
user@host>show security firewall-authentication users address 211.0.0.6
Username: hello
Source IP: 211.0.0.6
Authentication state: Success
Authentication method: Pass-through using Telnet
Access time remaining: 0
Source zone: z2
Destination zone: z1
Policy index: 5
Access profile: profile1
Interface Name: ge-0/0/2.0
Bytes sent by this user: 0
Bytes received by this user: 0
Client-groups: Sunnyvale Bangalore
```

## Sample Output

show security firewall-authentication

```
user@host> show security firewall-authentication users address 100.0.0.1 node local
node0:
--------------------------------------------------------------------------
```


Copyright © 2013, Juniper Networks, Inc.

**users address 100.0.0.1 node local**

```
Username: local1
Source IP: 100.0.0.1
Authentication state: Success
Authentication method: Pass-through using Telnet
Age: 2
Access time remaining: 4
Source zone: z1
Destination zone: z2
Policy name: POL1
Access profile: p1
Interface Name: reth1.0
Bytes sent by this user: 614
Bytes received by this user: 1880
```

Copyright © 2013, Juniper Networks, Inc.

## show security firewall-authentication users identifier

**Syntax** **show security firewall-authentication users identifier** *identifier*
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Display firewall authentication details about the user with this identification number.

**Options**

- **identifier** *identifier*—Identification number of the user for which to display authentication details.
- **node**—(Optional) For chassis cluster configurations, display the firewall authentication details security firewall authentication entry on a specific node (device) in the cluster for the user with this identification number.
  - *node-id* —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**

- firewall-authentication (Security) on page 590
- clear security firewall-authentication users identifier on page 1405

**List of Sample Output**
show security firewall-authentication users identifier 3 on page 1819
show security firewall-authentication users identifier 3 node primary on page 1819

**Output Fields** Table 100 on page 1818 lists the output fields for the **show security firewall-authentication users identifier** command. Output fields are listed in the approximate order in which they appear.

Table 100: show security firewall-authentication users identifier Output Fields

| Field Name | Field Description |
|---|---|
| **Username** | User ID. |
| **Source IP** | IP address of the authentication source. |
| **Authentication state** | Status of authentication (success or failure). |
| **Authentication method** | Path chosen for authentication. |
| **Age** | Idle timeout for the user. |


Copyright © 2013, Juniper Networks, Inc.

Table 100: show security firewall-authentication users identifier Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Access time remaining** | Duration for which the connection exists. |
| **Source zone** | User traffic received from the zone. |
| **Destination Zone** | User traffic destined to the zone. |
| **Policy Name** | Name of the policy. |
| **Access profile** | Name of profile used for authentication. |
| **Interface Name** | Name of the interface |
| **Bytes sent by this user** | Number of bytes sent by the user. |
| **Bytes received by this user** | Number of bytes received by the user. |

## Sample Output

show security firewall-authentication users identifier 3

```
user@host> show security firewall-authentication users identifier 3
Username: u1
Source IP: 4.4.4.2
Authentication state: Success
Authentication method: Pass-through using HTTP
Age: 1
Access time remaining: 254
Source zone: Z1
Destination zone: Z2
Policy name: Z1-Z2
Access profile: profile-local
Interface Name: ge-0/0/1.0
Bytes sent by this user: 0
Bytes received by this user: 449
```

## Sample Output

show security firewall-authentication

```
user@host> show security firewall-authentication users identifier 3 node primary
node0:
--------------------------------------------------------------------------
```

users identifier 3 node primary

```
Username: local1
Source IP: 100.0.0.1
Authentication state: Success
Authentication method: Pass-through using Telnet
Age: 1
Access time remaining: 5
Source zone: z1
Destination zone: z2
Policy name: POL1
Access profile: p1
Interface Name: reth1.0
Bytes sent by this user: 614
Bytes received by this user: 1880
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow cp-session

**Syntax** **show security flow cp-session**
[<filter>] [summary | terse]

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display central point session-related flow information.

**Options**
- destination-port—Destination port
- destination-prefix—Destination prefix
- family—Display session by family.
- protocol—IP protocol number
- source-port—Source port
- source-prefix—Source IP prefix or address
- summary | terse–Display the specified level of output.

**Required Privilege Level** view

**List of Sample Output**
show security flow cp-session summary on page 1822
show security flow cp-session terse on page 1822

**Output Fields** Table 101 on page 1821 lists the output fields for the **show security flow cp-session** command. Output fields are listed in the approximate order in which they appear.

### Table 101: show security flow cp-session Output Fields

| Field Name | Field Description |
|---|---|
| Valid gates | Number of valid central point sessions. |
| Pending gates | Number of pending central point sessions. |
| Invalidated gates | Number of invalid central point sessions. |
| Gates in other states | Number of central point sessions in other states. |
| Total gates | Number of central point sessions in total. |
| Maximum sessions | Number of maximum central point sessions. |
| Maximum inet6 sessions | Number of maximum inet6 central point sessions. |
| Session ID | Number that identifies the session. Use this ID to get more information about the session. |
| SPU | Services Processing Unit. |

Copyright © 2013, Juniper Networks, Inc.

Table 101: show security flow cp-session Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| In | Incoming flow (source and destination IP addresses). |
| Out | Reverse flow (source and destination IP addresses). |

## Sample Output

### show security flow cp-session summary

```
root> show security flow cp-session summary
Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
Maximum sessions: 10485760
Maximum inet6 sessions: 5242880
```

### show security flow cp-session terse

```
root> show security flow cp-session terse
Session ID: 160000015, SPU: 17, Valid
  In: 40.0.0.111/32838 --> 30.0.0.100/21;tcp,
  Out: 30.0.0.100/21 --> 40.0.0.111/32838;tcp,
Total sessions: 1
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow cp-session destination-port

**Syntax** **show security flow cp-session destination-port** *destination-port-number* **[summary | terse]**

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display central point session-related flow information for the specified destination port.

**Options**

- *destination-port-number* —Number of the destination port for which to display central point session information.

  **Range**: 1 through 65,535

- summary | terse—Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**

- show security flow cp-session on page 1821
- show security flow cp-session destination-prefix on page 1825

**List of Sample Output**

show security flow cp-session destination-port summary on page 1824
show security flow cp-session destination-port terse on page 1824

**Output Fields** Table 102 on page 1823 lists the output fields for the **show security flow cp-session destination-port** command. Output fields are listed in the approximate order in which they appear.

Table 102: show security flow cp-session destination-port Output Fields

| Field Name | Field Description |
|---|---|
| Valid gates | Number of valid central point sessions. |
| Pending gates | Number of pending central point sessions. |
| Invalidated gates | Number of invalid central point sessions. |
| Gates in other states | Number of central point sessions in other states. |
| Total gates | Number of central point sessions in total. |
| Session ID | Number that identifies the session. Use this ID to get more information about the session. |
| SPU | Services Processing Unit. |
| In | Incoming flow (source and destination IP addresses). |
| Out | Reverse flow (source and destination IP addresses). |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow cp-session destination-port summary

```
root> show security flow cp-session destination-port 21 summary
Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

### show security flow cp-session destination-port terse

```
root> show security flow cp-session destination-port 21 terse
Session ID: 160000015, SPU: 17, Valid
  In: 40.0.0.111/32838 --> 30.0.0.100/21;tcp,
  Out: 30.0.0.100/21 --> 40.0.0.111/32838;tcp,
Total sessions: 1
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow cp-session destination-prefix

**Syntax** **show security flow cp-session destination-prefix** *destination-IP-prefix* **[summary | terse]**

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display central point session-related flow information for the specified destination prefix.

**Options**

- *destination-IP-prefix* —Destination IP prefix or address for which to display central point session information.

  **Range**: 1 through 65,535.

- summary | terse—Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**

- show security flow cp-session on page 1821
- show security flow cp-session destination-port on page 1823

**List of Sample Output**

show security flow cp-session destination-prefix summary on page 1826
show security flow cp-session destination-prefix terse on page 1826

**Output Fields** Table 103 on page 1825 lists the output fields for the **show security flow cp-session destination-prefix** command. Output fields are listed in the approximate order in which they appear.

### Table 103: show security flow cp-session destination-prefix Output Fields

| Field Name | Field Description |
|---|---|
| Valid gates | Number of valid central point sessions. |
| Pending gates | Number of pending central point sessions. |
| Invalidated gates | Number of invalid central point sessions. |
| Gates in other states | Number of central point sessions in other states. |
| Total gates | Number of central point sessions in total. |
| Session ID | Number that identifies the session. Use this ID to get more information about the session. |
| SPU | Services Processing Unit. |
| In | Incoming flow (source and destination IP addresses). |
| Out | Reverse flow (source and destination IP addresses). |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow cp-session destination-prefix summary

```
root> show security flow cp-session destination-prefix 30/8 summary
Valid sessions: 1
Pending sessions: 1
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 2
```

### show security flow cp-session destination-prefix terse

```
root> show security flow cp-session destination-prefix 30/8 terse
Session ID: 160000015, SPU: 17, Valid
  In: 40.0.0.111/32838 --> 30.0.0.100/21;tcp,
  Out: 30.0.0.100/21 --> 40.0.0.111/32838;tcp,
Total sessions: 1
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow cp-session family

**Syntax** **show security flow cp-session family *family* [summary | terse]**

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display central point session-related flow information for the specified family.

**Options**
- *family*–Display session by family.
- inet—Display IPv4 sessions.
- inet6–Display IPv6 and IPv6-NATPT sessions.
- summary | terse–Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**
- show security flow cp-session on page 1821

**List of Sample Output**
show security flow cp-session family summary on page 1828
show security flow cp-session family terse on page 1828

**Output Fields** Table 104 on page 1827 lists the output fields for the **show security flow cp-session** family command. Output fields are listed in the approximate order in which they appear.

### Table 104: show security flow cp-session family Output Fields

| Field Name | Field Description |
|---|---|
| Valid gates | Number of valid central point sessions. |
| Pending gates | Number of pending central point sessions. |
| Invalidated gates | Number of invalid central point sessions. |
| Gates in other states | Number of central point sessions in other states. |
| Total gates | Number of central point sessions in total. |
| Session ID | Number that identifies the session. Use this ID to get more information about the session. |
| SPU | Services Processing Unit. |
| In | Incoming flow (source and destination IP addresses). |
| Out | Reverse flow (source and destination IP addresses). |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow cp-session family summary

```
root> show security flow cp-session family inet summary
Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

### show security flow cp-session family terse

```
root> show security flow cp-session family inet terse
Session ID: 160000015, SPU: 17, Valid
  In: 40.0.0.111/32838 --> 30.0.0.100/21;tcp,
  Out: 30.0.0.100/21 --> 40.0.0.111/32838;tcp,
Total sessions: 1
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow cp-session protocol

**Syntax** **show security flow cp-session protocol *protocol-name* [summary | terse]**

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display central point session-related flow information for the specified protocol.

**Options**

- *protocol-name* —Protocol to use as a central point session filter. Information about the central point session that uses this protocol is displayed.

  Possible protocols are:

  - ah—IP Security Authentication Header
  - egp—Exterior gateway protocol
  - esp—IPsec Encapsulating Security Payload
  - gre—Generic routing encapsulation
  - icmp—Internet Control Message Protocol
  - icmp6—Internet Control Message Protocol
  - igmp—Internet Group Management Protocol
  - ipip—IP over IP
  - ospf—Open Shortest Path First
  - pim—Protocol Independent Multicast
  - rsvp—Resource Reservation Protocol
  - sctp—Stream Control Transmission Protocol
  - tcp—Transmission Control Protocol
  - udp—User Datagram Protocol

- summary | terse–Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**

- show security flow cp-session on page 1821

**List of Sample Output**

show security flow cp-session protocol summary on page 1830
show security flow cp-session protocol terse on page 1830

**Output Fields** Table 105 on page 1830 lists the output fields for the **show security flow cp-session** protocol command. Output fields are listed in the approximate order in which they appear.

Copyright © 2013, Juniper Networks, Inc.

### Table 105: show security flow cp-session protocol Output Fields

| Field Name | Field Description |
|---|---|
| Valid gates | Number of valid central point sessions. |
| Pending gates | Number of pending central point sessions. |
| Invalidated gates | Number of invalid central point sessions. |
| Gates in other states | Number of central point sessions in other states. |
| Total gates | Number of central point sessions in total. |
| Session ID | Number that identifies the session. Use this ID to get more information about the session. |
| SPU | Services Processing Unit. |
| In | Incoming flow (source and destination IP addresses). |
| Out | Reverse flow (source and destination IP addresses). |

## Sample Output

### show security flow cp-session protocol summary

```
root> show security flow cp-session protocol tcp summary
Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

### show security flow cp-session protocol terse

```
root> show security flow cp-session protocol tcp terse
Session ID: 160000015, SPU: 17, Valid
  In: 40.0.0.111/32838 --> 30.0.0.100/21;tcp,
  Out: 30.0.0.100/21 --> 40.0.0.111/32838;tcp,
Total sessions: 1
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow cp-session source-port

**Syntax** **show security flow cp-session source-port** *source-port-number* **[summary | terse]**

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display central point session-related flow information for the specified source-port.

**Options** *source-port-number*—Number of the source port about which to display central point session information.

**Range**: 1 through 65,535

**summary | terse**—Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**
- show security flow cp-session on page 1821
- show security flow cp-session source-prefix on page 1833

**List of Sample Output**
show security flow cp-session source-port summary on page 1832
show security flow cp-session source-port terse on page 1832

**Output Fields** Table 106 on page 1831 lists the output fields for the **show security flow cp-session source-port** command. Output fields are listed in the approximate order in which they appear.

Table 106: show security flow cp-session source-port Output Fields

| Field Name | Field Description |
|---|---|
| Valid gates | Number of valid central point sessions. |
| Pending gates | Number of pending central point sessions. |
| Invalidated gates | Number of invalid central point sessions. |
| Gates in other states | Number of central point sessions in other states. |
| Total gates | Number of central point sessions in total. |
| Session ID | Number that identifies the session. Use this ID to get more information about the session. |
| SPU | Services Processing Unit. |
| In | Incoming flow (source and destination IP addresses). |
| Out | Reverse flow (source and destination IP addresses). |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow cp-session source-port summary

```
root> show security flow cp-session source-port 32838 summary
Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

### show security flow cp-session source-port terse

```
root> show security flow cp-session source-port 32838 terse
Session ID: 160000015, SPU: 17, Valid
  In: 40.0.0.111/32838 --> 30.0.0.100/21;tcp,
  Out: 30.0.0.100/21 --> 40.0.0.111/32838;tcp,
Total sessions: 1
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow cp-session source-prefix

**Syntax** **show security flow cp-session source-prefix** *source-IP-prefix* **[summary | terse]**

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display central point session related flow information for the specified source-prefix.

**Options**
- *source-IP-prefix*—Source IP prefix or address for which to display central point session information.
- summary | terse—Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**
- show security flow cp-session on page 1821
- show security flow cp-session source-port on page 1831

**List of Sample Output**
show security flow cp-session source-prefix summary on page 1834
show security flow cp-session source-prefix terse on page 1834

**Output Fields** Table 107 on page 1833 lists the output fields for the **show security flow cp-session source-prefix** command. Output fields are listed in the approximate order in which they appear.

### Table 107: show security flow cp-session source-prefix Output Fields

| Field Name | Field Description |
|---|---|
| Valid gates | Number of valid central point sessions. |
| Pending gates | Number of pending central point sessions. |
| Invalidated gates | Number of invalid central point sessions. |
| Gates in other states | Number of central point sessions in other states. |
| Total gates | Number of central point sessions in total. |
| Session ID | Number that identifies the session. Use this ID to get more information about the session. |
| SPU | Services Processing Unit. |
| In | Incoming flow (source and destination IP addresses). |
| Out | Reverse flow (source and destination IP addresses). |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security flow cp-session source-prefix summary

```
root> show security flow cp-session source-prefix 40/8 summary
Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

show security flow cp-session source-prefix terse

```
root> show security flow cp-session source-prefix 40/8 terse
Session ID: 160000015, SPU: 17, Valid
  In: 40.0.0.111/32838 --> 30.0.0.100/21;tcp,
  Out: 30.0.0.100/21 --> 40.0.0.111/32838;tcp,
Total sessions: 1
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow gate

**Syntax**

**show security flow gate**
[<filter>] [brief | summary}

**Release Information**

Command introduced in Release 8.5 of Junos OS; Filter and display options added in Release 10.2 of Junos OS.

**Description**

Display information about temporary openings known as pinholes or gates in the security firewall.

Pinholes are used by applications that commonly have both control and data sessions and must create openings in the firewall for the data sessions based on information from the parent sessions.

**Options**

- destination-port—Destination port
- destination-prefix—Destination IP prefix or address
- protocol—IP protocol number
- source-port—Source port
- source-prefix—Source IP prefix or address
- brief | summary—Display the specified level of output.

**Required Privilege Level**

view

**Related Documentation**

- show security flow gate brief node on page 1839
- show security flow gate destination-port on page 1845
- show security flow gate destination-prefix on page 1849
- show security flow gate protocol on page 1856
- show security flow gate source-port on page 1860
- show security flow gate source-prefix on page 1864
- show security flow gate summary node on page 1868

**List of Sample Output**

show security flow gate on page 1837
show security flow gate brief on page 1837
show security flow gate summary on page 1838

**Output Fields**

Table 108 on page 1836 lists the output fields for the **show security flow gate** command. Output fields are listed in the approximate order in which they appear.

Copyright © 2013, Juniper Networks, Inc.

### Table 108: show security flow gate Output Fields

| Field Name | Field Description |
|---|---|
| **Hole** | Range of flows permitted by the pinhole. |
| **Translated** | Tuples used to create the session if it matches the pinhole.<br>• Source address and port<br>• Destination address and port |
| **Protocol** | Application protocol, such as UDP or TCP. |
| **Application** | Name of the application. |
| **Age** | Idle timeout for the pinhole. |
| **Flags** | Internal debug flags for the pinhole. |
| **Zone** | Incoming zone. |
| **Reference count** | Number of resource manager references to the pinhole. |
| **Resource** | Resource manager information about the pinhole. |
| **Valid gates** | Number of valid gates. |
| **Pending gates** | Number of pending gates. |
| **Invalidated gates** | Number of invalid gates. |
| **Gates in other states** | Number of gates in other states. |
| **Total gates** | Number of gates in total. |
| **Maximum gates** | Number of maximum gates |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow gate

```
user@host> show security flow gate
Hole: 0.0.0.0-0.0.0.0/0-0->40.1.1.252-40.1.1.252/64515-64515
Translated: 0.0.0.0/0->11.0.31.161/25415
Protocol: udp
Application: none/0
Age: 101 seconds
Flags: 0xe001
Zone: untrust
Reference count: 1
Resource: 5-1024-8185
Hole: 0.0.0.0-0.0.0.0/0-0->40.1.1.252-40.1.1.252/1046-1046
Translated: 40.1.1.250/36039->11.0.31.161/5060
Protocol: udp
Application: junos-sip/63
Age: 65535 seconds
Flags: 0xe200
Zone: untrust
Reference count: 1
Resource: 5-1024-8189
Hole: 0.0.0.0-0.0.0.0/0-0->40.1.1.5-40.1.1.5/24101-24101
Translated: 0.0.0.0/0->40.1.1.5/24101
Protocol: udp
Application: none/0
Age: 93 seconds
Flags: 0xe001
Zone: trust
Reference count: 1
Resource: 5-1024-8188
Hole: 0.0.0.0-0.0.0.0/0-0->40.1.1.5-40.1.1.5/24100-24100
Translated: 0.0.0.0/0->40.1.1.5/24100
Protocol: udp
Application: none/0
Age: 93 seconds
Flags: 0xe001
Zone: trust
Reference count: 1
Resource: 5-1024-8191
Hole: 0.0.0.0-0.0.0.0/0-0->40.1.1.250-40.1.1.250/5060-5060
Translated: 0.0.0.0/0->40.1.1.250/5060
Protocol: udp
Application: junos-sip/63
Age: 65535 seconds
Flags: 0xe200
Zone: trust
Reference count: 1
Resource: 5-1024-8190
```

### show security flow gate brief

```
root> show security flow gate brief
Flow Gates on FPC4 PIC1:

Hole: 40.0.0.111-40.0.0.111/0-0->30.0.0.100-30.0.0.100/38143-38143
  Translated: 40.0.0.111/0->30.0.0.100/38143
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65532 seconds
  Flags: 0x0080
  Zone: trust
```

Copyright © 2013, Juniper Networks, Inc.

```
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

### show security flow gate summary

```
root> show security flow gate summary
Flow Gates on FPC4 PIC1:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow gate brief node

**Syntax** **show security flow gate brief node (*node-id* | all | local | primary)**

**Release Information** Command introduced in Release 8.5 of Junos OS; node options added in Release 9.0 of Junos OS. Filter options added in Release 10.2 of Junos OS.

**Description** Display information about temporary openings known as pinholes or gates in the security firewall for the specified node options in brief mode.

**Options** **node**—(Optional) For chassis cluster configurations, display gate information on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**
- show security flow gate on page 1835
- show security flow gate summary node on page 1868

**List of Sample Output**
show security flow gate brief node 0 on page 1841
show security flow gate brief node 1 on page 1841
show security flow gate brief node all on page 1842
show security flow gate brief node local on page 1843
show security flow gate brief node primary on page 1844

**Output Fields** Table 109 on page 1839 lists the output fields for the **show security flow gate brief node** command. Output fields are listed in the approximate order in which they appear.

### Table 109: show security flow gate brief node Output Fields

| Field Name | Field Description |
|---|---|
| **Valid gates** | Number of valid gates. |
| **Pending gates** | Number of pending gates. |
| **Invalidated gates** | Number of invalid gates. |
| **Gates in other states** | Number of gates in other states. |
| **Total gates** | Number of gates in total. |
| **Hole** | Range of flows permitted by the pinhole. |

Copyright © 2013, Juniper Networks, Inc.

Table 109: show security flow gate brief node Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Translated** | Tuples used to create the session if it matches the pinhole.<br>• Source address and port<br>• Destination address and port |
| **Protocol** | Application protocol, such as UDP or TCP. |
| **Application** | Name of the application. |
| **Age** | Idle timeout for the pinhole. |
| **Flags** | Internal debug flags for the pinhole. |
| **Zone** | Incoming zone. |
| **Reference count** | Number of resource manager references to the pinhole. |
| **Resource** | Resource manager information about the pinhole. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow gate brief node 0

```
root@antbert> show security flow gate brief node 0
node0:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC4 PIC0:

Hole: 1.0.0.100-1.0.0.100/0-0->2.0.0.100-2.0.0.100/32707-32707
  Translated: 1.0.0.100/0->2.0.0.100/32707
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65518 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

### show security flow gate brief node 1

```
root@antbert> show security flow gate brief node 1
node1:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC4 PIC0:

Hole: 1.0.0.100-1.0.0.100/0-0->2.0.0.100-2.0.0.100/32707-32707
  Translated: 1.0.0.100/0->2.0.0.100/32707
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65514 seconds
```

Copyright © 2013, Juniper Networks, Inc.

```
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

### show security flow gate brief node all

```
root@antbert> show security flow gate brief node all
node0:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC4 PIC0:

Hole: 1.0.0.100-1.0.0.100/0-0->2.0.0.100-2.0.0.100/32707-32707
  Translated: 1.0.0.100/0->2.0.0.100/32707
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65512 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

node1:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:
```


Copyright © 2013, Juniper Networks, Inc.

```
Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC4 PIC0:

Hole: 1.0.0.100-1.0.0.100/0-0->2.0.0.100-2.0.0.100/32707-32707
  Translated: 1.0.0.100/0->2.0.0.100/32707
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65510 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

## show security flow gate brief node local

```
root@antbert> show security flow gate brief node local
node0:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC4 PIC0:

Hole: 1.0.0.100-1.0.0.100/0-0->2.0.0.100-2.0.0.100/32707-32707
  Translated: 1.0.0.100/0->2.0.0.100/32707
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65504 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
```

```
Total gates: 1

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

### show security flow gate brief node primary

```
root@antbert> show security flow gate brief node primary
node0:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC4 PIC0:

Hole: 1.0.0.100-1.0.0.100/0-0->2.0.0.100-2.0.0.100/32707-32707
  Translated: 1.0.0.100/0->2.0.0.100/32707
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65500 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow gate destination-port

**Syntax** **show security flow gate destination-port *destination-port-number* [brief | summary]**

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display information about temporary openings known as pinholes or gates in the security firewall that for the specified destination port.

NOTE: **Destination port filter matches the gate only if the given port falls within the range of ports specified in the gate.**

**Options**

- *destination-port-number*—Number of the destination port for which to display gate information.

  **Range**: 1 through 65,535

- brief | summary—Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**

- show security flow gate on page 1835
- show security flow gate destination-prefix on page 1849

**List of Sample Output**

show security flow gate destination-port brief on page 1847
show security flow gate destination-port summary on page 1847

**Output Fields** Table 110 on page 1845 lists the output fields for the **show security flow gate destination-port** command. Output fields are listed in the approximate order in which they appear.

### Table 110: show security flow gate destination-port Output Fields

| Field Name | Field Description |
|---|---|
| Hole | Range of flows permitted by the pinhole. |
| Translated | Tuples used to create the session if it matches the pinhole.<br>• Source address and port<br>• Destination address and port |
| Protocol | Application protocol, such as UDP or TCP. |
| Application | Name of the application. |
| Age | Idle timeout for the pinhole. |

Copyright © 2013, Juniper Networks, Inc.

Table 110: show security flow gate destination-port Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| Flags | Internal debug flags for the pinhole. |
| Zone | Incoming zone. |
| Reference count | Number of resource manager references to the pinhole. |
| Resource | Resource manager information about the pinhole. |
| Valid gates | Number of valid gates. |
| Pending gates | Number of pending gates. |
| Invalidated gates | Number of invalid gates. |
| Gates in other states | Number of gates in other states. |
| Total gates | Number of gates in total. |
| Maximum gates | Number of maximum gates. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow gate destination-port brief

```
root> show security flow gate destination-port 33253 brief
Flow Gates on FPC4 PIC1:

Hole: 40.0.0.111-40.0.0.111/0-0->30.0.0.100-30.0.0.100/33253-33253
  Translated: 40.0.0.111/0->30.0.0.100/33253
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65526 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

### show security flow gate destination-port summary

```
root> show security flow gate destination-port 33253 summary
Flow Gates on FPC4 PIC1:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC5 PIC1:

Valid gates: 0
```

Copyright © 2013, Juniper Networks, Inc.

```
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow gate destination-prefix

**Syntax** **show security flow gate destination-prefix *destination-IP-prefix* [brief | summary]**

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display information about temporary openings known as pinholes or gates in the security firewall for the specified destination prefix.



NOTE: **Destination prefix must match both the starting and ending address in the gate.**

**Options**

- *destination-IP-prefix*—Destination IP prefix or address for which to display gate information.
- brief | summary—Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**

- show security flow gate on page 1835
- show security flow gate destination-port on page 1845

**List of Sample Output**

show security flow gate destination-prefix brief on page 1851
show security flow gate destination-prefix summary on page 1851

**Output Fields** Table 111 on page 1849 lists the output fields for the **show security flow gate destination-prefix** command. Output fields are listed in the approximate order in which they appear.

### Table 111: show security flow gate destination-prefix Output Fields

| Field Name | Field Description |
|---|---|
| Hole | Range of flows permitted by the pinhole. |
| Translated | Tuples used to create the session if it matches the pinhole.<br>• Source address and port<br>• Destination address and port |
| Protocol | Application protocol, such as UDP or TCP. |
| Application | Name of the application. |
| Age | Idle timeout for the pinhole. |
| Flags | Internal debug flags for the pinhole. |

Copyright © 2013, Juniper Networks, Inc.

Table 111: show security flow gate destination-prefix Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| Zone | Incoming zone. |
| Reference count | Number of resource manager references to the pinhole. |
| Resource | Resource manager information about the pinhole. |
| Valid gates | Number of valid gates. |
| Pending gates | Number of pending gates. |
| Invalidated gates | Number of invalid gates. |
| Gates in other states | Number of gates in other states. |
| Total gates | Number of gates in total. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow gate destination-prefix brief

```
root> show security flow gate destination-prefix 30.0.0.100 brief
Hole: 40.0.0.111-40.0.0.111/0-0->30.0.0.100-30.0.0.100/37308-37308
  Translated: 40.0.0.111/0->30.0.0.100/37308
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65456 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24575-86015

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

### show security flow gate destination-prefix summary

```
root> show security flow gate destination-prefix 30.0.0.100 summary
Flow Gates on FPC4 PIC1:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

## show security flow gate family

**Syntax** show security flow gate family (inet | inet6)

**Release Information** Command introduced in Release 10.4 of Junos OS.

**Description** Display filtered summary of information about existing gates, types of gates, and the maximum allowed number of gates.

**Options**
- inet—Displays IPv4 information.
- inet6—Displays IPv6 gate information.

**Required Privilege Level** view

**Related Documentation**
- Layer 2 Bridging and Transparent Mode for Security Devices
- show security flow gate on page 1835

**Output Fields** Table 1 lists the output fields for the **show security flow gate family** command. Output fields are listed in the approximate order in which they appear.

### Table 112: show security flow gate family Output Fields

| Field Name | Field Description |
|---|---|
| **Valid gates** | Number of valid gates. |
| **Pending gates** | Number of pending gates. |
| **Invalidated gates** | Number of invalid gates. |
| **Gates in other states** | Number of gates in other states. |
| **Total gates** | Total number of gates. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

```
user@host> show security flow gate family inet6
Hole: 2001:13::8-0-0->2001:12::8-33135-33135

  Translated: ::/0->::/0

  Protocol: tcp

  Application: FTP ALG/79

  Age: 24 seconds

  Flags: 0x8080

  Zone: zserver

  Reference count: 1

  Resource: 1-2-2


Valid gates: 1

Pending gates: 0

Invalidated gates: 0

Gates in other states: 0

Total gates: 1
```

```
user@host> show security flow gate family inet6 destination-prefix 2001:12::8 or source-prefix
Hole: 2001:13::8-0-0->2001:12::8-33135-33135

  Translated: ::/0->::/0

  Protocol: tcp

  Application: FTP ALG/79

  Age: 26 seconds

  Flags: 0x8080

  Zone: zserver

  Reference count: 1

  Resource: 1-2-2


Valid gates: 1

Pending gates: 0

Invalidated gates: 0
```


Copyright © 2013, Juniper Networks, Inc.

```
Gates in other states: 0

Total gates: 1
```

Copyright © 2013, Juniper Networks, Inc.

## show security flow gate protocol

**Syntax** **show security flow gate protocol *protocol-name* [brief | summary]**

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display information about temporary openings known as pinholes or gates in the security firewall for the specified protocol.

**Options**

- *protocol-name* —Protocol to use as a gate filter. Information about gates that use this protocol is displayed.

  Possible protocols are:

  - ah—IP Security Authentication Header
  - egp—Exterior gateway protocol
  - esp—IPsec Encapsulating Security Payload
  - gre—Generic routing encapsulation
  - icmp—Internet Control Message Protocol
  - icmp6—Internet Control Message Protocol
  - igmp—Internet Group Management Protocol
  - ipip—IP over IP
  - ospf—Open Shortest Path First
  - pim—Protocol Independent Multicast
  - rsvp—Resource Reservation Protocol
  - sctp—Stream Control Transmission Protocol
  - tcp—Transmission Control Protocol
  - udp—User Datagram Protocol

- brief | summary—Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**

- show security flow gate on page 1835

**List of Sample Output**

show security flow gate protocol brief on page 1858
show security flow gate protocol summary on page 1858

**Output Fields** Table 113 on page 1857 lists the output fields for the **show security flow gate protocol** command. Output fields are listed in the approximate order in which they appear.


Copyright © 2013, Juniper Networks, Inc.

### Table 113: show security flow gate protocol Output Fields

| Field Name | Field Description |
|---|---|
| Hole | Range of flows permitted by the pinhole. |
| Translated | Tuples used to create the session if it matches the pinhole.<br>• Source address and port<br>• Destination address and port |
| Protocol | Application protocol, such as UDP or TCP. |
| Application | Name of the application. |
| Age | Idle timeout for the pinhole. |
| Flags | Internal debug flags for the pinhole. |
| Zone | Incoming zone. |
| Reference count | Number of resource manager references to the pinhole. |
| Resource | Resource manager information about the pinhole. |
| Valid gates | Number of valid gates. |
| Pending gates | Number of pending gates. |
| Invalidated gates | Number of invalid gates. |
| Gates in other states | Number of gates in other states. |
| Total gates | Number of gates in total. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow gate protocol brief

```
root> root> show security flow gate protocol tcp brief
Hole: 40.0.0.111-40.0.0.111/0-0->30.0.0.100-30.0.0.100/37308-37308
  Translated: 40.0.0.111/0->30.0.0.100/37308
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65414 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24575-86015

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

### show security flow gate protocol summary

```
root> show security flow gate protocol tcp summary
Flow Gates on FPC4 PIC1:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```


Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

## show security flow gate source-port

**Syntax** **show security flow gate source-port** *source-port-number* **[brief | summary]**

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display information about temporary openings known as pinholes or gates in the security firewall for the specified source port.



NOTE: Source port filter matches the gate only if the given port falls within the range of ports specified in the gate.

**Options**

- *source-port-number*—Number of the source port for which to display gate information.

  **Range**: 1 through 65,535

- brief | summary—Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**

- show security flow gate on page 1835
- show security flow gate source-prefix on page 1864

**List of Sample Output**

show security flow gate source-port brief on page 1862
show security flow gate source-port summary on page 1862

**Output Fields** Table 114 on page 1860 lists the output fields for the **show security flow gate source-port** command. Output fields are listed in the approximate order in which they appear.

### Table 114: show security flow gate source-port Output Fields

| Field Name | Field Description |
|---|---|
| Hole | Range of flows permitted by the pinhole. |
| Translated | Tuples used to create the session if it matches the pinhole.<br>• Source address and port<br>• Destination address and port |
| Protocol | Application protocol, such as UDP or TCP. |
| Application | Name of the application. |
| Age | Idle timeout for the pinhole. |
| Flags | Internal debug flags for the pinhole. |


Copyright © 2013, Juniper Networks, Inc.

Table 114: show security flow gate source-port Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| Zone | Incoming zone. |
| Reference count | Number of resource manager references to the pinhole. |
| Resource | Resource manager information about the pinhole. |
| Valid gates | Number of valid gates. |
| Pending gates | Number of pending gates. |
| Invalidated gates | Number of invalid gates. |
| Gates in other states | Number of gates in other states. |
| Total gates | Number of gates in total. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow gate source-port brief

```
root> show security flow gate source-port 5004 brief
Flow Gates on FPC4 PIC1:

Hole: 30.0.0.111-30.0.0.111/5004-5004->40.0.0.100-40.0.0.100/2646-2646
  Translated: 0.0.0.0/0->0.0.0.0/0
  Protocol: udp
  Application: RTSP ALG/0
  Age: 28 seconds
  Flags: 0x0080
  Zone: untrust
  Reference count: 1
  Resource: 0-1050869761-1050869762

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

### show security flow gate source-port summary

```
root> show security flow gate source-port 5004 summary
Flow Gates on FPC4 PIC1:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
```


Copyright © 2013, Juniper Networks, Inc.

```
Gates in other states: 0
Total gates: 0
```

Copyright © 2013, Juniper Networks, Inc.

## show security flow gate source-prefix

**Syntax** **show security flow gate source-prefix *source-IP-prefix* [brief | summary]**

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display information about temporary openings known as pinholes or gates in the security firewall for the specified source prefix.

NOTE: **Source prefix must match both the starting and ending address in the gate.**

**Options**

- source-IP-prefix—Source IP prefix or address for which to display gate information.
- brief | summary—Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**

- show security flow gate on page 1835
- show security flow gate source-port on page 1860

**List of Sample Output**

show security flow gate source-prefix brief on page 1866
show security flow gate source-prefix summary on page 1866

**Output Fields** Table 115 on page 1864 lists the output fields for the **show security flow gate source-prefix** command. Output fields are listed in the approximate order in which they appear.

### Table 115: show security flow gate source-prefix Output Fields

| Field Name | Field Description |
|---|---|
| Hole | Range of flows permitted by the pinhole. |
| Translated | Tuples used to create the session if it matches the pinhole.<br>• Source address and port<br>• Destination address and port |
| Protocol | Application protocol, such as UDP or TCP. |
| Application | Name of the application. |
| Age | Idle timeout for the pinhole. |
| Flags | Internal debug flags for the pinhole. |
| Zone | Incoming zone. |


Copyright © 2013, Juniper Networks, Inc.

Table 115: show security flow gate source-prefix Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| Reference count | Number of resource manager references to the pinhole. |
| Resource | Resource manager information about the pinhole. |
| Valid gates | Number of valid gates. |
| Pending gates | Number of pending gates. |
| Invalidated gates | Number of invalid gates. |
| Gates in other states | Number of gates in other states. |
| Total gates | Number of gates in total. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow gate source-prefix brief

```
root> show security flow gate source-prefix 30.0.0.100 brief
Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC0:

Hole: 30.0.0.100-30.0.0.100/0-0->40.0.0.111-40.0.0.111/32834-32834
  Translated: 30.0.0.100/0->40.0.0.111/32834
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65442 seconds
  Flags: 0x0080
  Zone: untrust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

### show security flow gate source-prefix summary

```
root> show security flow gate source-prefix 30.0.0.100 summary
Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0

Flow Gates on FPC5 PIC0:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
```


Copyright © 2013, Juniper Networks, Inc.

```
Gates in other states: 0
Total gates: 0
```

Copyright © 2013, Juniper Networks, Inc.

## show security flow gate summary node

**Syntax** **show security flow gate summary node (*node-id* | all | local | primary)**

**Release Information** Command introduced in Release 8.5 of Junos OS; node options added in Release 9.0 of Junos OS. Filter options added in Release 10.2 of Junos OS.

**Description** Display information about temporary openings known as pinholes or gates in the security firewall for the specified node options in summary mode.

**Options** **node**—(Optional) For chassis cluster configurations, display gate information on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**
- show security flow gate
- show security flow gate brief node on page 1839

**List of Sample Output**
show security flow gate summary node 0 on page 1870
show security flow gate summary node 1 on page 1870
show security flow gate summary node all on page 1871
show security flow gate summary node local on page 1872
show security flow gate summary node primary on page 1872

**Output Fields** Table 116 on page 1868 lists the output fields for the **show security flow gate summary node** command. Output fields are listed in the approximate order in which they appear.

### Table 116: show security flow gate summary node Output Fields

| Field Name | Field Description |
|---|---|
| **Valid gates** | Number of valid gates. |
| **Pending gates** | Number of pending gates. |
| **Invalidated gates** | Number of invalid gates. |
| **Gates in other states** | Number of gates in other states. |
| **Total gates** | Number of gates in total. |
| **Hole** | Range of flows permitted by the pinhole. |


Copyright © 2013, Juniper Networks, Inc.

Table 116: show security flow gate summary node Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Translated** | Tuples used to create the session if it matches the pinhole.<br>• Source address and port<br>• Destination address and port |
| **Protocol** | Application protocol, such as UDP or TCP. |
| **Application** | Name of the application. |
| **Age** | Idle timeout for the pinhole. |
| **Flags** | Internal debug flags for the pinhole. |
| **Zone** | Incoming zone. |
| **Reference count** | Number of resource manager references to the pinhole. |
| **Resource** | Resource manager information about the pinhole. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow gate summary node 0

```
root@antbert> show security flow gate summary node 0
node0:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC4 PIC0:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072
```

### show security flow gate summary node 1

```
root@antbert> show security flow gate summary node 1
node1:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC4 PIC0:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
```


Copyright © 2013, Juniper Networks, Inc.

```
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072
```

### show security flow gate summary node all

```
root@antbert> show security flow gate summary node all
node0:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC4 PIC0:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

node1:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC4 PIC0:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
```

```
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072
```

### show security flow gate summary node local

```
root@antbert> show security flow gate summary node local
node0:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC4 PIC0:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC4 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072
```

### show security flow gate summary node primary

```
root@antbert> show security flow gate summary node primary
node0:
--------------------------------------------------------------------------

Flow Gates on FPC3 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC4 PIC0:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC4 PIC1:
```


Copyright © 2013, Juniper Networks, Inc.

```
Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072
```

Copyright © 2013, Juniper Networks, Inc.

## show security flow ip-action

**Syntax** **show security flow ip-action** [ <filter> ] [ summary family (inet | inet6) ]

**Release Information** Command introduced in Release 10.1 of Junos OS. Logical systems option added in Release 11.2 of Junos OS. Summary option introduced in Release 12.1 of Junos OS.

**Description** Display the current IP-action settings, based on filtered options, for IP sessions running on the device.

**Options**

- *filter*—Filter the display based on the specified criteria.

  The following filters display those sessions that match the criteria specified by the filter. Refer to the sample output for filtered output examples.

  **all |** [*filter*]—All active sessions on the device.

  **destination-port** ***destination-port***—Destination port number of the traffic. Range is 1 through 65,535.

  **destination-prefix** ***destination-prefix***—Destination IP prefix or address.

  **family (inet | inet6)** [*filter*]—IPv4 traffic or IPv6-NATPT traffic and filtered options.

  **logical-system** ***logical-system-name*** **| all** [*filter*]—Specified logical system or all logical systems.

  **protocol** ***protocol-name*** **|** ***protocol-number*** [*filter*]—Protocol name or number and filtered options.

  - **ah** or **51**
  - **egp** or **8**
  - **esp** or **50**
  - **gre** or **47**
  - **icmp** or **1**
  - **icmp6** or **58**
  - **igmp** or **2**
  - **ipip** or **4**
  - **ospf** or **89**
  - **pim** or **103**
  - **rsvp** or **46**
  - **sctp** or **132**
  - **tcp** or **6**
  - **udp** or **17**

  **root-logical-system** [*filter*]—Default logical system information and filtered options.


Copyright © 2013, Juniper Networks, Inc.

**source-port *source-port***—Source port number of the traffic. Range is 1 through 65,535.

**source-prefix *source-prefix***—Source IP prefix or address of the traffic.

- **summary** —Summary information about IP-action entries.

  **family**—Display summary of IP-action entries by family. This option is used to filter the output.

  - **inet**—Display summary of IPv4 entries.
  - **inet6**—Display summary of IPv6 entries.

**Required Privilege Level** view

**Related Documentation**

- Layer 2 Bridging and Transparent Mode for Security Devices
- clear security flow ip-action on page 1406

**List of Sample Output**

show security flow ip-action destination-port on page 1877
show security flow ip-action destination-prefix on page 1877
show security flow ip-action family inet protocol on page 1877
show security flow ip-action family inet logical-system all on page 1877
show security flow ip-action source-prefix on page 1877
show security flow ip-action | count on page 1877
show security flow ip-action summary on page 1877
show security flow ip-action summary family inet on page 1878
show security flow ip-action summary family inet6 on page 1878

**Output Fields** Table 117 on page 1875 lists the output fields for the **show security flow ip-action** command. Output fields are listed in the approximate order in which they appear.

### Table 117: show security flow ip-action Output Fields

| Field Name | Field Description |
|---|---|
| **Src-Addr** | Source address of outbound IP traffic. |
| **Src-Port** | Source port number of outbound IP traffic. |
| **Dst-Addr** | Destination address of inbound IP traffic. |
| **Dst-Port/Proto** | Destination port number and protocol type of inbound IP traffic. |
| **Timeout (sec)** | Configured timeouts and time remaining for an IP session. |
| **Zone** | Security zone associated with an IP session. |
| **Action** | Configured action type, for example, block, close, and notify. |
| **IPv4 action count** | The total number of IPv4 entries. |

Copyright © 2013, Juniper Networks, Inc.

Table 117: show security flow ip-action Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **IPv6 action count** | The total number of IPv6 entries. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow ip-action destination-port

```
user@host> show security flow ip-action destination-port 161

Src-Addr        Src-Port Dst-Addr Dst-Port/Proto Timeout(sec) Zone Action
146.107.179.107 *        5.0.0.1  161/udp        200/200      *    close
27.38.182.32    *        5.0.0.1  161/udp        198/200      *    close
53.69.226.79    *        5.0.0.1  161/udp        175/200      *    close
220.53.101.56   *        5.0.0.1  161/udp        159/200      *    close
98.114.199.126  *        5.0.0.1  161/udp        194/200      *    close
```

### show security flow ip-action destination-prefix

```
user@host> show security flow ip-action destination-prefix 5.0.0.0/8

Src-Addr        Src-Port Dst-Addr Dst-Port/Proto Timeout(sec) Zone Action
146.107.179.107 *        5.0.0.1  161/udp        200/200      *    close
27.38.182.32    *        5.0.0.1  161/udp        198/200      *    close
53.69.226.79    *        5.0.0.1  161/udp        175/200      *    close
220.53.101.56   *        5.0.0.1  161/udp        159/200      *    close
98.114.199.126  *        5.0.0.1  161/udp        194/200      *    close
```

### show security flow ip-action family inet protocol

```
user@host> show security flow ip-action family inet protocol icmp

Src-Addr        Src-Port Dst-Addr Dst-Port/Proto Timeout(sec) Zone Action
190.205.17.194  *        5.0.0.1  0/icmp         87/200       *    close
125.185.38.244  *        5.0.0.1  0/icmp         156/200      *    close
201.46.164.123  *        5.0.0.1  0/icmp         174/200      *    close
66.64.249.134   *        5.0.0.1  0/icmp         97/200       *    close
104.65.181.148  *        5.0.0.1  0/icmp         167/200      *    close
```

### show security flow ip-action family inet logical-system all

```
user@host> show security flow ip-action family inet logical-system all

Src-Addr        Src-Port Dst-Addr Dst-Port/Proto Timeout(sec) Zone Action
175.87.147.87   *        *        */*            51/200       *    close
32.28.234.28    *        *        */*            112/200      *    close
24.231.158.231  *        *        */*            124/200      *    close
0.113.112.113   *        *        */*            138/200      *    close
```

### show security flow ip-action source-prefix

```
user@host> show security flow ip-action source-prefix 212.0.0.0/8

Src-Addr        Src-Port Dst-Addr Dst-Port/Proto Timeout(sec) Zone Action
212.178.48.164  *        *        */*            21/200       *    close
212.141.190.190 *        *        */*            93/200       *    close
212.193.112.136 *        *        */*            145/200      *    close
212.235.103.142 *        5.0.0.1  161/udp        171/200      *    close
212.4.132.110   *        *        */*            181/200      *    close
```

### show security flow ip-action | count

```
user@host> show security flow ip-action | count

 Count: 203 lines
```

### show security flow ip-action summary

```
user@host> show security flow ip-action summary

 IPv4 action count: 2000
```

Copyright © 2013, Juniper Networks, Inc.

```
IPv6 action count: 0
```

### show security flow ip-action summary family inet

```
user@host> show security flow ip-action summary

IPv4 action count: 50
```

### show security flow ip-action summary family inet6

```
user@host> show security flow ip-action summary family inet6

IPv6 action count: 0
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow session

**Syntax** **show security flow session**
[*filter* ] **[brief | extensive | summary ]**

**Release Information** Command introduced in Release 8.5 of Junos OS. Filter and view options added in Release 10.2 of Junos OS. Application firewall, dynamic application, and logical system filters added in Release 11.2 of Junos OS.

**Description** Display information about all currently active security sessions on the device.

**Options**

- *filter*—Filter the display by the specified criteria.

  The following filters reduce the display to those sessions that match the criteria specified by the filter. Refer to the specific **show** command for examples of the filtered output.

  **application**—Application name

  **application-firewall**—Application firewall enabled

  **application-firewall-rule-set**—Application firewall enabled with the specified rule-set

  **application-traffic-control**—Application traffic control rule set name and rule name

  **destination-port**—Destination port

  **destination-prefix**—Destination IP prefix or address

  **dynamic-application**—Dynamic application or nested dynamic application

  **dynamic-application-group**—Dynamic application or nested dynamic application group

  **encrypted**—Encrypted traffic.

  **family**—Display session by family

  **idp**—IDP enabled sessions

  **interface**—Name of incoming or outgoing interface

  **logical-system (all | *logical-system-name*)**—Name of a specific logical system or **all** to display all logical systems

  **nat**—Display sessions with network address translation

  **protocol**—IP protocol number

  **resource-manager**—Resource manager

  **session-identifier**—Session identifier

  **source-port**—Source port

Copyright © 2013, Juniper Networks, Inc.

**source-prefix**—Source IP prefix

**tunnel**—Tunnel sessions

- brief | extensive | summary—Display the specified level of output.
- none—Display information about all active sessions.

**Required Privilege Level** view

**Related Documentation**
- Application Identification for Security Devices
- Application Firewall
- Application Quality of Service
- clear security flow session all on page 1408
- Logical Systems for Security Devices

**List of Sample Output**
show security flow session on page 1882
show security flow session brief on page 1882
show security flow session extensive on page 1882
show security flow session summary on page 1883

**Output Fields** Table 118 on page 1880 lists the output fields for the **show security flow session** command. Output fields are listed in the approximate order in which they appear.

Table 118: show security flow session Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the session. Use this ID to get more information about the session. |
| **Policy name** | Policy that permitted the traffic. |
| **Timeout** | Idle timeout after which the session expires. |
| **In** | Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Out** | Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Total sessions** | Total number of sessions. |
| **Status** | Session status. |
| **Flag** | Internal flag depicting the state of the session, used for debugging purposes. |
| **Policy name** | Name and ID of the policy that the first packet of the session matched. |


Copyright © 2013, Juniper Networks, Inc.

Table 118: show security flow session Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Source NAT pool** | The name of the source pool where NAT is used. |
| **Dynamic application** | Name of the application. |
| **Application traffic control rule-set** | AppQoS rule set for this session. |
| **Rule** | AppQoS rule for this session. |
| **Forwarding class** | The AppQoS forwarding class name for this session that distinguishes the transmission priority |
| **DSCP code point** | Differentiated Services (DiffServ) code point (DSCP) value remarked by the matching rule for this session. |
| **Loss priority** | One of four priority levels set by the matching rule to control discarding a packet during periods of congestion. A high loss priority means a high probability that the packet could be dropped during a period of congestion. |
| **Rate limiter client to server** | The rate-limiter profile assigned to the client-to-server traffic defining a unique combination of **bandwidth-limit** and **burst-size-limit** specifications. |
| **Rate limiter server to client** | The rate-limiter profile assigned to the server-to-client traffic defining a unique combination of **bandwidth-limit** and **burst-size-limit** specifications. |
| **Maximum timeout** | Maximum session timeout. |
| **Current timeout** | Remaining time for the session unless traffic exists in the session. |
| **Session State** | Session state. |
| **Start time** | Time when the session was created, offset from the system start time. |
| **Unicast-sessions** | Number of unicast sessions. |
| **Multicast-sessions** | Number of multicast sessions. |
| **Failed-sessions** | Number of failed sessions. |
| **Sessions-in-use** | Number of sessions in use.<br>• Valid sessions<br>• Pending sessions<br>• Invalidated sessions<br>• Sessions in other states |
| **Maximum-sessions** | Maximum number of sessions permitted. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session

```
root> show security flow session
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Session ID: 200000001, Policy name: default-policy/2, Timeout: 1794, Valid
  In: 40.0.0.111/32852 --> 30.0.0.100/21;tcp, If: ge-0/0/2.0, Pkts: 25, Bytes:
1138
  Out: 30.0.0.100/21 --> 40.0.0.111/32852;tcp, If: ge-0/0/1.0, Pkts: 20, Bytes:
1152
Total sessions: 1

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session brief

```
root> show security flow session brief
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Session ID: 200000001, Policy name: default-policy/2, Timeout: 1794, Valid
  In: 40.0.0.111/32852 --> 30.0.0.100/21;tcp, If: ge-0/0/2.0, Pkts: 25, Bytes:
1138
  Out: 30.0.0.100/21 --> 40.0.0.111/32852;tcp, If: ge-0/0/1.0, Pkts: 20, Bytes:
1152
Total sessions: 1

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session extensive

```
root> show security flow session extensive
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:

  Session ID: 3729, Status: Normal, State: Active
  Flag: 0x40
  Policy name: self-traffic-policy/1
  Source NAT pool: Null
  Dynamic application: junos:HTTP, Dynamic nested application: junos:FACEBOOK
  Application traffic control rule-set: ruleset1, Rule: rule2
     Forwarding class: AppQoS-Bad-Traffic, queue number 2
     DSCP code point: 111011
     Loss priority: high
    Rate limiter client to server: Rate1k, bandwidth-limit 1024, burst-size-limit
 1024
    Rate limiter server to client: Rate3k, bandwidth-limit 1024, burst-size-limit
 1024
Maximum timeout: 300, Current timeout: 276
  Session State: Valid
  Start time: 18292, Duration: 603536
     In: 201.34.0.4/1 --> 224.0.0.13/1;pim,
      Interface: reth1.0,
```


Copyright © 2013, Juniper Networks, Inc.

```
      Session token: 0x1c0, Flag: 0x0x21
      Route: 0x0, Gateway: 201.34.0.4, Tunnel: 0
      Port sequence: 0, FIN sequence: 0,
      FIN state: 0,
      Pkts: 21043, Bytes: 1136322
     Out: 224.0.0.13/1 --> 201.34.0.4/1;pim,
      Interface: .local..0,
      Session token: 0x80, Flag: 0x0x30
      Route: 0xfffd0000, Gateway: 224.0.0.13, Tunnel: 0
      Port sequence: 0, FIN sequence: 0,
      FIN state: 0,
      Pkts: 0, Bytes: 0

Total sessions: 1

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

## show security flow session summary

```
root> show security flow session summary
Flow Sessions on FPC4 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 819200

Flow Sessions on FPC5 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 819200

Flow Sessions on FPC5 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 819200
```

Copyright © 2013, Juniper Networks, Inc.

## show security flow session application

**Syntax**

**show security flow session application**
***application-name*** **[brief | extensive | summary]**

**Release Information**

Command introduced in Junos OS Release 8.5. Filter and view options added in Junos OS Release 10.2.

**Description**

Display information about each session of the specified application type.

**Options**

- ***application-name***—Type of application about which to display sessions information. Possible values are:
  - dns—Domain Name System
  - ftp—File Transfer Protocol
  - ignore—Ignore application type
  - mgcp-ca—Media Gateway Control Protocol with Call Agent
  - mgcp-ua—MGCP with User Agent
  - pptp—Point-to-Point Tunneling Protocol
  - q931—ISDN connection control protocol
  - ras—Remote Access Server
  - realaudio—RealAudio
  - rsh—UNIX remote shell services
  - rtsp—Real-Time Streaming Protocol
  - sccp—Skinny Client Control Protocol
  - sip—Session Initiation Protocol
  - sqlnet-v2—Oracle SQLNET
  - talk—TALK program
  - tftp—Trivial File Transfer Protocol
- brief | extensive | summary—Display the specified level of output.

**Required Privilege Level**

view

**Related Documentation**

- clear security flow session application on page 1409
- Security Policy Applications for Security Devices

**List of Sample Output**

show security flow session application telnet on page 1887
show security flow session application telnet brief on page 1887
show security flow session application telnet extensive on page 1887


Copyright © 2013, Juniper Networks, Inc.

show security flow session application telnet summary on page 1888

**Output Fields** Table 119 on page 1885 lists the output fields for the **show security flow session application** command. Output fields are listed in the approximate order in which they appear.

Table 119: show security flow session application Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the session. You can use this ID to get additional information about the session. |
| **Policy name** | Policy that permitted the traffic. |
| **Timeout** | Idle timeout after which the session expires. |
| **In** | Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Out** | Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Total sessions** | Total number of sessions. |
| **Status** | Session status. |
| **Flag** | Internal flag depicting the state of the session, used for debugging purposes. |
| **Policy name** | Name and ID of the policy that the first packet of the session matched. |
| **Source NAT pool** | The name of the source pool where NAT is used. |
| **Application** | Name of the application. |
| **Maximum timeout** | Maximum session timeout. |
| **Current timeout** | Remaining time for the session unless traffic exists in the session. |
| **Session State** | Session state. |
| **Start time** | Time when the session was created, offset from the system start time. |
| **Unicast-sessions** | Number of unicast sessions. |
| **Multicast-sessions** | Number of multicast sessions. |
| **Failed-sessions** | Number of failed sessions. |

Copyright © 2013, Juniper Networks, Inc.

Table 119: show security flow session application Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Sessions-in-use** | Number of sessions in use.<br>• Valid sessions<br>• Pending sessions<br>• Invalidated sessions<br>• Sessions in other states |
| **Maximum-sessions** | Number of maximum sessions. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session application telnet

```
root> show security flow session application telnet
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Session ID: 210067547, Policy name: default-policy/2, Timeout: 1796, Valid
  In: 40.0.0.100/32781 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 10, Bytes:
610
  Out: 30.0.0.100/23 --> 40.0.0.100/32781;tcp, If: ge-0/0/1.0, Pkts: 9, Bytes:
602
Total sessions: 1
```

### show security flow session application telnet brief

```
root> show security flow session application telnet brief
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Session ID: 210067547, Policy name: default-policy/2, Timeout: 1796, Valid
  In: 40.0.0.100/32781 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 10, Bytes:
610
  Out: 30.0.0.100/23 --> 40.0.0.100/32781;tcp, If: ge-0/0/1.0, Pkts: 9, Bytes:
602
Total sessions: 1
```

### show security flow session application telnet extensive

```
root>  show security flow session application telnet extensive
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Session ID: 210067547, Status: Normal
Flag: 0x40
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-telnet/10
Maximum timeout: 1800, Current timeout: 1788
Session State: Valid
Start time: 670184, Duration: 33
   In: 40.0.0.100/32781 --> 30.0.0.100/23;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 10, Bytes: 610
   Out: 30.0.0.100/23 --> 40.0.0.100/32781;tcp,
```

```
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 9, Bytes: 602
Total sessions: 1
```

### show security flow session application telnet summary

```
root> show security flow session application telnet summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow session application-firewall

**Syntax**

show security flow session application-firewall
< dynamic-application (*dyn-app-name* | junos:UNKNOWN) >
< dynamic-application-group (*dyn-app-group* | junos:UNASSIGNED) >
< application-firewall-rule-set *rule-set-name* >
< rule *rule-name* >
< brief | extensive | summary >

**Release Information**

Command introduced in Release 11.2 of Junos OS.

**Description**

Display all sessions where application firewall is enabled.

Include options to filter the output and display only those enabled sessions with the specified features.

**Options**

- **dynamic-application (*dyn-app-name* | junos:UNKNOWN)**—Display only those enabled sessions with the specified dynamic application. Enter **junos:UNKNOWN** to display all enabled sessions where no dynamic application can be determined.
- **dynamic-application-group (*dyn-app-group* | junos:UNASSIGNED)**— Display only those enabled session with the specified dynamic application group. Enter **junos:UNASSIGNED** to display all enabled sessions where no dynamic application group can be determined.
- **application-firewall-rule-set *rule-set-name***—Display only those enabled sessions that match the specified rule set.
- **rule *rule-name***—Display only those enabled sessions that match the specified rule.
- **brief | extensive | summary**—Specify the level of detail for the display.

  The output fields for the **brief** and **summary** options are the same as those of the **show security flow session** command. Only the **extensive** display is different and is shown in the following output table and examples.

**Required Privilege Level**

view

**Related Documentation**

- Application Firewall
- show security flow session on page 1879

**List of Sample Output**

show security flow session application-firewall extensive on page 1891
show security flow session application-firewall dynamic-application junos:FTP extensive on page 1891
show security flow session application-firewall dynamic-application junos:UNKNOWN extensive on page 1892
show security flow session application-firewall dynamic-application-group junos:WEB extensive on page 1893
show security flow session application-firewall application-firewall-rule-set rule-set1 extensive on page 1894

Copyright © 2013, Juniper Networks, Inc.

**Output Fields** Table 120 on page 1890 lists the output fields for the **show security flow session application-firewall extensive** command. Output fields are listed in the approximate order in which they appear in the extensive display.

Table 120: show security flow session application-firewall extensive Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the session. Use this ID to display more information about a session. |
| **Status** | Session status. |
| **State** | Current state of the session: Active, Pending, Closed, Unknown. |
| **Flag** | Internal flag depicting the state of the session. It is used for debugging purposes. |
| **Policy name** | The name of the policy that permitted the traffic. |
| **Source NAT pool** | The name of the source pool where NAT is used. |
| **Dynamic application** | Name of the dynamic application of the session. If the dynamic application has yet to be determined, the output indicates Pending. If the dynamic application cannot be determined, the output indicates junos:UNKNOWN. |
| **Dynamic application group** | Name of the dynamic application group of the session. If the dynamic application cannot be determined, the output indicates junos:UNASSIGNED. |
| **Dynamic nested application** | Name of the dynamic nested application of the session if one exists. If the dynamic nested application is yet to be determined, the output indicates Pending. If the dynamic nested application cannot be determined, the output indicates junos:UNKNOWN. |
| **Application firewall rule-set** | Name of the rule set that the session matched. |
| **Rule** | Name of the rule that the session matched. If the match has not yet been made, the output indicates Pending. If the rule has been deleted since the match was made, the output indicates the rule is invalid. |
| **Maximum timeout** | Maximum amount of idle time allowed for the session. |
| **Current timeout** | Number of seconds that the current session has been idle. |
| **Session State** | Session state. |
| **Start time** | Time when the session was created. Start time is indicated as an offset from the system start time. |
| **In** | Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets, and bytes). |


Copyright © 2013, Juniper Networks, Inc.

Table 120: show security flow session application-firewall extensive Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Out** | Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Total sessions** | Total number of sessions per PIC that fit the display criteria. |

## Sample Output

### show security flow session application-firewall extensive

The displayed information is similar to the **show security flow session** output but includes dynamic application and application firewall details for the session.

```
user@host> show security flow session application-firewall extensive
Flow Sessions on FPC9 PIC0:

     Session ID: 3729, Status: Normal, State: Active
      Policy name: self-traffic-policy/1
      Source NAT pool: Null
     Dynamic application: junos:HTTP, Dynamic nested application: junos:FACEBOOK

      Application firewall rule-set: rule-set1, Rule: rule2
      Maximum timeout: 300, Current timeout: 276
      Session State: Valid
      Start time: 18292, Duration: 603536
         In: 201.34.0.4/1 --> 224.0.0.13/1;pim,
          Interface: reth1.0,
          Session token: 0x1c0, Flag: 0x0x21
          Route: 0x0, Gateway: 201.34.0.4, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 21043, Bytes: 1136322
         Out: 224.0.0.13/1 --> 201.34.0.4/1;pim,
          Interface: .local..0,
          Session token: 0x80, Flag: 0x0x30
          Route: 0xfffd0000, Gateway: 224.0.0.13, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 0, Bytes: 0

     Total sessions: 1
```

### show security flow session application-firewall

Entering a specific dynamic application in the command line filters the output and displays only those sessions with the specified application.

```
user@host> show security flow session application-firewall dynamic-application junos:FTP
extensive
```

Copyright © 2013, Juniper Networks, Inc.

dynamic-application junos:FTP extensive

```
Flow Sessions on FPC3 PIC0:

     Session ID: 180013338, Policy name: policy1/4, Timeout: 1776, Valid
      Dynamic application: junos:FTP
      Application firewall rule-set: rule-set1, Rule: rule1
      Maximum timeout: 300, Current timeout: 276
      Session State: Valid
      Start time: 18292, Duration: 603536
         In: 201.34.0.4/1 --> 224.0.0.13/1;pim,
          Interface: reth1.0,
          Session token: 0x1c0, Flag: 0x0x21
          Route: 0x0, Gateway: 201.34.0.4, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 21043, Bytes: 1136322
         Out: 224.0.0.13/1 --> 201.34.0.4/1;pim,
          Interface: .local..0,
          Session token: 0x80, Flag: 0x0x30
          Route: 0xfffd0000, Gateway: 224.0.0.13, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 0, Bytes: 0

      Total sessions: 1
```

show security flow session application-firewall dynamic-application

Using the keyword **junos:UNKNOWN** displays those enabled sessions where the dynamic application cannot be determined.

```
user@host> show security flow session application-firewall dynamic-application junos:UNKNOWN extensive
```


Copyright © 2013, Juniper Networks, Inc.

### junos:UNKNOWN extensive

```
Flow Sessions on FPC9 PIC0:

     Session ID: 180013338, Policy name: policy1/4, Timeout: 1776, Valid
      Dynamic application: junos:UNKNOWN
      Application firewall rule-set: rule-set1, Rule:rule1
      Maximum timeout: 300, Current timeout: 276
      Session State: Valid
      Start time: 18292, Duration: 603536
         In: 201.34.0.4/1 --> 224.0.0.13/1;pim,
          Interface: reth1.0,
          Session token: 0x1c0, Flag: 0x0x21
          Route: 0x0, Gateway: 201.34.0.4, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 21043, Bytes: 1136322
         Out: 224.0.0.13/1 --> 201.34.0.4/1;pim,
          Interface: .local..0,
          Session token: 0x80, Flag: 0x0x30
          Route: 0xfffd0000, Gateway: 224.0.0.13, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 0, Bytes: 0

      Session ID: 180013339, Policy name: policy1/4, Timeout: 1776, Valid
     Dynamic application: junos:HTTP, Dynamic nested application: junos:UNKNOWN

      Application firewall rule-set: rule-set1, Rule:rule1
      Maximum timeout: 300, Current timeout: 276
      Session State: Valid
      Start time: 18292, Duration: 603536
         In: 201.34.0.4/1 --> 224.0.0.13/1;pim,
          Interface: reth1.0,
          Session token: 0x1c0, Flag: 0x0x21
          Route: 0x0, Gateway: 201.34.0.4, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 21043, Bytes: 1136322
         Out: 224.0.0.13/1 --> 201.34.0.4/1;pim,
          Interface: .local..0,
          Session token: 0x80, Flag: 0x0x30
          Route: 0xfffd0000, Gateway: 224.0.0.13, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 0, Bytes: 0

      Total sessions: 2
```

### show security flow session application-firewall

Entering a specific dynamic application group in the command line filters the output and displays only those sessions with the specified application group.

```
user@host> show security flow session application-firewall dynamic-application-group junos:WEB
extensive
```

Copyright © 2013, Juniper Networks, Inc.

### dynamic-application-group junos:WEB extensive

```
Flow Sessions on FPC9 PIC0:

     Session ID: 180013338, Policy name: policy1/4, Timeout: 1776, Valid
      Dynamic application: junos:HOTMAIL
      Application firewall rule-set: rule-set1, Rule: rule1
      Maximum timeout: 300, Current timeout: 276
      Session State: Valid
      Start time: 18292, Duration: 603536
         In: 201.34.0.4/1 --> 224.0.0.13/1;pim,
          Interface: reth1.0,
          Session token: 0x1c0, Flag: 0x0x21
          Route: 0x0, Gateway: 201.34.0.4, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 21043, Bytes: 1136322
         Out: 224.0.0.13/1 --> 201.34.0.4/1;pim,
          Interface: .local..0,
          Session token: 0x80, Flag: 0x0x30
          Route: 0xfffd0000, Gateway: 224.0.0.13, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 0, Bytes: 0

      Total sessions: 1
```

### show security flow session application-firewall

Specifying a rule set name reduces the display to only those sessions matching the specified rule set.

```
user@host> show security flow session application-firewall application-firewall-rule-set rule-set1
extensive
```


Copyright © 2013, Juniper Networks, Inc.

application-firewall-rule-set rule-set1 extensive

```
Flow Sessions on FPC9 PIC0:

     Session ID: 180013338, Policy name: policy1/4, Timeout: 1776, Valid
      Dynamic application: junos:FTP
      Application firewall rule-set: rule-set1, Rule: rule1
      Maximum timeout: 300, Current timeout: 276
      Session State: Valid
      Start time: 18292, Duration: 603536
         In: 201.34.0.4/1 --> 224.0.0.13/1;pim,
          Interface: reth1.0,
          Session token: 0x1c0, Flag: 0x0x21
          Route: 0x0, Gateway: 201.34.0.4, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 21043, Bytes: 1136322
         Out: 224.0.0.13/1 --> 201.34.0.4/1;pim,
          Interface: .local..0,
          Session token: 0x80, Flag: 0x0x30
          Route: 0xfffd0000, Gateway: 224.0.0.13, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 0, Bytes: 0

     Session ID: 180013339, Policy name: policy1/4, Timeout: 1776, Valid
     Dynamic application: junos:HTTP, Dynamic nested application: junos:FACEBOOK

      Application firewall rule-set: rule-set1, Rule: rule2
      Maximum timeout: 300, Current timeout: 276
      Session State: Valid
      Start time: 18292, Duration: 603536
         In: 201.34.0.4/1 --> 224.0.0.13/1;pim,
          Interface: reth1.0,
          Session token: 0x1c0, Flag: 0x0x21
          Route: 0x0, Gateway: 201.34.0.4, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 21043, Bytes: 1136322
         Out: 224.0.0.13/1 --> 201.34.0.4/1;pim,
          Interface: .local..0,
          Session token: 0x80, Flag: 0x0x30
          Route: 0xfffd0000, Gateway: 224.0.0.13, Tunnel: 0
          Port sequence: 0, FIN sequence: 0,
          FIN state: 0,
          Pkts: 0, Bytes: 0


      Total sessions: 2
```

Copyright © 2013, Juniper Networks, Inc.

## show security flow session brief node

**Syntax** **show security flow session brief node (*node-id* | all | local | primary)**

**Release Information** Command introduced in Release 8.5 of Junos OS; node options added in Release 9.0 of Junos OS. Filter options added in Release 10.2 of Junos OS.

**Description** Display information about all currently active security sessions on the device for the specified node options in brief mode.

**Options** **node**—(Optional) For chassis cluster configurations, display session information on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**
- show security flow session

**List of Sample Output**
show security flow session brief node 0 on page 1898
show security flow session brief node 1 on page 1898
show security flow session brief node all on page 1898
show security flow session brief node local on page 1899
show security flow session brief node primary on page 1899

**Output Fields** Table 121 on page 1896 lists the output fields for the **show security flow session brief node** command. Output fields are listed in the approximate order in which they appear.

### Table 121: show security flow session brief node Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the session. Use this ID to get more information about the session. |
| **Policy name** | Policy that permitted the traffic. |
| **State** | Session state. |
| **Timeout** | Idle timeout after which the session expires. |
| **In** | Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |


Copyright © 2013, Juniper Networks, Inc.

Table 121: show security flow session brief node Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Out** | Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Total sessions** | Total number of sessions. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session brief node 0

```
root@antbert> show security flow session brief node 0
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000011, Policy name: default-policy/2, State: Backup,
Timeout: 13978, Valid
  In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp, If: reth2.0, Pkts: 0, Bytes:
0
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

### show security flow session brief node 1

```
root@antbert> show security flow session brief node 1
node1:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000272, Policy name: default-policy/2, State: Active,
Timeout: 1788, Valid
  In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp, If: reth1.0, Pkts: 69, Bytes:
3024
  Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp, If: reth2.0, Pkts: 62, Bytes:
4002
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

### show security flow session brief node all

```
root@antbert> show security flow session brief node all
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000011, Policy name: default-policy/2, State: Backup,
Timeout: 13972, Valid
  In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp, If: reth2.0, Pkts: 0, Bytes:
0
Total sessions: 1

Flow Sessions on FPC4 PIC1:
```


Copyright © 2013, Juniper Networks, Inc.

```
Total sessions: 0

node1:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000272, Policy name: default-policy/2, State: Active,
Timeout: 1784, Valid
  In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp, If: reth1.0, Pkts: 69, Bytes:
3024
  Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp, If: reth2.0, Pkts: 62, Bytes:
4002
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

### show security flow session brief node local

```
root@antbert> show security flow session brief node local
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000011, Policy name: default-policy/2, State: Backup,
Timeout: 13964, Valid
  In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp, If: reth2.0, Pkts: 0, Bytes:
0
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

### show security flow session brief node primary

```
root@antbert> show security flow session brief node primary
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000011, Policy name: default-policy/2, State: Backup,
Timeout: 13958, Valid
  In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp, If: reth1.0, Pkts: 0, Bytes: 0
  Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp, If: reth2.0, Pkts: 0, Bytes:
0
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

## show security flow session destination-port

**Syntax** **show security flow session destination-port**
***destination-port-number*** **[brief | extensive | summary]**

**Release Information** Command introduced in Release 8.5 of Junos OS; Filter and view options added in Release 10.2 of Junos OS.

**Description** Display information about each session that uses the specified destination port.

**Options**

- ***destination-port-number*** —Number of the destination port for which to display sessions information.
- **Range:** 1 through 65,535

**brief | extensive | summary**—Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**

- clear security flow session destination-port on page 1411

**List of Sample Output**

show security flow session destination-port 23 on page 1902
show security flow session destination-port 23 brief on page 1902
show security flow session destination-port 23 extensive on page 1902
show security flow session destination-port 23 summary on page 1903

**Output Fields** Table 122 on page 1900 lists the output fields for the **show security flow session destination-port** command. Output fields are listed in the approximate order in which they appear.

### Table 122: show security flow session destination-port Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the session. You can use this ID to get additional information about the session. |
| **Policy name** | Policy that permitted the traffic. |
| **Timeout** | Idle timeout after which the session expires. |
| **In** | Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Out** | Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Total sessions** | Total number of sessions. |


Copyright © 2013, Juniper Networks, Inc.

Table 122: show security flow session destination-port Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Status** | Session status. |
| **Flag** | Internal flag depicting the state of the session, used for debugging purposes. |
| **Policy name** | Name and ID of the policy that the first packet of the session matched. |
| **Source NAT pool** | The name of the source pool where NAT is used. |
| **Application** | Name of the application. |
| **Maximum timeout** | Maximum session timeout. |
| **Current timeout** | Remaining time for the session unless traffic exists in the session. |
| **Session State** | Session state. |
| **Start time** | Time when the session was created, offset from the system start time. |
| **Unicast-sessions** | Number of unicast sessions. |
| **Multicast-sessions** | Number of multicast sessions. |
| **Failed-sessions** | Number of failed sessions. |
| **Sessions-in-use** | Number of sessions in use.<br>• Valid sessions<br>• Pending sessions<br>• Invalidated sessions<br>• Sessions in other states |
| **Maximum-sessions** | Number of maximum sessions. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session destination-port 23

```
root> show security flow session destination-port 23
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Session ID: 200067563, Policy name: default-policy/2, Timeout: 1798, Valid
  In: 40.0.0.100/32783 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 10, Bytes:
610
  Out: 30.0.0.100/23 --> 40.0.0.100/32783;tcp, If: ge-0/0/1.0, Pkts: 9, Bytes:
602
Total sessions: 1

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session destination-port 23 brief

```
root> show security flow session destination-port 23 brief
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Session ID: 200067563, Policy name: default-policy/2, Timeout: 1798, Valid
  In: 40.0.0.100/32783 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 10, Bytes:
610
  Out: 30.0.0.100/23 --> 40.0.0.100/32783;tcp, If: ge-0/0/1.0, Pkts: 9, Bytes:
602
Total sessions: 1

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session

```
root> show security flow session destination-port 23 extensive
Flow Sessions on FPC4 PIC1:
Total sessions: 0
```


Copyright © 2013, Juniper Networks, Inc.

### destination-port 23 extensive

```
Flow Sessions on FPC5 PIC0:

Session ID: 200067563, Status: Normal
Flag: 0x40
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-telnet/10
Maximum timeout: 1800, Current timeout: 1794
Session State: Valid
Start time: 670359, Duration: 26
   In: 40.0.0.100/32783 --> 30.0.0.100/23;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 10, Bytes: 610
   Out: 30.0.0.100/23 --> 40.0.0.100/32783;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 9, Bytes: 602
Total sessions: 1

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session destination-port 23 summary

```
root> show security flow session destination-port 23 summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```

Copyright © 2013, Juniper Networks, Inc.

## show security flow session destination-prefix

**Syntax** **show security flow session destination-prefix**
***destination-IP-prefix*** **[brief | extensive | summary]**

**Release Information** Command introduced in Release 8.5 of Junos OS. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Release 10.4 of Junos OS.
Support for IPv6 addresses added in Release 10.2 of Junos OS.
Filter and view options added in Release 10.2 of Junos OS.

**Description** Display information about each session that matches the specified IP destination prefix.

**Options**
- ***destination-IP-prefix***—Destination IP prefix or address for which to display session information.
- brief | extensive | summary—Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**
- clear security flow session destination-port on page 1411

**List of Sample Output**
show security flow session destination-prefix 30/8 on page 1905
show security flow session destination-prefix 30/8 brief on page 1906
show security flow session destination-prefix 30/8 extensive on page 1906
show security flow session destination-prefix 30/8 summary on page 1907
show security flow session destination-prefix 10::10 on page 1907

**Output Fields** Table 123 on page 1904 lists the output fields for the **show security flow session destination-prefix** command. Output fields are listed in the approximate order in which they appear.

### Table 123: show security flow session destination-prefix Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the session. You can use this ID to get additional information about the session. |
| **Policy name** | Policy that permitted the traffic. |
| **Timeout** | Idle timeout after which the session expires. |
| **In** | Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Out** | Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |


Copyright © 2013, Juniper Networks, Inc.

Table 123: show security flow session destination-prefix Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Total sessions** | Total number of sessions. |
| **Status** | Session status. |
| **Flag** | Internal flag depicting the state of the session, used for debugging purposes. |
| **Policy name** | Name and ID of the policy that the first packet of the session matched. |
| **Source NAT pool** | The name of the source pool where NAT is used. |
| **Application** | Name of the application. |
| **Maximum timeout** | Maximum session timeout. |
| **Current timeout** | Remaining time for the session unless traffic exists in the session. |
| **Session State** | Session state. |
| **Start time** | Time when the session was created, offset from the system start time. |
| **Unicast-sessions** | Number of unicast sessions. |
| **Multicast-sessions** | Number of multicast sessions. |
| **Failed-sessions** | Number of failed sessions. |
| **Sessions-in-use** | Number of sessions in use.<br>• Valid sessions<br>• Pending sessions<br>• Invalidated sessions<br>• Sessions in other states |
| **Maximum-sessions** | Number of maximum sessions. |

## Sample Output

### show security flow session

```
root> show security flow session destination-prefix 30/8
Flow Sessions on FPC4 PIC1:
```

Copyright © 2013, Juniper Networks, Inc.

destination-prefix 30/8

```
Session ID: 170068346, Policy name: default-policy/2, Timeout: 1792, Valid
  In: 40.0.0.100/32782 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 11, Bytes:
662
  Out: 30.0.0.100/23 --> 40.0.0.100/32782;tcp, If: ge-0/0/1.0, Pkts: 11, Bytes:
708
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session destination-prefix 30/8 brief

```
root> show security flow session destination-prefix 30/8 brief
Flow Sessions on FPC4 PIC1:

Session ID: 170068346, Policy name: default-policy/2, Timeout: 1792, Valid
  In: 40.0.0.100/32782 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 11, Bytes:
662
  Out: 30.0.0.100/23 --> 40.0.0.100/32782;tcp, If: ge-0/0/1.0, Pkts: 11, Bytes:
708
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session

```
root> show security flow session destination-prefix 30/8 extensive
Flow Sessions on FPC4 PIC1:
```


Copyright © 2013, Juniper Networks, Inc.

destination-prefix 30/8 extensive

```
Session ID: 170068346, Status: Normal
Flag: 0x40
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-telnet/10
Maximum timeout: 1800, Current timeout: 1780
Session State: Valid
Start time: 670272, Duration: 40
   In: 40.0.0.100/32782 --> 30.0.0.100/23;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 11, Bytes: 662
   Out: 30.0.0.100/23 --> 40.0.0.100/32782;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 11, Bytes: 708
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session destination-prefix 30/8 summary

```
root> show security flow session destination-prefix 30/8 summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```

show security flow session

```
user@host> show security flow session destination-prefix 10::10
Session ID: 50000004, Policy name: self-traffic-policy/1, Timeout: 2
In: 10::11/42756 --> 10::10/0;icmp, If: .local..0
```

destination-prefix 10::10

```
Out: 10::10/0 --> 10::11/42756;icmp, If: ge-0/3/0.0

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow session extensive node

**Syntax** **show security flow session extensive node (*node-id* | all | local | primary)**

**Release Information** Command introduced in Release 8.5 of Junos OS; node options added in Release 9.0 of Junos OS. Filter options added in Release 10.2 of Junos OS.

**Description** Display information about all currently active security sessions on the device for the specified node options in extensive mode.

**Options** **node**—(Optional) For chassis cluster configurations, display session information on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**
- show security flow session on page 1879

**List of Sample Output**
show security flow session extensive node 0 on page 1911
show security flow session extensive node 1 on page 1911
show security flow session extensive node all on page 1912
show security flow session extensive node local on page 1913
show security flow session extensive node primary on page 1913

**Output Fields** Table 124 on page 1909 lists the output fields for the **show security flow session extensive node** command. Output fields are listed in the approximate order in which they appear.

Table 124: show security flow session extensive node Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the session. You can use this ID to get additional information about the session. |
| **Status** | Session status. |
| **State** | Session state. |
| **Flag** | Internal flag depicting the state of the session, used for debugging purposes. |
| **Policy name** | Policy that permitted the traffic. |
| **Source NAT pool** | The name of the source pool where NAT is used. |

Copyright © 2013, Juniper Networks, Inc.

Table 124: show security flow session extensive node Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Maximum timeout** | Maximum session timeout. |
| **Current timeout** | Remaining time for the session unless traffic exists in the session. |
| **Start time** | Time when the session was created, offset from the system start time. |
| **Duration** | Length of time for which the session is active. |
| **In** | Incoming flow (source and destination IP addresses, application protocol, interface, session token, flag, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Out** | Reverse flow (source and destination IP addresses, application protocol, interface, session token, flag, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Total sessions** | Total number of sessions. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session extensive node 0

```
root@antbert> show security flow session extensive node 0
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000011, Status: Normal, State: Backup
Flag: 0x10000042
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 13946
Session State: Valid
Start time: 2021, Duration: 469
   In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp,
    Interface: reth1.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x0, Gateway: 1.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
   Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp,
    Interface: reth2.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x0, Gateway: 2.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

### show security flow session extensive node 1

```
root@antbert> show security flow session extensive node 1
node1:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000272, Status: Normal, State: Active
Flag: 0x8000042
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 1756
Session State: Valid
Start time: 2023, Duration: 473
   In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp,
    Interface: reth1.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x84863c2, Gateway: 1.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
```

Copyright © 2013, Juniper Networks, Inc.

```
    Pkts: 69, Bytes: 3024
   Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp,
    Interface: reth2.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x84843c2, Gateway: 2.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 62, Bytes: 4002
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

### show security flow session extensive node all

```
root@antbert> show security flow session extensive node all
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000011, Status: Normal, State: Backup
Flag: 0x10000042
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 13936
Session State: Valid
Start time: 2021, Duration: 478
   In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp,
    Interface: reth1.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x0, Gateway: 1.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
   Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp,
    Interface: reth2.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x0, Gateway: 2.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0

node1:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000272, Status: Normal, State: Active
Flag: 0x8000042
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 1750
```


Copyright © 2013, Juniper Networks, Inc.

```
Session State: Valid
Start time: 2023, Duration: 479
   In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp,
    Interface: reth1.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x84863c2, Gateway: 1.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 69, Bytes: 3024
   Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp,
    Interface: reth2.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x84843c2, Gateway: 2.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 62, Bytes: 4002
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

### show security flow session extensive node local

```
root@antbert> show security flow session extensive node local
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000011, Status: Normal, State: Backup
Flag: 0x10000042
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 13930
Session State: Valid
Start time: 2021, Duration: 484
   In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp,
    Interface: reth1.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x0, Gateway: 1.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
   Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp,
    Interface: reth2.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x0, Gateway: 2.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```

### show security flow session extensive node primary

```
root@antbert> show security flow session extensive node primary
node0:
--------------------------------------------------------------------------
```

```
Flow Sessions on FPC3 PIC1:
Total sessions: 0

Flow Sessions on FPC4 PIC0:

Session ID: 160000011, Status: Normal, State: Backup
Flag: 0x10000042
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 13924
Session State: Valid
Start time: 2021, Duration: 490
   In: 1.0.0.100/53036 --> 2.0.0.100/21;tcp,
    Interface: reth1.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x0, Gateway: 1.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
   Out: 2.0.0.100/21 --> 1.0.0.100/53036;tcp,
    Interface: reth2.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x0, Gateway: 2.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
Total sessions: 1

Flow Sessions on FPC4 PIC1:
Total sessions: 0
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow session family

**Syntax** show security flow session family (inet | inet6)
[brief | extensive | summary]

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display filtered summary of information about existing sessions, including types of sessions, active and failed sessions, and the maximum allowed number of sessions.

**Options**
- **inet**—Display details summary of IPv4 sessions.
- **inet6**—Display details summary of IPv6 sessions.
- brief | extensive | summary–Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**
- Layer 2 Bridging and Transparent Mode for Security Devices
- clear security flow session family on page 1414

**List of Sample Output**
show security flow session family inet on page 1917
show security flow session family inet brief on page 1917
show security flow session family inet extensive on page 1917
show security flow session family inet summary on page 1919

**Output Fields** Table 125 on page 1915 lists the output fields for the **show security flow session family** command. Output fields are listed in the approximate order in which they appear.

### Table 125: show security flow session family Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the session. Use this ID to get more information about the session. |
| **Policy name** | Policy that permitted the traffic. |
| **Timeout** | Idle timeout after which the session expires. |
| **In** | Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Out** | Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Total sessions** | Total number of sessions. |
| **Status** | Session status. |

Copyright © 2013, Juniper Networks, Inc.

Table 125: show security flow session family Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Flag** | Internal flag depicting the state of the session, used for debugging purposes. |
| **Policy name** | Name and ID of the policy that the first packet of the session matched. |
| **Source NAT pool** | The name of the source pool where NAT is used. |
| **Application** | Name of the application. |
| **Maximum timeout** | Maximum session timeout. |
| **Current timeout** | Remaining time for the session unless traffic exists in the session. |
| **Session State** | Session state. |
| **Start time** | Time when the session was created, offset from the system start time. |
| **Unicast-sessions** | Number of unicast sessions. |
| **Multicast-sessions** | Number of multicast sessions. |
| **Failed-sessions** | Number of failed sessions. |
| **Sessions-in-use** | Number of sessions in use.<br>• Valid sessions<br>• Pending sessions<br>• Invalidated sessions<br>• Sessions in other states |
| **Maximum-sessions** | Number of maximum sessions. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session family inet

```
root> show security flow session family inet
Flow Sessions on FPC4 PIC1:

Session ID: 170067516, Policy name: self-traffic-policy/1, Timeout: 4, Valid
  In: 40.0.0.100/23 --> 40.0.0.1/26637;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84
  Out: 40.0.0.1/26637 --> 40.0.0.100/23;icmp, If: .local..0, Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200066737, Policy name: self-traffic-policy/1, Timeout: 2, Valid
  In: 40.0.0.100/21 --> 40.0.0.1/26637;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84
  Out: 40.0.0.1/26637 --> 40.0.0.100/21;icmp, If: .local..0, Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Session ID: 210066726, Policy name: self-traffic-policy/1, Timeout: 2, Valid
  In: 40.0.0.100/22 --> 40.0.0.1/26637;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84
  Out: 40.0.0.1/26637 --> 40.0.0.100/22;icmp, If: .local..0, Pkts: 1, Bytes: 84
Total sessions: 1
```

### show security flow session family inet brief

```
root> show security flow session family inet brief
Flow Sessions on FPC4 PIC1:

Session ID: 170067516, Policy name: self-traffic-policy/1, Timeout: 4, Valid
  In: 40.0.0.100/23 --> 40.0.0.1/26637;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84
  Out: 40.0.0.1/26637 --> 40.0.0.100/23;icmp, If: .local..0, Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200066737, Policy name: self-traffic-policy/1, Timeout: 2, Valid
  In: 40.0.0.100/21 --> 40.0.0.1/26637;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84
  Out: 40.0.0.1/26637 --> 40.0.0.100/21;icmp, If: .local..0, Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Session ID: 210066726, Policy name: self-traffic-policy/1, Timeout: 2, Valid
  In: 40.0.0.100/22 --> 40.0.0.1/26637;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84
  Out: 40.0.0.1/26637 --> 40.0.0.100/22;icmp, If: .local..0, Pkts: 1, Bytes: 84
Total sessions: 1
```

### show security flow session family inet extensive

```
root> show security flow session family inet extensive
Flow Sessions on FPC4 PIC1:

Session ID: 170067527, Status: Normal
Flag: 0x80000040
Policy name: self-traffic-policy/1
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 2
Session State: Valid
Start time: 667332, Duration: 1
   In: 40.0.0.100/56 --> 40.0.0.1/26637;icmp,
    Interface: ge-0/0/2.0,
```

Copyright © 2013, Juniper Networks, Inc.

```
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 40.0.0.1/26637 --> 40.0.0.100/56;icmp,
    Interface: .local..0,
    Session token: 0x80, Flag: 0x0x30
    Route: 0xfffb0006, Gateway: 40.0.0.1, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200066749, Status: Normal
Flag: 0x80000040
Policy name: self-traffic-policy/1
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 4
Session State: Valid
Start time: 667329, Duration: 1
   In: 40.0.0.100/57 --> 40.0.0.1/26637;icmp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 40.0.0.1/26637 --> 40.0.0.100/57;icmp,
    Interface: .local..0,
    Session token: 0x80, Flag: 0x0x30
    Route: 0xfffb0006, Gateway: 40.0.0.1, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Session ID: 210066737, Status: Normal
Flag: 0x80000040
Policy name: self-traffic-policy/1
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 2
Session State: Valid
Start time: 667326, Duration: 3
   In: 40.0.0.100/55 --> 40.0.0.1/26637;icmp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 40.0.0.1/26637 --> 40.0.0.100/55;icmp,
    Interface: .local..0,
    Session token: 0x80, Flag: 0x0x30
    Route: 0xfffb0006, Gateway: 40.0.0.1, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
```


Copyright © 2013, Juniper Networks, Inc.

```
    Pkts: 1, Bytes: 84
Total sessions: 1
```

### show security flow session family inet summary

```
root> show security flow session family inet summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 1
Sessions in other states: 0
Total sessions: 2

Flow Sessions on FPC5 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 1
Sessions in other states: 0
Total sessions: 2
```

Copyright © 2013, Juniper Networks, Inc.

## show security flow session idp summary

**Syntax** **show security flow session idp summary**

**Release Information** Command introduced in Release 10.2 of Junos OS

**Description** Display summary output.

**Options**

- application—Application name
- destination-port—Destination port
- destination-prefix—Destination IP prefix or address
- family—Display session by family.
- interface–Name of incoming or outgoing interface
- protocol—IP protocol number
- source-port—Source port
- source-prefix—Source IP prefix

**Required Privilege Level** view

**Related Documentation**

- show security flow session on page 1879
- IDP Policies for Security Devices

**List of Sample Output** show security flow session idp summary on page 1921

**Output Fields** Table 126 on page 1920 lists the output fields for the **show security flow session idp summary** command. Output fields are listed in the approximate order in which they appear.

### Table 126: show security flow session idp summary Output Fields

| Field Name | Field Description |
|---|---|
| Valid session | Number of valid sessions. |
| Pending sessions | Number of pending sessions. |
| Invalidated sessions | Number of invalid sessions. |
| Sessions in other states | Number of sessions in other states. |
| Total sessions | Total number of sessions. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session idp summary

```
root@ show security flow session idp summary
Flow Sessions on FPC4 PIC0:

Valid sessions: 3
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 3

Flow Sessions on FPC5 PIC0:

Valid sessions: 4
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 4
```

Copyright © 2013, Juniper Networks, Inc.

## show security flow session interface

**Syntax** **show security flow session interface**
***interface-name*** **[brief | extensive | summary]**

**Release Information** Command introduced in Release 8.5 of Junos OS; Filter and view options added in Release 10.2 of Junos OS.

**Description** Display information about each session that uses the specified interface. The interface name can be a session's incoming or outgoing interface.

**Options**
- ***interface-name***—Name of the interface on the device for which to display sessions information.
- brief | extensive | summary–Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**
- clear security flow session interface on page 1415

**List of Sample Output**
show security flow session interface ge-0/0/2.0 on page 1924
show security flow session interface ge-0/0/2.0 brief on page 1924
show security flow session interface ge-0/0/2.0 extensive on page 1924
show security flow session interface ge-0/0/2.0 summary on page 1926

**Output Fields** Table 127 on page 1922 lists the output fields for the **show security flow session interface** command. Output fields are listed in the approximate order in which they appear.

### Table 127: show security flow session interface Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the session. You can use this ID to get additional information about the session. |
| **Policy name** | Policy that permitted the traffic. |
| **Timeout** | Idle timeout after which the session expires. |
| **In** | Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Out** | Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Total sessions** | Total number of sessions. |
| **Status** | Session status. |


Copyright © 2013, Juniper Networks, Inc.

Table 127: show security flow session interface Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Flag** | Internal flag depicting the state of the session, used for debugging purposes. |
| **Policy name** | Name and ID of the policy that the first packet of the session matched. |
| **Source NAT pool** | The name of the source pool where NAT is used. |
| **Application** | Name of the application. |
| **Maximum timeout** | Maximum session timeout. |
| **Current timeout** | Remaining time for the session unless traffic exists in the session. |
| **Session State** | Session state. |
| **Start time** | Time when the session was created, offset from the system start time. |
| **Unicast-sessions** | Number of unicast sessions. |
| **Multicast-sessions** | Number of multicast sessions. |
| **Failed-sessions** | Number of failed sessions. |
| **Sessions-in-use** | Number of sessions in use.<br>• Valid sessions<br>• Pending sessions<br>• Invalidated sessions<br>• Sessions in other states |
| **Maximum-sessions** | Number of maximum sessions. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session interface ge-0/0/2.0

```
root> show security flow session interface ge-0/0/2.0
Flow Sessions on FPC4 PIC1:

Session ID: 170068353, Policy name: default-policy/2, Timeout: 4, Valid
  In: 40.0.0.100/18 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84

  Out: 30.0.0.100/5907 --> 40.0.0.100/18;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200067569, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/16 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84

  Out: 30.0.0.100/5907 --> 40.0.0.100/16;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Session ID: 210067554, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/17 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84

  Out: 30.0.0.100/5907 --> 40.0.0.100/17;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1
```

### show security flow session interface ge-0/0/2.0 brief

```
root> show security flow session interface ge-0/0/2.0 brief
Flow Sessions on FPC4 PIC1:

Session ID: 170068353, Policy name: default-policy/2, Timeout: 4, Valid
  In: 40.0.0.100/18 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84

  Out: 30.0.0.100/5907 --> 40.0.0.100/18;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200067569, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/16 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84

  Out: 30.0.0.100/5907 --> 40.0.0.100/16;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Session ID: 210067554, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/17 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes: 84

  Out: 30.0.0.100/5907 --> 40.0.0.100/17;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1
```


Copyright © 2013, Juniper Networks, Inc.

### show security flow session interface ge-0/0/2.0 extensive

```
root> show security flow session interface ge-0/0/2.0 extensive
Flow Sessions on FPC4 PIC1:

Session ID: 170068354, Status: Normal
Flag: 0x80000040
Policy name: default-policy/2
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 2
Session State: Valid
Start time: 670502, Duration: 2
   In: 40.0.0.100/21 --> 30.0.0.100/5907;icmp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 30.0.0.100/5907 --> 40.0.0.100/21;icmp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200067571, Status: Normal
Flag: 0x80000040
Policy name: default-policy/2
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 2
Session State: Valid
Start time: 670500, Duration: 1
   In: 40.0.0.100/22 --> 30.0.0.100/5907;icmp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 30.0.0.100/5907 --> 40.0.0.100/22;icmp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Session ID: 210067556, Status: Normal
Flag: 0x80000040
Policy name: default-policy/2
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 2
Session State: Valid
Start time: 670499, Duration: 1
   In: 40.0.0.100/23 --> 30.0.0.100/5907;icmp,
```

```
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 30.0.0.100/5907 --> 40.0.0.100/23;icmp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
Total sessions: 1
```

### show security flow session interface ge-0/0/2.0 summary

```
root> show security flow session interface ge-0/0/2.0 summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow session nat

**Syntax** **show security flow session nat [brief | extensive | summary]**

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display sessions with network address translation.

**Options** **brief | extensive | summary**—Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**
- show security flow session on page 1879

**List of Sample Output**
show security flow session nat brief on page 1929
show security flow session nat extensive on page 1929
show security flow session nat summary on page 1929

**Output Fields** Table 128 on page 1927 lists the output fields for the **show security flow session nat** command. Output fields are listed in the approximate order in which they appear.

### Table 128: show security flow session nat Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the session. You can use this ID to get additional information about the session. |
| **Policy name** | Policy that permitted the traffic. |
| **Timeout** | Idle timeout after which the session expires. |
| **Resource information** | Information about the session particular to the resource manager, including the name of the ALG, the group ID. and the resource ID. |
| **In** | Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Out** | Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Total sessions** | Total number of sessions. |
| **Status** | Session status. |
| **Flag** | Internal flag depicting the state of the session, used for debugging purposes. |
| **Policy name** | Name and ID of the policy that the first packet of the session matched. |

Copyright © 2013, Juniper Networks, Inc.

Table 128: show security flow session nat Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Source NAT pool** | The name of the source pool where NAT is used. |
| **Application** | Name of the application. |
| **Maximum timeout** | Maximum session timeout. |
| **Current timeout** | Remaining time for the session unless traffic exists in the session. |
| **Session State** | Session state. |
| **Start time** | Time when the session was created, offset from the system start time. |
| **Valid sessions** | Number of valid sessions. |
| **Pending sessions** | Number of pending sessions. |
| **Invalidated sessions** | Number of invalidated sessions. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session nat brief

```
root> show security flow session nat brief
Flow Sessions on FPC4 PIC1:

Session ID: 170000019, Policy name: idp/4, Timeout: 1790, Valid
  In: 40.0.0.111/32817 --> 30.0.0.100/21;tcp, If: ge-0/0/2.0, Pkts: 13, Bytes:
610
  Out: 30.0.0.100/21 --> 30.0.0.1/64508;tcp, If: ge-0/0/1.0, Pkts: 11, Bytes: 640
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session nat extensive

```
root> show security flow session nat extensive
Flow Sessions on FPC4 PIC1:

Session ID: 170000019, Status: Normal
Flag: 0x2
Policy name: idp/4
Source NAT pool: interface, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 1784
Session State: Valid
Start time: 1780, Duration: 16
   In: 40.0.0.111/32817 --> 30.0.0.100/21;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x40010, Gateway: 40.0.0.111, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 13, Bytes: 610
   Out: 30.0.0.100/21 --> 30.0.0.1/64508;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x50010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 11, Bytes: 640
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session nat summary

```
root> show security flow session nat summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

Copyright © 2013, Juniper Networks, Inc.

```
Flow Sessions on FPC5 PIC0:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow session protocol

**Syntax** **show security flow session protocol** ( ***protocol-name*** | ***protocol-number*** )
[brief | extensive | summary]

**Release Information** Command introduced in Release 8.5 of Junos OS; Filter and view options introduced in Release 10.2 of Junos OS.

**Description** Display information about each session that uses the specified protocol.

**Options** ***protocol-name*** —(Optional) Protocol to use as a sessions filter. Information about sessions that use this protocol is displayed. Possible protocols are:

- **ah**—IP Security Authentication Header
- **egp**—Exterior gateway protocol
- **esp**—IPsec Encapsulating Security Payload
- **gre**—Generic routing encapsulation
- **icmp**—Internet Control Message Protocol
- **igmp**—Internet Group Management Protocol
- **ipip**—IP over IP
- **ospf**—Open Shortest Path First
- **pim**—Protocol Independent Multicast
- **rsvp**—Resource Reservation Protocol
- **sctp**—Stream Control Transmission Protocol
- **tcp**—Transmission Control Protocol
- **udp**—User Datagram Protocol

***protocol-number*** —(Optional) Numeric protocol value. For a complete list of possible numeric values, see RFC 1700, *Assigned Numbers* (*for the Internet Protocol Suite*).

**Range:** 0 through 255

**brief | extensive | summary**—Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**
- clear security flow session protocol on page 1416

**List of Sample Output**
show security flow session protocol icmp on page 1934
show security flow session protocol icmp brief on page 1934
show security flow session protocol icmp extensive on page 1934
show security flow session protocol icmp summary on page 1936

Copyright © 2013, Juniper Networks, Inc.

**Output Fields** Table 129 on page 1932 lists the output fields for the **show security flow session protocol** command. Output fields are listed in the approximate order in which they appear.

### Table 129: show security flow session protocol Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the session. You can use this ID to get additional information about the session. |
| **Policy name** | Policy that permitted the traffic. |
| **Timeout** | Idle timeout after which the session expires. |
| **In** | Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Out** | Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Total sessions** | Total number of sessions. |
| **Status** | Session status. |
| **Flag** | Internal flag depicting the state of the session, used for debugging purposes. |
| **Policy name** | Name and ID of the policy that the first packet of the session matched. |
| **Source NAT pool** | The name of the source pool where NAT is used. |
| **Application** | Name of the application. |
| **Maximum timeout** | Maximum session timeout. |
| **Current timeout** | Remaining time for the session unless traffic exists in the session. |
| **Session State** | Session state. |
| **Start time** | Time when the session was created, offset from the system start time. |
| **Unicast-sessions** | Number of unicast sessions. |
| **Multicast-sessions** | Number of multicast sessions. |
| **Failed-sessions** | Number of failed sessions. |


Copyright © 2013, Juniper Networks, Inc.

Table 129: show security flow session protocol Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Sessions-in-use** | Number of sessions in use.<br>• Valid sessions<br>• Pending sessions<br>• Invalidated sessions<br>• Sessions in other states |
| **Maximum-sessions** | Number of maximum sessions. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session protocol icmp

```
root> show security flow session protocol icmp
Flow Sessions on FPC4 PIC1:

Session ID: 170068388, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/121 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes:
84
  Out: 30.0.0.100/5907 --> 40.0.0.100/121;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200067603, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/119 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes:
84
  Out: 30.0.0.100/5907 --> 40.0.0.100/119;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Session ID: 210067588, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/120 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes:
84
  Out: 30.0.0.100/5907 --> 40.0.0.100/120;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1
```

### show security flow session protocol icmp brief

```
root> show security flow session protocol icmp brief
Flow Sessions on FPC4 PIC1:

Session ID: 170068388, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/121 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes:
84
  Out: 30.0.0.100/5907 --> 40.0.0.100/121;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200067603, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/119 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes:
84
  Out: 30.0.0.100/5907 --> 40.0.0.100/119;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Session ID: 210067588, Policy name: default-policy/2, Timeout: 2, Valid
  In: 40.0.0.100/120 --> 30.0.0.100/5907;icmp, If: ge-0/0/2.0, Pkts: 1, Bytes:
84
  Out: 30.0.0.100/5907 --> 40.0.0.100/120;icmp, If: ge-0/0/1.0, Pkts: 1, Bytes:
84
Total sessions: 1
```


Copyright © 2013, Juniper Networks, Inc.

### show security flow session protocol icmp extensive

```
root> show security flow session protocol icmp extensive
Flow Sessions on FPC4 PIC1:

Session ID: 170068389, Status: Normal
Flag: 0x80000040
Policy name: default-policy/2
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 2
Session State: Valid
Start time: 670605, Duration: 2
   In: 40.0.0.100/124 --> 30.0.0.100/5907;icmp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 30.0.0.100/5907 --> 40.0.0.100/124;icmp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Session ID: 200067605, Status: Normal
Flag: 0x80000040
Policy name: default-policy/2
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 4
Session State: Valid
Start time: 670603, Duration: 1
   In: 40.0.0.100/125 --> 30.0.0.100/5907;icmp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 30.0.0.100/5907 --> 40.0.0.100/125;icmp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Session ID: 210067590, Status: Normal
Flag: 0x80000040
Policy name: default-policy/2
Source NAT pool: Null
Maximum timeout: 4, Current timeout: 4
Session State: Valid
Start time: 670602, Duration: 1
   In: 40.0.0.100/126 --> 30.0.0.100/5907;icmp,
```

```
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
   Out: 30.0.0.100/5907 --> 40.0.0.100/126;icmp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 84
Total sessions: 1
```

## show security flow session protocol icmp summary

```
root> show security flow session protocol icmp summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow session resource-manager

**Syntax** **show security flow session resource-manager**
[brief | extensive | summary]

**Release Information** Command introduced in Release 8.5 of Junos OS; Filter and view options introduced in Release 10.2 of Junos OS.

**Description** Display information about sessions created by the resource manager.

**Options** none—Display all resource manager sessions.

**brief | extensive | summary**—Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**
- clear security flow session resource-manager on page 1418

**List of Sample Output**
show security flow session resource-manager on page 1939
show security flow session resource-manager brief on page 1939
show security flow session resource-manager extensive on page 1939
show security flow session resource-manager summary on page 1940

**Output Fields** Table 130 on page 1937 lists the output fields for the **show security flow session resource-manager** command. Output fields are listed in the approximate order in which they appear.

### Table 130: show security flow session resource-manager Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the session. You can use this ID to get additional information about the session. |
| **Policy name** | Policy that permitted the traffic. |
| **Timeout** | Idle timeout after which the session expires. |
| **Resource information** | Information about the session particular to the resource manager, including the name of the ALG, the group ID. and the resource ID. |
| **In** | Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Out** | Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Total sessions** | Total number of sessions. |

Copyright © 2013, Juniper Networks, Inc.

Table 130: show security flow session resource-manager Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Status** | Session status. |
| **Flag** | Internal flag depicting the state of the session, used for debugging purposes. |
| **Policy name** | Name and ID of the policy that the first packet of the session matched. |
| **Source NAT pool** | The name of the source pool where NAT is used. |
| **Application** | Name of the application. |
| **Maximum timeout** | Maximum session timeout. |
| **Current timeout** | Remaining time for the session unless traffic exists in the session. |
| **Session State** | Session state. |
| **Start time** | Time when the session was created, offset from the system start time. |
| **Valid sessions** | Number of valid sessions. |
| **Pending sessions** | Number of pending sessions. |
| **Invalidated sessions** | Number of invalidated sessions. |
| **Sessions in other states** | Number of sessions in other states. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session resource-manager

```
root> show security flow session resource-manager
Flow Sessions on FPC4 PIC1:

Session ID: 170068496, Policy name: default-policy/2, Timeout: 1798, Valid
Resource information : FTP ALG, 24576, 0
  In: 40.0.0.111/32797 --> 30.0.0.100/21;tcp, If: ge-0/0/2.0, Pkts: 82, Bytes:
3964
  Out: 30.0.0.100/21 --> 40.0.0.111/32797;tcp, If: ge-0/0/1.0, Pkts: 72, Bytes:
4998

Session ID: 170068501, Policy name: default-policy/2, Timeout: 150, Valid
Resource information : FTP ALG, 24576, 86016
  In: 30.0.0.100/20 --> 40.0.0.111/32802;tcp, If: ge-0/0/1.0, Pkts: 53637, Bytes:
 79808988
  Out: 40.0.0.111/32802 --> 30.0.0.100/20;tcp, If: ge-0/0/2.0, Pkts: 20856, Bytes:
 1084520
Total sessions: 2

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session resource-manager brief

```
root> show security flow session resource-manager brief
Flow Sessions on FPC4 PIC1:

Session ID: 170068496, Policy name: default-policy/2, Timeout: 1798, Valid
Resource information : FTP ALG, 24576, 0
  In: 40.0.0.111/32797 --> 30.0.0.100/21;tcp, If: ge-0/0/2.0, Pkts: 82, Bytes:
3964
  Out: 30.0.0.100/21 --> 40.0.0.111/32797;tcp, If: ge-0/0/1.0, Pkts: 72, Bytes:
4998

Session ID: 170068501, Policy name: default-policy/2, Timeout: 150, Valid
Resource information : FTP ALG, 24576, 86016
  In: 30.0.0.100/20 --> 40.0.0.111/32802;tcp, If: ge-0/0/1.0, Pkts: 53637, Bytes:
 79808988
  Out: 40.0.0.111/32802 --> 30.0.0.100/20;tcp, If: ge-0/0/2.0, Pkts: 20856, Bytes:
 1084520
Total sessions: 2

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session

```
root> show security flow session resource-manager extensive
Flow Sessions on FPC4 PIC1:
```

resource-manager extensive

```
Session ID: 170068496, Status: Normal
Flag: 0x42
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 1800
Session State: Valid
Start time: 672899, Duration: 110
Client: FTP ALG, Group: 24576, Resource: 0
   In: 40.0.0.111/32797 --> 30.0.0.100/21;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x2621
    Route: 0x90010, Gateway: 40.0.0.111, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 84, Bytes: 4044
   Out: 30.0.0.100/21 --> 40.0.0.111/32797;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x2620
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 74, Bytes: 5116

Session ID: 170068501, Status: Normal
Flag: 0x80001040
Policy name: default-policy/2
Source NAT pool: Null
Maximum timeout: 2, Current timeout: 2
Session State: Valid
Start time: 673004, Duration: 5
Client: FTP ALG, Group: 24576, Resource: 86016
   In: 30.0.0.100/20 --> 40.0.0.111/32802;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x21
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 2,
    Pkts: 177002, Bytes: 263785189
   Out: 40.0.0.111/32802 --> 30.0.0.100/20;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x20
    Route: 0x90010, Gateway: 40.0.0.111, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 2,
    Pkts: 66402, Bytes: 3452912
Total sessions: 2

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

show security flow session

```
root> show security flow session resource-manager summary
Flow Sessions on FPC4 PIC1:
```


Copyright © 2013, Juniper Networks, Inc.

resource-manager summary

```
Valid sessions: 2
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 2

Flow Sessions on FPC5 PIC0:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```

Copyright © 2013, Juniper Networks, Inc.

## show security flow session services-offload

**Syntax** **show security flow session services-offload**
[*filter*] [**brief | extensive | summary**]

**Release Information** Command introduced in Junos OS Release 11.4. Low-latency option introduced in Junos OS Release 12.1X44-D10.

**Description** Display information about all currently active services-offload security sessions on the device.

**Options**

- *filter*—Filter the display by the specified criteria.

  The following filters reduce the display to those sessions that match the criteria specified by the filter:

  **application** —Application name.

  **application-firewall-rule-set**—Application firewall enabled with the specified rule set.

  **application-traffic-control-rule-set**—Application traffic control enabled with the specified rule set.

  **destination-port**—Destination port.

  **destination-prefix**—Destination IP prefix or address.

  **dynamic-application**—Dynamic application name.

  **dynamic-application-group**—Dynamic application group name.

  **encrypted**—Show encrypted traffic.

  **family**—Protocol family.

  **interface**—Name of incoming or outgoing interface.

  **logical-system**—Logical system name.

  **protocol**—IP protocol number.

  **root-logical-system**—Root logical system name.

  **source-port**—Source port.

  **source-prefix**—Source IP prefix or address.

- **brief | extensive | summary**—Display the specified level of output.

**Required Privilege Level** view

**Related Documentation**

- clear security flow session services-offload on page 1419

 Copyright © 2013, Juniper Networks, Inc.

List of Sample Output

show security flow session services-offload on page 1944
show security flow session services-offload brief on page 1944
show security flow session services-offload extensive on page 1944
show security flow session services-offload summary on page 1945

Output Fields

Table 131 on page 1943 lists the output fields for the **show security flow session services-offload** command. Output fields are listed in the approximate order in which they appear.

### Table 131: show security flow session services-offload Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the services-offload session. Use this ID to get more information about the session. |
| **Policy name** | Policy that permits the services-offload traffic. |
| **Timeout** | Idle timeout period after which the services-offload session expires. |
| **In** | Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets, and bytes). |
| **Out** | Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets, and bytes). |
| **Total sessions** | Total number of services-offload sessions. |
| **Status** | Services-offload session status. |
| **Flag** | Internal flag depicting the state of the services-offload session, used for debugging purposes. |
| **Policy name** | Name and ID of the policy that the first packet of the services-offload session matched. |
| **Source NAT pool** | The name of the source pool where NAT is used. |
| **Application** | Name of the application. |
| **Dynamic application** | Name of the dynamic application. |
| **Maximum timeout** | Maximum amount of idle time allowed for the services-offload session. |
| **Current timeout** | Number of seconds that the current services-offload session has been idle. |
| **Session State** | Services-offload session state. |
| **Start time** | Time when the services-offload session was created, offset from the system start time. |
| **Duration** | Duration of the services-offload session. |

Copyright © 2013, Juniper Networks, Inc.

Table 131: show security flow session services-offload Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Valid sessions** | Number of valid services-offload sessions. |
| **Pending sessions** | Number of pending services-offload sessions. |
| **Invalidated sessions** | Number of invalidated services-offload sessions. |
| **Sessions in other states** | Number of services-offload sessions in other states. |
| **Total sessions** | Total number of services-offload sessions. |

## Sample Output

### show security flow session services-offload

```
user@host>show security flow session services-offload
Flow Sessions on FPC1 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC0:

Session ID: 40001386, Policy name: p1/4, Timeout: 1794, Valid
  In: 1.0.0.2/35987 --> 2.0.0.2/22;tcp, If: ge-0/0/0.0, Pkts: 15, Bytes: 1890
  Out: 2.0.0.2/22 --> 1.0.0.2/35987;tcp, If: ge-0/0/1.0, Pkts: 13, Bytes: 2171
Total sessions: 1

Flow Sessions on FPC3 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC0:
Total sessions: 0
```

### show security flow session services-offload brief

```
user@host>show security flow session services-offload brief
Flow Sessions on FPC1 PIC0:
Total sessions: 0

Flow Sessions on FPC2 PIC0:

Session ID: 40001386, Policy name: p1/4, Timeout: 1794, Valid
  In: 1.0.0.2/35987 --> 2.0.0.2/22;tcp, If: ge-0/0/0.0, Pkts: 15, Bytes: 1890
  Out: 2.0.0.2/22 --> 1.0.0.2/35987;tcp, If: ge-0/0/1.0, Pkts: 13, Bytes: 2171
Total sessions: 1

Flow Sessions on FPC3 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC0:
Total sessions: 0
```

### show security flow session

```
user@host>show security flow session services-offload extensive
Flow Sessions on FPC1 PIC0:
Total sessions: 0
```


Copyright © 2013, Juniper Networks, Inc.

### services-offload extensive

```
Flow Sessions on FPC2 PIC0:
Total sessions: 0

Flow Sessions on FPC3 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Session ID: 100000001, Status: Normal
Flag: 0x40, services-offload
Policy name: p1/4
Source NAT pool: Null, Application: junos-ssh/22
Dynamic application: junos:UNKNOWN,
Maximum timeout: 1800, Current timeout: 1768
Session State: Valid
Start time: 94, Duration: 32
   In: 1.0.0.2/36250 --> 2.0.0.2/22;tcp,
    Interface: ge-0/0/0.0,
    Session token: 0x6, Flag: 0x21
    Route: 0xb0010, Gateway: 1.0.0.2, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 11, Bytes: 1538
   Out: 2.0.0.2/22 --> 1.0.0.2/36250;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x7, Flag: 0x20
    Route: 0xc0010, Gateway: 2.0.0.2, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 11, Bytes: 1987
Total sessions: 1
```

### show security flow session

```
user@host>show security flow session services-offload summary
Flow Sessions on FPC1 PIC0:
```

services-offload summary

```
Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC2 PIC0:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC3 PIC0:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow session session-identifier

**Syntax** **show security flow session session-identifier**
***session-identifier***

**Release Information** Command introduced in Release 8.5 of Junos OS;

**Description** Display detailed information for the session with this identifier.

**Options** ***session-identifier*** —Identifier of the session about which to display information.

**Required Privilege Level** view

**Related Documentation**
- clear security flow session session-identifier on page 1422

**List of Sample Output**
show security flow session session-identifier 36 on page 1949
show security flow session session-identifier 2218 on page 1949
show security flow session session-identifier 33 on page 1949

**Output Fields** Table 132 on page 1947 lists the output fields for the **show security flow session session-identifier** command. Output fields are listed in the approximate order in which they appear.

### Table 132: show security flow session session-identifier Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the session. You can use this ID to get additional information about the session. |
| **Status** | Session status. |
| **Flag** | Internal flag depicting the state of the session, used for debugging purposes. |
| **Virtual system** | Virtual system to which the session belongs. |
| **Policy name** | Name and ID of the policy that the first packet of the session matched. |
| **Maximum timeout** | Maximum session timeout. |
| **Current timeout** | Remaining time for the session unless traffic exists in the session. |
| **Start time** | Time when the session was created, offset from the system start time. |
| **Duration** | Length of time for which the session is active. |

Copyright © 2013, Juniper Networks, Inc.

Table 132: show security flow session session-identifier Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **In** | For the input flow:<br>• Source and destination addresses and protocol tuple for the input flow.<br>• **Interface**: Input flow interface.<br>• **Session token**: Internal token derived from the virtual routing instance.<br>• **Flag**: Internal debugging flags.<br>• **Route**: Internal next hop of the route to be used by the flow.<br>• **Gateway**: Next-hop gateway of the flow.<br>• **Tunnel**: If the flow is going into a tunnel, the tunnel ID. Otherwise, 0 (zero).<br>• **Port Sequence, FIN sequence, FIN state, Cookie**: Internal TCP state tracking information. |
| **Out** | For the reverse flow:<br>• Source and destination addresses, and protocol tuple for the reverse flow.<br>• **Interface**: Reverse flow interface.<br>• **Session token**: Internal token derived from the virtual routing instance.<br>• **Flag**: Internal debugging flags.<br>• **Route**: Internal next hop of the route to be used by the flow.<br>• **Gateway**: Next-hop gateway of the flow.<br>• **Tunnel**: If the flow is going into a tunnel, the tunnel ID. Otherwise, 0 (zero).<br>• **Port Sequence, FIN sequence, FIN state, Cookie**: Internal TCP state tracking information. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security flow session session-identifier 36

```
user@host> show security flow session session-identifier 36
Session ID: 36, Status: Normal, Flag: 0x8094540
Virtual system: Root VSYS(I), Policy name: foo/4
Maximum timeout: 1800, Current timeout: 1646
Start time: 61995, Duration: 158
   In: 10.10.10.1/4923 --> 3.3.3.2/23;tcp,
    Interface: t1-1/0/0.0,
    Session token: 0x12, Flag: 0x8094530
    Route: 0x70010, Gateway: 10.10.10.0, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0, Cookie: 0,
   Out: 3.3.3.2/23 --> 10.10.10.1/4923;tcp,
    Interface: .local..0,
    Session token: 0x4, Flag: 0x8094530
    Route: 0xfffb0006, Gateway: 3.3.3.2, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0, Cookie: 0,
1 sessions displayed
```

## Sample Output

show security flow session session-identifier 2218

```
user@host> show security flow session session-identifier 2218
Session ID: 2218, Status: Normal, Flag: 0x8094660
Virtual system: Root VSYS(I), Policy name: foo/4
Maximum timeout: 60, Current timeout: 60
Start time: 0, Duration: 0
Client: MGCP ALG, Group: 2047, Resource: 8188
   In: 12.0.102.26/28072 --> 11.0.101.236/23252;udp,
    Interface: ge-0/0/2.0,
    Session token: 0xa, Flag: 0x8094740
    Route: 0xb0010, Gateway: 12.0.102.26, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0, Cookie: 0,
   Out: 11.0.101.236/23252 --> 12.0.102.26/28072;udp,
    Interface: ge-0/0/1.0,
    Session token: 0x8, Flag: 0x8094740
Route: 0xa0010, Gateway: 11.0.101.236, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0, Cookie: 0,
1 sessions displayed
```

## Sample Output

show security flow session session-identifier 33

```
user@host> show security flow session session-identifier 33
Session ID: 33, Status: Normal, Flag: 0x80a15f0
Virtual system: Root VSYS(I), Policy name: default-policy/2
Application: junos-ftp/1
Maximum timeout: 1800, Current timeout: 1492
Start time: 31128, Duration: 121
   In: 10.10.10.1/2851 --> 192.168.0.2/21;tcp,
    Interface: t1-1/0/0.0,
Session token: 0x6, Flag: 0x80a15e0
    Route: 0x60010, Gateway: 10.10.10.0, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0, Cookie: 0,
   Out: 192.168.0.2/21 --> 10.10.10.1/2851;tcp,
```

Copyright © 2013, Juniper Networks, Inc.

```
    Interface: ge-0/0/1.0,
    Session token: 0x6, Flag: 0x80a15e0
    Route: 0x90010, Gateway: 192.168.0.2, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0, Cookie: 0,
1 sessions displayed
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow session source-port

**Syntax**
**show security flow session source-port**
source-port-number
[brief | extensive | summary]

**Release Information**
Command introduced in Release 8.5 of Junos OS; Filter and view options introduced in Release 10.2 of Junos OS.

**Description**
Display information about each session that uses the specified source port.

**Options**
- ***source-port-number*** —Number of the source port about which to display sessions information.
- brief | extensive | summary–Display the specified level of output.

**Required Privilege Level**
view

**Related Documentation**
- clear security flow session source-port on page 1423

**List of Sample Output**
show security flow session source-port 32785 on page 1953
show security flow session source-port 32785 brief on page 1953
show security flow session source-port 32785 extensive on page 1953
show security flow session source-port 32785 summary on page 1954

**Output Fields**
Table 133 on page 1951 lists the output fields for the **show security flow session source-port** command. Output fields are listed in the approximate order in which they appear.

### Table 133: show security flow session source-port Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the session. You can use this ID to get additional information about the session. |
| **Policy name** | Policy that permitted the traffic. |
| **Timeout** | Idle timeout after which the session expires. |
| **Resource information** | Information about the session particular to the resource manager, including the name of the ALG, the group ID, and the resource ID. |
| **In** | Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Out** | Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |

Copyright © 2013, Juniper Networks, Inc.

Table 133: show security flow session source-port Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Total sessions** | Total number of sessions. |
| **Status** | Session status. |
| **Flag** | Internal flag depicting the state of the session, used for debugging purposes. |
| **Policy name** | Name and ID of the policy that the first packet of the session matched. |
| **Source NAT pool** | The name of the source pool where NAT is used. |
| **Application** | Name of the application. |
| **Maximum timeout** | Maximum session timeout. |
| **Current timeout** | Remaining time for the session unless traffic exists in the session. |
| **Session State** | Session state. |
| **Start time** | Time when the session was created, offset from the system start time. |
| **Valid sessions** | Number of valid sessions. |
| **Pending sessions** | Number of pending sessions. |
| **Invalidated sessions** | Number of invalidated sessions. |
| **Sessions in other states** | Number of sessions in other states. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session source-port 32785

```
root> show security flow session source-port 32785
Flow Sessions on FPC4 PIC1:

Session ID: 170068424, Policy name: default-policy/2, Timeout: 1758, Valid
  In: 40.0.0.100/32785 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 10, Bytes:
610
  Out: 30.0.0.100/23 --> 40.0.0.100/32785;tcp, If: ge-0/0/1.0, Pkts: 9, Bytes:
602
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session source-port 32785 brief

```
root> show security flow session source-port 32785 brief
Flow Sessions on FPC4 PIC1:

Session ID: 170068424, Policy name: default-policy/2, Timeout: 1758, Valid
  In: 40.0.0.100/32785 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 10, Bytes:
610
  Out: 30.0.0.100/23 --> 40.0.0.100/32785;tcp, If: ge-0/0/1.0, Pkts: 9, Bytes:
602
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session source-port 32785 extensive

```
root> show security flow session source-port 32785 extensive
Flow Sessions on FPC4 PIC1:

Session ID: 170068424, Status: Normal
Flag: 0x40
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-telnet/10
Maximum timeout: 1800, Current timeout: 1754
Session State: Valid
Start time: 670711, Duration: 67
   In: 40.0.0.100/32785 --> 30.0.0.100/23;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 10, Bytes: 610
   Out: 30.0.0.100/23 --> 40.0.0.100/32785;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 9, Bytes: 602
```

Copyright © 2013, Juniper Networks, Inc.

```
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session source-port 32785 summary

```
root> show security flow session source-port 32785 summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow session source-prefix

**Syntax**
**show security flow session source-prefix**
*source-prefix-number*
[brief | extensive | summary]

**Release Information**
Command introduced in Release 8.5 of Junos OS.
Support for IPv6 addresses added in Release 10.2 of Junos OS. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Release 10.4 of Junos OS.
Filter and view options introduced in Release 10.2 of Junos OS.

**Description**
Display information about each session that uses the specified source prefix.

**Options**
*source-prefix-number*—Source IP prefix or address for which to display sessions information.

**brief | extensive | summary**—Display the specified level of output.

**Required Privilege Level**
view

**Related Documentation**
- clear security flow session source-prefix on page 1424

**List of Sample Output**
show security flow session source-prefix 40/8 on page 1957
show security flow session source-prefix 40/8 brief on page 1957
show security flow session source-prefix 40/8 extensive on page 1957
show security flow session source-prefix 40/8 summary on page 1958

**Output Fields**
Table 134 on page 1955 lists the output fields for the **show security flow session source-prefix** command. Output fields are listed in the approximate order in which they appear.

### Table 134: show security flow session source-prefix Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the session. You can use this ID to get additional information about the session. |
| **Policy name** | Policy that permitted the traffic. |
| **Timeout** | Idle timeout after which the session expires. |
| **In** | Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Out** | Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |

Copyright © 2013, Juniper Networks, Inc.

Table 134: show security flow session source-prefix Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Total sessions** | Total number of sessions. |
| **Status** | Session status. |
| **Flag** | Internal flag depicting the state of the session, used for debugging purposes. |
| **Policy name** | Name and ID of the policy that the first packet of the session matched. |
| **Source NAT pool** | The name of the source pool where NAT is used. |
| **Application** | Name of the application. |
| **Maximum timeout** | Maximum session timeout. |
| **Current timeout** | Remaining time for the session unless traffic exists in the session. |
| **Session State** | Session state. |
| **Start time** | Time when the session was created, offset from the system start time. |
| **Valid sessions** | Number of valid sessions. |
| **Pending sessions** | Number of pending sessions. |
| **Invalidated sessions** | Number of invalidated sessions. |
| **Sessions in other states** | Number of sessions in other states. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session source-prefix 40/8

```
root> show security flow session source-prefix 40/8
Flow Sessions on FPC4 PIC1:

Session ID: 170068424, Policy name: default-policy/2, Timeout: 1784, Valid
  In: 40.0.0.100/32785 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 3, Bytes: 194

  Out: 30.0.0.100/23 --> 40.0.0.100/32785;tcp, If: ge-0/0/1.0, Pkts: 2, Bytes:
112
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session source-prefix 40/8 brief

```
root> show security flow session source-prefix 40/8 brief
Flow Sessions on FPC4 PIC1:

Session ID: 170068424, Policy name: default-policy/2, Timeout: 1784, Valid
  In: 40.0.0.100/32785 --> 30.0.0.100/23;tcp, If: ge-0/0/2.0, Pkts: 3, Bytes: 194

  Out: 30.0.0.100/23 --> 40.0.0.100/32785;tcp, If: ge-0/0/1.0, Pkts: 2, Bytes:
112
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session source-prefix 40/8 extensive

```
root> show security flow session source-prefix 40/8 extensive
Flow Sessions on FPC4 PIC1:

Session ID: 170068424, Status: Normal
Flag: 0x40
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-telnet/10
Maximum timeout: 1800, Current timeout: 1800
Session State: Valid
Start time: 670711, Duration: 21
   In: 40.0.0.100/32785 --> 30.0.0.100/23;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 40.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 10, Bytes: 610
   Out: 30.0.0.100/23 --> 40.0.0.100/32785;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 30.0.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 9, Bytes: 602
```

Copyright © 2013, Juniper Networks, Inc.

```
Total sessions: 1

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session source-prefix 40/8 summary

```
root> show security flow session source-prefix 40/8 summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1

Flow Sessions on FPC5 PIC0:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow session summary family

**Syntax** show security flow session summary family (inet | inet6)

**Release Information** Command introduced in Release 10.2 of Junos OS.
Support on SRX Series and J Series devices for flow-based mode for family inet6 added in Release 10.2 of Junos OS.
Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Release 10.4 of Junos OS.

**Description** Display filtered summary of information about existing sessions, including types of sessions, active and failed sessions, and the maximum allowed number of sessions.

**Options**
- **inet**—Display details summary of IPv4 sessions.
- **inet6**—Display details summary of IPv6 sessions.

**Required Privilege Level** view

**Related Documentation**
- clear security flow session all on page 1408

**List of Sample Output**
show security flow session summary family inet on page 1960
show security flow session summary family inet6 on page 1960

**Output Fields** Table 135 on page 1959 lists the output fields for the **show security flow session summary family** command. Output fields are listed in the approximate order in which they appear.

### Table 135: show security flow session summary Output Fields

| Field Name | Field Description |
|---|---|
| **Valid sessions** | Count of valid sessions. |
| **Pending sessions** | Count of pending sessions. |
| **Invalidated sessions** | Count of sessions the security device has determined to be invalid. |
| **Sessions in other states** | Count of sessions not in valid, pending, or invalidated state. |
| **Total sessions** | Total of the above counts. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session summary family inet

```
user@host> show security flow session summary family inet
Session summary for family inet:
Valid sessions: 20
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 20
```

### show security flow session summary family inet6

```
user@host> show security flow session summary family inet6
Session summary for family inet6:
Valid sessions: 20
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 20
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow session summary node

**Syntax** **show security flow session summary node (*node-id* | all | local | primary)**

**Release Information** Command introduced in Release 8.5 of Junos OS; node options added in Release 9.0 of Junos OS. Filter options added in Release 10.2 of Junos OS.
Support on SRX Series and J Series devices for flow-based mode for family inet6 added in Release 10.2 of Junos OS.
Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Release 10.4 of Junos OS.

**Description** Display information about all currently active security sessions on the device for the specified node options in summary mode.

**Options** **node**—(Optional) For chassis cluster configurations, display session information on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**
- show security flow session on page 1879

**List of Sample Output**
show security flow session summary node 0 on page 1963
show security flow session summary node 1 on page 1963
show security flow session summary node all on page 1964
show security flow session summary node local on page 1965
show security flow session summary node primary on page 1966

**Output Fields** Table 136 on page 1961 lists the output fields for the **show security flow session summary node** command. Output fields are listed in the approximate order in which they appear.

### Table 136: show security flow session summary node Output Fields

| Field Name | Field Description |
|---|---|
| **Unicast-sessions** | Number of unicast sessions. |
| **Multicast-sessions** | Number of multicast sessions. |
| **Failed-sessions** | Number of failed sessions. |

Copyright © 2013, Juniper Networks, Inc.

Table 136: show security flow session summary node Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Sessions-in-use** | Number of sessions in use.<br>• Valid sessions<br>• Pending sessions<br>• Invalidated sessions<br>• Sessions in other states |
| **Maximum-sessions** | Number of maximum sessions. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session summary node 0

```
root@antbert> show security flow session summary node 0
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 524288

Flow Sessions on FPC4 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576

Flow Sessions on FPC4 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576
```

### show security flow session summary node 1

```
root@antbert> show security flow session summary node 1
node1:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 524288

Flow Sessions on FPC4 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
```

Copyright © 2013, Juniper Networks, Inc.

```
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576

Flow Sessions on FPC4 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576
```

### show security flow session summary node all

```
root@antbert> show security flow session summary node all
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 524288

Flow Sessions on FPC4 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576

Flow Sessions on FPC4 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576

node1:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
```


Copyright © 2013, Juniper Networks, Inc.

```
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 524288

Flow Sessions on FPC4 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576

Flow Sessions on FPC4 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576
```

### show security flow session summary node local

```
root@antbert> show security flow session summary node local
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 524288

Flow Sessions on FPC4 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576

Flow Sessions on FPC4 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
```

```
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576
```

### show security flow session summary node primary

```
root@antbert> show security flow session summary node primary
node0:
--------------------------------------------------------------------------

Flow Sessions on FPC3 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 524288

Flow Sessions on FPC4 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576

Flow Sessions on FPC4 PIC1:
Unicast-sessions: 0
Multicast-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 1048576
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow session summary services-offload

**Syntax** **show security flow session summary services-offload** [*filter*]

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Display information about all currently active services-offload security sessions on the device in summary mode.

**Options**

- *filter*—Filter the display by the specified criteria.

  The following filters reduce the display to those sessions that match the criteria specified by the filter:

  **application**—Application name.

  **application-firewall-rule-set**—Application firewall enabled with the specified rule set.

  **application-traffic-control-rule-set**—Application traffic control enabled with the specified rule set.

  **destination-port**—Destination port.

  **destination-prefix**—Destination IP prefix or address.

  **dynamic-application**—Dynamic application name.

  **dynamic-application-group**—Dynamic application group name.

  **family**—Protocol family.

  **interface**—Name of incoming or outgoing interface.

  **logcal-system**—Logical system name.

  **protocol**—IP protocol number.

  **root-logical-system**—Root logical system name.

  **source-port**—Source port.

  **source-prefix**—Source IP prefix or address.

**Required Privilege Level** view

**Related Documentation**

- clear security flow session services-offload on page 1419

**List of Sample Output**

show security flow session summary services-offload on page 1969
show security flow session summary services-offload application on page 1969
show security flow session summary services-offload destination-port on page 1970

Copyright © 2013, Juniper Networks, Inc.

**Output Fields** Table 137 on page 1968 lists the output fields for the **show security flow session summary services-offload** command. Output fields are listed in the approximate order in which they appear.

Table 137: show security flow session summary services-offload Output Fields

| Field Name | Field Description |
|---|---|
| **Unicast-sessions** | Number of unicast sessions. |
| **Multicast-sessions** | Number of multicast sessions. |
| **Services-offload-sessions** | Number of services-offload sessions. |
| **Failed-sessions** | Number of failed sessions. |
| **Sessions-in-use** | Number of sessions in use:<br>• Valid<br>• Pending<br>• Invalidated<br>• Sessions in other states |
| **Maximum-sessions** | Maximum number of sessions. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session summary services-offload

```
user@host> show security flow session summary services-offload
Flow Sessions on FPC1 PIC0:
Unicast-sessions: 0
Multicast-sessions: 0
Services-offload-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 409600

Flow Sessions on FPC2 PIC0:
Unicast-sessions: 1
Multicast-sessions: 0
Services-offload-sessions: 1
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 819200

Flow Sessions on FPC3 PIC0:
Unicast-sessions: 0
Multicast-sessions: 0
Services-offload-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 819200

Flow Sessions on FPC5 PIC0:
Unicast-sessions: 0
Multicast-sessions: 0
Services-offload-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 819200
```

### show security flow session summary

```
user@host> show security flow session summary services-offload application tftp
Flow Sessions on FPC5 PIC0:
Valid sessions: 0
```

Copyright © 2013, Juniper Networks, Inc.

services-offload application

```
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```

show security flow session summary services-offload destination-port

```
user@host> show security flow session summary services-offload destination-port 25
Flow Sessions on FPC5 PIC0:
Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC1:
Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```


Copyright © 2013, Juniper Networks, Inc.

## show security flow session tunnel

**Syntax** **show security flow session tunnel**
[brief | extensive | summary]

**Release Information** Command introduced in Release 8.5 of Junos OS; Filter and view options introduced in Release 10.2 of Junos OS.

**Description** Display information about all tunnel sessions.

**Options** none—Display all tunnel sessions.

**brief | extensive | summary**—Display the specified level of output.

**Required Privilege Level** view

**List of Sample Output**
show security flow session tunnel on page 1973
show security flow session tunnel brief on page 1973
show security flow session tunnel extensive on page 1973
show security flow session tunnel summar on page 1974

**Output Fields** Table 138 on page 1971 lists the output fields for the **show security flow session tunnel** command. Output fields are listed in the approximate order in which they appear.

### Table 138: show security flow session tunnel Output Fields

| Field Name | Field Description |
|---|---|
| **Session ID** | Number that identifies the session. You can use this ID to get additional information about the session. |
| **Policy name** | Policy that permitted the traffic. NA (Not Applicable) for a tunnel session. |
| **Timeout** | Idle timeout after which the session expires. NA (Not Applicable) for a tunnel session. |
| **In** | Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes). |
| **Total sessions** | Total number of sessions. |
| **Status** | Session status. |
| **Flag** | Internal flag depicting the state of the session, used for debugging purposes. |
| **Policy name** | Name and ID of the policy that the first packet of the session matched. |
| **Source NAT pool** | The name of the source pool where NAT is used. |
| **Application** | Name of the application. |

Copyright © 2013, Juniper Networks, Inc.

Table 138: show security flow session tunnel Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Maximum timeout** | Maximum session timeout. |
| **Current timeout** | Remaining time for the session unless traffic exists in the session. |
| **Session State** | Session state. |
| **Start time** | Time when the session was created, offset from the system start time. |
| **Valid sessions** | Number of valid sessions. |
| **Pending sessions** | Number of pending sessions. |
| **Invalidated sessions** | Number of invalidated sessions. |
| **Sessions in other states** | Number of sessions in other states. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow session tunnel

```
root> show security flow session tunnel
Flow Sessions on FPC4 PIC1:

Session ID: 170000327, Policy name: N/A, Timeout: N/A, Valid
  In: 50.0.0.111/0 --> 50.0.0.1/513;esp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0

Session ID: 170000328, Policy name: N/A, Timeout: N/A, Valid
  In: 50.0.0.111/0 --> 50.0.0.1/0;esp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0
Total sessions: 2

Flow Sessions on FPC5 PIC0:

Session ID: 200000325, Policy name: N/A, Timeout: N/A, Valid
  In: 50.0.0.111/0 --> 50.0.0.1/0;esp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0

Session ID: 200000326, Policy name: N/A, Timeout: N/A, Valid
  In: 50.0.0.111/0 --> 50.0.0.1/0;esp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0
Total sessions: 2

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session tunnel brief

```
root> show security flow session tunnel brief
Flow Sessions on FPC4 PIC1:

Session ID: 170000327, Policy name: N/A, Timeout: N/A, Valid
  In: 50.0.0.111/0 --> 50.0.0.1/513;esp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0

Session ID: 170000328, Policy name: N/A, Timeout: N/A, Valid
  In: 50.0.0.111/0 --> 50.0.0.1/0;esp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0
Total sessions: 2

Flow Sessions on FPC5 PIC0:

Session ID: 200000325, Policy name: N/A, Timeout: N/A, Valid
  In: 50.0.0.111/0 --> 50.0.0.1/0;esp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0

Session ID: 200000326, Policy name: N/A, Timeout: N/A, Valid
  In: 50.0.0.111/0 --> 50.0.0.1/0;esp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0
Total sessions: 2

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

### show security flow session tunnel extensive

```
root> show security flow session tunnel extensive
Flow Sessions on FPC4 PIC1:

Session ID: 170000327, Status: Normal
Flag: 0x10000
Policy name: N/A
Source NAT pool: Null
Maximum timeout: N/A, Current timeout: N/A
Session State: Valid
Start time: 8073, Duration: 241
   In: 50.0.0.111/0 --> 50.0.0.1/513;esp,
    Interface: ge-0/0/1.0,
```

Copyright © 2013, Juniper Networks, Inc.

```
    Session token: 0x1c0, Flag: 0x0x4000621
    Route: 0x50010, Gateway: 50.0.0.111, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0

Session ID: 170000328, Status: Normal
Flag: 0x10000
Policy name: N/A
Source NAT pool: Null
Maximum timeout: N/A, Current timeout: N/A
Session State: Valid
Start time: 8073, Duration: 241
   In: 50.0.0.111/0 --> 50.0.0.1/0;esp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x621
    Route: 0x50010, Gateway: 50.0.0.111, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
Total sessions: 2

Flow Sessions on FPC5 PIC0:

Session ID: 200000325, Status: Normal
Flag: 0x10000
Policy name: N/A
Source NAT pool: Null
Maximum timeout: N/A, Current timeout: N/A
Session State: Valid
Start time: 8072, Duration: 241
   In: 50.0.0.111/0 --> 50.0.0.1/0;esp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x4000621
    Route: 0x50010, Gateway: 50.0.0.111, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0

Session ID: 200000326, Status: Normal
Flag: 0x10000
Policy name: N/A
Source NAT pool: Null
Maximum timeout: N/A, Current timeout: N/A
Session State: Valid
Start time: 8072, Duration: 241
   In: 50.0.0.111/0 --> 50.0.0.1/0;esp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x621
    Route: 0x50010, Gateway: 50.0.0.111, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
Total sessions: 2

Flow Sessions on FPC5 PIC1:
Total sessions: 0
```

## show security flow session tunnel summar

```
root> show security flow session tunnel summary
Flow Sessions on FPC4 PIC1:
```


Copyright © 2013, Juniper Networks, Inc.

```
Valid sessions: 2
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 2

Flow Sessions on FPC5 PIC0:

Valid sessions: 2
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 2

Flow Sessions on FPC5 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0
```

Copyright © 2013, Juniper Networks, Inc.

## show security flow statistics

**Syntax** **show security flow statistics**

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display flow-related system statistics.

**Required Privilege Level** view

**Related Documentation**
- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices

**List of Sample Output** show security flow statistics on page 1977

**Output Fields** Table 139 on page 1976 lists the output fields for the **show security flow statistics** command. Output fields are listed in the approximate order in which they appear.

### Table 139: show security flow statistics Output Fields

| Field Name | Field Description |
|---|---|
| Current sessions | Number of current sessions. |
| Packets forwarded | Number of packets forwarded. |
| Packets dropped | Number of Packets dropped. |
| Fragment packets | Number of fragment packets. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow statistics

```
root> show security flow statistics
Flow Statistics of FPC4 PIC1:
    Current sessions: 63
    Packets forwarded: 3001
    Packets dropped: 1281
    Fragment packets: 0

  Flow Statistics of FPC5 PIC0:
    Current sessions: 22
    Packets forwarded: 859
    Packets dropped: 0
    Fragment packets: 0

  Flow Statistics of FPC5 PIC1:
    Current sessions: 22
    Packets forwarded: 858
    Packets dropped: 0
    Fragment packets: 0

  Flow Statistics Summary:
    System total valid sessions: 107
    Packets forwarded: 4718
    Packets dropped: 1281
    Fragment packets: 0
```

Copyright © 2013, Juniper Networks, Inc.

## show security flow status

**Syntax** **show security flow status**

**Release Information** Command introduced in Junos OS Release 10.2 ; session distribution mode option added in Junos OS Release 12.1X44-D10.

**Description** Display the flow processing modes and logging status.

**Required Privilege Level** view

**Related Documentation**
- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- MPLS for Security Devices

**List of Sample Output** show security flow status on page 1979

**Output Fields** Table 140 on page 1978 lists the output fields for the **show security flow status** command. Output fields are listed in the approximate order in which they appear.

### Table 140: show security flow status Output Fields

| Field Name | Field Description |
|---|---|
| Flow forwarding mode | Flow processing mode.<br>• Inet forwarding mode<br>• Inet6 forwarding mode<br>• MPLS forwarding mode<br>• ISO forwarding mode<br>• Session distribution mode |
| Flow trace status | Flow logging status.<br>• Flow tracing status<br>• Flow tracing options |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security flow status

```
root> show security flow status
  Flow forwarding mode:
    Inet forwarding mode: flow based
    Inet6 forwarding mode: flow based
    MPLS forwarding mode: drop
    ISO forwarding mode: drop
    Session distribution mode: hash based


  Flow trace status
    Flow tracing status: on
    Flow tracing options: all
```

Copyright © 2013, Juniper Networks, Inc.

## show security gprs sctp association

**Syntax** **show security gprs sctp association**

**Release Information** Command introduced in Junos OS Release 12.1X44-D10.

**Description** Display the Stream Control Transmission Protocol (SCTP) association information.

**Options** none—Display the security SCTP association.

**Required Privilege Level** view

**Related Documentation**
- clear security gprs sctp counters on page 1427
- General Packet Radio Service for Security Devices

**List of Sample Output** show security gprs sctp association on page 1980

**Output Fields** Table 141 on page 1980 lists the output fields for the **show security gprs sctp association** command. Output fields are listed in the approximate order in which they appear.

Table 141: show security gprs sctp association

| Field Name | Field Description |
|---|---|
| Association Information | Association Information of FPC and PIC. |
| SCTP association numbers<br>• Total association<br>• Output association | Number of SCTP associations. The SCTP association numbers field contains the total number of associations and number of output associations. |

### Sample Output

show security gprs sctp association

```
user@host>show security gprs sctp association
node0:
--------------------------------------------------------------------------
Association Information for FPC: 6      PIC: 0
SCTP association numbers:
Total association 0
Output association 0

node1:
--------------------------------------------------------------------------
Association Information for FPC: 6      PIC: 0
SCTP association numbers:
Total association 0
Output association 0
```


Copyright © 2013, Juniper Networks, Inc.

## show security gprs sctp counters

**Syntax** **show security gprs sctp counters**

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display the statistics of the received and dropped Stream Control Transmission Protocol (SCTP) packets.

**Options** none—Display the statistics of all received and dropped SCTP packets.

**Required Privilege Level** view

**Related Documentation**
- General Packet Radio Service for Security Devices
- clear security gprs sctp counters on page 1427

**List of Sample Output** show security gprs sctp counters on page 1982

**Output Fields** Table 142 on page 1981 lists the output fields for the **show security gprs sctp counters** command. Output fields are listed in the approximate order in which they appear.

### Table 142: show security gprs sctp counters

| Field Name | Field Description |
|---|---|
| Name | Name of the SCTP payload protocol identifier. |
| Received Counter | Number of SCTP packet counters received. |
| Drop Counter | Number of SCTP packet counters dropped due to error. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security gprs sctp counters

```
user@host> show security gprs sctp counters
Received/Dropped SCTP packet counters:
Name           Recevied Counter    Drop Counter
reserved       0                   0
iua            0                   0
m2ua           0                   0
m3ua           0                   0
sua            0                   0
m2pa           0                   0
v5ua           0                   0
h248           0                   0
bicc           0                   0
tali           0                   0
dua            0                   0
asap           0                   0
enrp           0                   0
h323           0                   0
qipc           0                   0
simco          0                   0
```


Copyright © 2013, Juniper Networks, Inc.

## show security group-vpn member ike security-associations

**Syntax** show security group-vpn member ike security-associations [brief | detail] [index *sa-index*] [*peer-ipaddress*]

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display IKE security associations (SAs) for a group member.

**Options**

- none—Display summary information about all IKE SAs for the group member.
- **brief**—(Optional) Display summary output.
- **detail**—(Optional) Display detailed output.
- **index** *sa-index*—(Optional) Display detailed information about the specified SA identified by index number. To obtain a list of all SAs that includes their index numbers, use the command with no options.
- *peer-ipaddress*—(Optional) Display information about the SA with the specified peer.

**Required Privilege Level** view

**Related Documentation**

- clear security group-vpn member ike security-associations on page 1430

**List of Sample Output**

show security group-vpn member ike security-associations on page 1986
show security group-vpn member ike security-associations detail on page 1986

**Output Fields** Table 143 on page 1983 lists the output fields for the **show security group-vpn member ike security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 143: show security group-vpn member ike security-associations Output Fields

| Field Name | Field Description |
|---|---|
| **Index** | Index number of an SA. This number is an internally generated number you can use to display information about a single SA. |
| **Remote Address** | IP address of the destination peer with which the local peer communicates. |
| **State** | State of the IKE security associations:<br>• **DOWN**—SA has not been negotiated with the peer.<br>• **UP**—SA has been negotiated with the peer. |
| **Initiator cookie** | Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered. |

Copyright © 2013, Juniper Networks, Inc.

Table 143: show security group-vpn member ike security-associations Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Responder cookie** | Random number generated by the remote node and sent back to the initiator as a verification that the packets were received.<br><br>A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity. |
| **Mode** | Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between themselves. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are<br><br>• **main**—The exchange is done with six messages. This mode or exchange type encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate.<br>• **aggressive**—The exchange is done with three messages. This mode or exchange type does not encrypt the payload, leaving the identity of the neighbor unprotected. |
| **IKE Peer** | IP address of the destination peer with which the local peer communicates. |
| **Exchange type** | Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between themselves. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are<br><br>• **main**—The exchange is done with six messages. This mode or exchange type encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate.<br>• **aggressive**—The exchange is done with three messages. This mode or exchange type does not encrypt the payload, leaving the identity of the neighbor unprotected. |
| **Authentication method** | Method the server uses to authenticate the source of IKE messages:<br><br>• **pre-shared-keys**—Preshared key for encryption and decryption that both participants must have before beginning tunnel negotiations.<br><br>**rsa-signatures** —Digital signature, a certificate that confirms the identity of the certificate holder. |
| **Local** | Address of the local peer. |
| **Remote** | Address of the remote peer. |
| **Lifetime** | Number of seconds remaining until the IKE SA expires. |


Copyright © 2013, Juniper Networks, Inc.

Table 143: show security group-vpn member ike security-associations Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Algorithms** | Internet Key Exchange (IKE) algorithms used to encrypt and secure exchanges between the peers during the IPsec Phase 2 process:<br>• **Authentication**—Type of authentication algorithm used.<br>  • **sha1**—Secure Hash Algorithm 1(sha1) authentication.<br>  • **md5**—MD5 authentication.<br>• **Encryption**—Type of encryption algorithm used.<br>  • **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption.<br>  • **aes-192-cbc**— AES192-bit encryption<br>  • **aes-128-cbc**—AES 128-bit encryption.<br>  • **3des-cbc**—3 Data Encryption Standard (DES) encryption.<br>  • **des-cbc**—DES encryption. |
| **Traffic statistics** | • **Input bytes—**Number of bytes received.<br>• **Output bytes—**Number of bytes transmitted.<br>• **Input packets—**Number of packets received.<br>• **Output packets—**Number of packets transmitted. |
| **IPSec security associations** | • ***number* created:** The number of SAs created.<br>• ***number* deleted**: The number of SAs deleted. |
| **Phase 2 negotiations in progress** | Number of Phase 2 IKE negotiations in progress and status information:<br>• **Negotiation type**—Type of Phase 2 negotiation. Junos OS currently supports quick mode.<br>• **Message ID**—Unique identifier for a Phase 2 negotiation.<br>• **Local identity**—Identity of the local Phase 2 negotiation. The format is id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation)<br>• **Remote identity**—Identity of the remote Phase 2 negotiation. The format is id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation)<br>• **Flags**—Notification to the key management process of the status of the IKE negotiation:<br>  • **caller notification sent**—Caller program notified about the completion of the IKE negotiation.<br>  • **waiting for done**—Negotiation is done. The library is waiting for the remote end retransmission timers to expire.<br>  • **waiting for remove**—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation.<br>  • **waiting for policy manager**—Negotiation is waiting for a response from the policy manager. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security group-vpn member ike security-associations

```
user@host> show security group-vpn member ike security-associations
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode
1       10.1.1.11       UP     a9b023fbdc7a6571  a67cefbc3397c3c2  Main
```

## Sample Output

show security group-vpn member ike security-associations detail

```
user@host> show security group-vpn member ike security-associations detail
IKE peer 10.1.1.11, Index 411,
  Role: Initiator, State: UP
  Initiator cookie: 941108c6c186324a, Responder cookie: 0000000000000000
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 10.1.1.13:848, Remote: 10.1.1.11:848
  Lifetime: Expires in 3536 seconds
  Algorithms:
   Authentication        : unknown
   Encryption            : unknown
   Pseudo random function: unknown
  Traffic statistics:
   Input  bytes  :                   0
   Output bytes  :                 560
   Input  packets:                   0
   Output packets:                   4
  IPSec security associations: 0 created, 0 deleted
  Phase 2 negotiations in progress: 0
```


Copyright © 2013, Juniper Networks, Inc.

## show security group-vpn member ipsec security-associations

**Syntax** show security group-vpn member ipsec security-associations [brief | detail] [index *sa-index*]

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display group VPN security associations (SAs) for a group member.

**Options**
- none—Display information about all group VPN SAs for the group member.
- **brief**—(Optional) Display summary output.
- **detail**—(Optional) Display detailed output.
- **index** *sa-index*—(Optional) Display detailed information about the specified SA identified by index number. To obtain a list of all SAs that includes their index numbers, use the command with no options.

**Required Privilege Level** view

**Related Documentation**
- clear security group-vpn member ipsec security-associations on page 1431

**List of Sample Output**
show security group-vpn member ipsec security-associations on page 1989
show security group-vpn member ipsec security-associations detail on page 1989

**Output Fields** Table 144 on page 1987 lists the output fields for the **show security group-vpn member ipsec security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 144: show security group-vpn member ipsec security-associations

| Field Name | Field Description |
|---|---|
| **Total active tunnels** | Total number of active IPsec tunnels. |
| **ID** | Index number of the SA. You can use this number to get additional information about the SA. |
| **Server** | IP address of the group server (remote gateway). |
| **Port** | If Network Address Translation-Traversal (NAT-T) is used, this value is 4500. Otherwise it is the standard IKE port, 500. |
| **Algorithm** | Cryptography used to secure exchanges between peers during the IKE Phase 2 negotiations includes<br>• An authentication algorithm used to authenticate exchanges between the peers. Options are **sha1** or **md5.**<br>• An encryption algorithm used to encrypt data traffic. Options are **3des**, **aes-128**, **aes-192**, **aes-256**, and **des**. |
| **SPI** | Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI. |

Copyright © 2013, Juniper Networks, Inc.

Table 144: show security group-vpn member ipsec security-associations *(continued)*

| Field Name | Field Description |
|---|---|
| **Life: sec/kb** | The lifetime of the SA, after which it expires, expressed either in seconds or kilobytes. |
| **GId** | Group identifier. |
| **vsys or Virtual-system** | The root system. |
| **Local Gateway** | Gateway address of the local system. |
| **GDOI Server** | IP address of the group server. |
| **Local Identity** | Identity of the local peer so that its partner destination gateway can communicate with it. The value is specified as an IPv4 address, fully qualified domain name, e-mail address, or distinguished name. |
| **Remote Identity** | IPv4 address of the destination peer gateway. |
| **DF-bit** | State of the don't fragment bit: set or cleared. |
| **Policy name** | Name of the applicable policy. |
| **Direction** | Direction of the security association; it can be inbound or outbound. |
| **AUX-SPI** | Value of the auxiliary security parameter index.<br>• When the value is AH or ESP, AUX-SPI is always 0.<br>• When the value is AH+ESP, AUX-SPI is always a positive integer. |
| **Hard lifetime** | The hard lifetime specifies the lifetime of the SA.<br>• **Expires in seconds**—Number of seconds left until the SA expires. |
| **Lifesize Remaining** | The lifesize remaining specifies the usage limits in kilobytes. If there is no lifesize specified, it shows unlimited.<br>• **Expires in kilobytes**—Number of kilobytes left until the SA expires. |
| **Soft lifetime** | The soft lifetime informs the IPsec key management system that the SA is about to expire.<br>Each lifetime of a security association has two display options, hard and soft, one of which must be present for a dynamic security association. This allows the key management system to negotiate a new SA before the hard lifetime expires.<br>• **Expires in seconds**—Number of seconds left until the SA expires. |
| **Mode** | Mode of the security association:<br>• transport—Protects host-to-host connections.<br>• tunnel—Protects connections between security gateways. |
| **Protocol** | Protocol supported. Transport mode supports Encapsulation Security Protocol (ESP). |


Copyright © 2013, Juniper Networks, Inc.

Table 144: show security group-vpn member ipsec security-associations *(continued)*

| Field Name | Field Description |
|---|---|
| **Anti-replay service** | State of the service that prevents packets from being replayed. It can be **Enabled** or **Disabled**. |

## Sample Output

show security group-vpn member ipsec security-associations

```
user@host> show security group-vpn member ipsec security-associations
  Total active tunnels: 1
  ID    Server          Port  Algorithm       SPI      Life:sec/kb  GId vsys
  >133955585 10.1.1.11   848   ESP:3des/sha1   d1d5e67d 587/  unlim   2   root
  <133955585 10.1.1.11   848   ESP:3des/sha1   d1d5e67d 587/  unlim   2   root
```

## Sample Output

show security group-vpn member ipsec security-associations detail

```
user@host> show security group-vpn member ipsec security-associations detail
  Virtual-system: root
  Local Gateway: 10.1.1.28, GDOI Server: 10.1.1.37
  Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
    DF-bit: clear
    Policy-name: p5-0001

    Direction: outbound, SPI: 68df21cc, AUX-SPI: 0, Group Id: 2
    Hard lifetime: Expires in 546 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 516 seconds
    Mode: shared, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Anti-replay service: time-based enabled, Replay window size: 100

    Direction: inbound, SPI: 68df21cc, AUX-SPI: 0, Group Id: 2
    Hard lifetime: Expires in 546 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 516 seconds
    Mode: shared, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Anti-replay service: time-based enabled, Replay window size: 100
```

Copyright © 2013, Juniper Networks, Inc.

## show security group-vpn member kek security-associations

**Syntax** show security group-vpn member kek security-associations [brief | detail] [index *sa-index*] [*peer-ipaddress*]

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display group VPN security associations (SAs) for a group member.

**Options**

- none—Display information about all group VPN SAs for the group member.
- **brief**—(Optional) Display summary output.
- **detail**—(Optional) Display detailed output.
- **index** *sa-index*—(Optional) Display detailed information about the specified SA identified by index number. To obtain a list of all SAs that includes their index numbers, use the command with no options.
- *peer-ipaddress*—(Optional) Display information about the SA with the specified peer.

**Required Privilege Level** view

**Related Documentation**

- clear security group-vpn member kek security-associations on page 1432

**List of Sample Output**

show security group-vpn member kek security-associations on page 1992
show security group-vpn member kek security-associations detail on page 1992

**Output Fields** Table 145 on page 1990 lists the output fields for the **show security group-vpn member kek security-associations** command. Output fields are listed in the approximate order in which they appear.

### Table 145: show security group-vpn member kek security-associations

| Field Name | Field Description |
|---|---|
| **Index** | Index number of an SA. This number is an internally generated number you can use to display information about a single SA. |
| **Remote Address** | IP address of the destination peer with which the local peer communicates. |
| **State** | State of the KEK security associations:<br>• **DOWN**—SA is not active.<br>• **UP**—SA is active. |
| **Initiator cookie** | Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered. |
| **Responder cookie** | Random number generated by the remote node and sent back to the initiator as a verification that the packets were received. |


Copyright © 2013, Juniper Networks, Inc.

Table 145: show security group-vpn member kek security-associations *(continued)*

| Field Name | Field Description |
|---|---|
| **SPI** | Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI. |
| **GroupID** | Group identifier. |
| **KEK Peer** | IP address of the destination peer with which the local peer communicates. |
| **Role** | For the member, it is always responder. |
| **State** | State of the KEK security associations, which is always up. |
| **Authentication method** | RSA is the supported authentication method. |
| **Local** | Address of the local peer. |
| **Remote** | Address of the remote peer. |
| **Lifetime** | Number of seconds remaining until the IKE SA expires. |
| **Algorithms** | Internet Key Exchange (IKE) algorithms used to encrypt and secure exchanges between the peers during the IPsec Phase 2 process:<br>• **Sig-hash**—Type of authentication algorithm used.<br>  ◦ **sha1**—Secure Hash Algorithm 1(sha1) authentication.<br>  ◦ **md5**—MD5 authentication.<br>• **Encryption**—Type of encryption algorithm used.<br>  ◦ **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption.<br>  ◦ **aes-192-cbc**— AES192-bit encryption<br>  ◦ **aes-128-cbc**—AES 128-bit encryption.<br>  ◦ **3des-cbc**—3 Data Encryption Standard (DES) encryption.<br>  ◦ **des-cbc**—DES encryption. |
| **Traffic statistics** | • **Input bytes**—Number of bytes received.<br>• **Output bytes**—Number of bytes transmitted.<br>• **Input packets**—Number of packets received.<br>• **Output packets**—Number of packets transmitted. |
| **Server Info Version** | Identify the latest set of information maintained in the server. |
| **Server Heartbeat Interval** | Interval in seconds at which the server sends heartbeats to group members. |
| **Member Heartbeat Threshold** | The heartbeat threshold configured on the group member for the IPsec VPN. If this number of heartbeats is missed on the member, the member reregisters with the server. |
| **Heartbeat Timeout Left** | Number of heartbeats until the heartbeat threshold is reached, at which time the member reregisters with the server.<br>NOTE: When this number reaches 0, reregistration happens within 60 seconds. |

Copyright © 2013, Juniper Networks, Inc.

Table 145: show security group-vpn member kek security-associations *(continued)*

| Field Name | Field Description |
|---|---|
| **Server Activation Delay** | Number of seconds before a group member can use a new key when the member reregisters with the server. |
| **Server Multicast Group** | Multicast IP address to which the server sends rekey messages. |
| **Server Replay Window** | Antireplay time window value in seconds. 0 means antireplay is disabled. |
| **Group Key Push sequence number** | Sequence number of the KEK SA groupkey-push message. This number is incremented with every groupkey-push message, including heartbeats. |

## Sample Output

show security group-vpn member kek security-associations

```
user@host> show security group-vpn member kek security-associations
  Index   Remote Address  State  Initiator cookie  Responder cookie  GroupId
42      10.1.1.11       UP     a53603e30716fb74  8076194a850d56d0  2
```

## Sample Output

show security group-vpn member kek security-associations detail

```
user@host> show security group-vpn member kek security-associations detail
KEK peer 10.1.1.37, Index 277
  Role: Responder, State: UP
  Initiator cookie: d858215649fba214, Responder cookie: e2ebd3fff04cf9d2
  Authentication method: RSA
  Local: 10.1.1.28:848, Remote: 10.1.1.37:848
  Lifetime: Expires in 37 seconds
  Algorithms:
   Sig-hash             : sha1
   Encryption           : 3des-cbc
  Traffic statistics:
   Input  bytes  :                 748
   Output bytes  :                  68
   Input  packets:                   3
   Output packets:                   1
  Group Id: 2
  Server Info Version: 5
  Server Heartbeat Interval: 60, Member Heartbeat Threshold: 5
  Heartbeat Timeout Left: 5
  Server Activation Delay: 10
  Server Multicast Group: Unicast, Server Replay Window: 100
  Group Key Push sequence number: 5
```


Copyright © 2013, Juniper Networks, Inc.

## show security group-vpn server ike security-associations

**Syntax** show security group-vpn server ike security-associations [brief | detail] [group *group-name* | group-id *group-id*] [index *sa-index*]

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display IKE security associations (SAs).

**Options**

- none—Display all IKE SAs for all groups.
- brief—(Optional) Display summary output.
- **detail**—(Optional) Display detailed level of output.
- **group**—(Optional) Display IKE SAs for the specified group.
- **group-id**—(Optional) Display IKE SAs for the specified group.



NOTE: An IKE SA can be used by a group member to register to multiple groups. When you specify the group or group-id options to list the IKE SAs for a specified group, all existing IKE SAs that could be used to register to the group are displayed.

- **index**—(Optional) Display information for a particular SA based on the index number of the SA. To obtain the index number for a particular SA, display the list of existing SAs by using the command with no options.

**Required Privilege Level** view

**Related Documentation**

- show security group-vpn member ike security-associations on page 1983

**List of Sample Output**

show security group-vpn server ike security-associations on page 1996
show security group-vpn server ike security-associations detail on page 1996

**Output Fields** Table 146 on page 1993 lists the output fields for the **show security group-vpn server ike security-associations** command. Output fields are listed in the approximate order in which they appear.

### Table 146: show security group-vpn member ike security-associations Output Fields

| Field Name | Field Description |
|---|---|
| **Index** | Index number of an SA. This number is an internally generated number you can use to display information about a single SA. |
| **Remote Address** | IP address of the destination peer with which the local peer communicates. |

Copyright © 2013, Juniper Networks, Inc.

Table 146: show security group-vpn member ike security-associations Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **State** | State of the IKE security associations:<br>• **DOWN**—SA has not been negotiated with the peer.<br>• **UP**—SA has been negotiated with the peer. |
| **Initiator cookie** | Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered. |
| **Responder cookie** | Random number generated by the remote node and sent back to the initiator as a verification that the packets were received.<br>A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity. |
| **Mode** | Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between themselves. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are<br>• **main**—The exchange is done with six messages. This mode or exchange type encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate.<br>• **aggressive**—The exchange is done with three messages. This mode or exchange type does not encrypt the payload, leaving the identity of the neighbor unprotected. |
| **IKE Peer** | IP address of the destination peer with which the local peer communicates. |
| **Exchange type** | Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between themselves. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are<br>• **main**—The exchange is done with six messages. This mode or exchange type encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate.<br>• **aggressive**—The exchange is done with three messages. This mode or exchange type does not encrypt the payload, leaving the identity of the neighbor unprotected. |
| **Authentication method** | Method the server uses to authenticate the source of IKE messages:<br>• **pre-shared-keys**—Preshared key for encryption and decryption that both participants must have before beginning tunnel negotiations.<br>**rsa-signatures**—Digital signature, a certificate that confirms the identity of the certificate holder. |
| **Local** | Address of the local peer. |
| **Remote** | Address of the remote peer. |
| **Lifetime** | Number of seconds remaining until the IKE SA expires. |


Copyright © 2013, Juniper Networks, Inc.

Table 146: show security group-vpn member ike security-associations Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Algorithms** | Internet Key Exchange (IKE) algorithms used to encrypt and secure exchanges between the peers during the IPsec Phase 2 process:<br>• **Authentication**—Type of authentication algorithm used.<br>  • **sha1**—Secure Hash Algorithm 1(sha1) authentication.<br>  • **md5**—MD5 authentication.<br>• **Encryption**—Type of encryption algorithm used.<br>  • **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption.<br>  • **aes-192-cbc**— AES192-bit encryption<br>  • **aes-128-cbc**—AES 128-bit encryption.<br>  • **3des-cbc**—3 Data Encryption Standard (DES) encryption.<br>  • **des-cbc**—DES encryption. |
| **Traffic statistics** | • **Input bytes—**Number of bytes received.<br>• **Output bytes—**Number of bytes transmitted.<br>• **Input packets—**Number of packets received.<br>• **Output packets—**Number of packets transmitted. |
| **IPSec security associations** | • ***number* created:** The number of SAs created.<br>• ***number* deleted**: The number of SAs deleted. |
| **Phase 2 negotiations in progress** | Number of Phase 2 IKE negotiations in progress and status information:<br>• **Negotiation type**—Type of Phase 2 negotiation. Junos OS currently supports quick mode.<br>• **Message ID**—Unique identifier for a Phase 2 negotiation.<br>• **Local identity**—Identity of the local Phase 2 negotiation. The format is id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation)<br>• **Remote identity**—Identity of the remote Phase 2 negotiation. The format is id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation)<br>• **Flags**—Notification to the key management process of the status of the IKE negotiation:<br>  • **caller notification sent**—Caller program notified about the completion of the IKE negotiation.<br>  • **waiting for done**—Negotiation is done. The library is waiting for the remote end retransmission timers to expire.<br>  • **waiting for remove**—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation.<br>  • **waiting for policy manager**—Negotiation is waiting for a response from the policy manager. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security group-vpn server ike security-associations

```
user@host> show security group-vpn server ike security-associations
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode
2059    10.1.1.13       UP     86c09e79d3f986b6  aadaaaf97129b8cc  Main
```

## Sample Output

show security group-vpn server ike security-associations detail

```
user@host> show security group-vpn server ike security-associations detail
IKE peer 10.1.1.13, Index 2059,
  Role: Responder, State: UP
  Initiator cookie: 86c09e79d3f986b6, Responder cookie: aadaaaf97129b8cc
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 10.1.1.11:848, Remote: 10.1.1.13:848
  Lifetime: Expires in 3571 seconds
  Algorithms:
   Authentication        : sha1
   Encryption            : 3des-cbc
   Pseudo random function: hmac-sha1
  Traffic statistics:
   Input  bytes  :                  628
   Output bytes  :                 1196
   Input  packets:                    5
   Output packets:                    5
  Flags: Caller notification sent
  IPSec security associations: 0 created, 0 deleted
  Phase 2 negotiations in progress: 1

    Negotiation type: Quick mode, Role: Responder, Message ID: 2158764791
    Local: 10.1.1.11:848, Remote: 10.1.1.13:848
    Local identity: 10.1.1.11
    Remote identity: 10.1.1.13
    Flags: Caller notification sent, Waiting for done
```


Copyright © 2013, Juniper Networks, Inc.

## show security group-vpn server ipsec security-associations

**Syntax** show security group-vpn server ipsec security-associations [brief | detail] [group *group-name* | group-id *group-id*]

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display IPsec security associations (SAs).

**Options**
- none—Display all IPsec SAs for all groups.
- **brief**—(Optional) Display summary output.
- **detail**—(Optional) Display detailed level of output.
- **group**—(Optional) Display IPsec SAs for the specified group.
- **group-id**—(Optional) Display IPsec SAs for the specified group.

**Required Privilege Level** view

**Related Documentation**
- show security group-vpn member ipsec security-associations on page 1987

**List of Sample Output**
show security group-vpn server ipsec security-associations on page 1998
show security group-vpn server ipsec security-associations detail on page 1998

**Output Fields** Table 147 on page 1997 lists the output fields for the **show security group-vpn server ipsec security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 147: show security group-vpn server ipsec security-associations

| Field Name | Field Description |
|---|---|
| **Group** | Group name. |
| **Group ID** | Group identifier. |
| **Total IPsec SAs** | The total number of IPsec SAs for each group is shown. |
| **IPsec SA** | Name of the SA. |
| **Protocol** | Protocol supported. Transport mode supports Encapsulation Security Protocol (ESP). |
| **Algorithm** | Cryptography used to secure exchanges between peers during the IKE Phase 2 negotiations includes<br>• An authentication algorithm used to authenticate exchanges between the peers. Options are **sha1** and **md5**.<br>• An encryption algorithm used to encrypt data traffic. Options are **3des**, **aes-128**, **aes-192**, **aes-256**, or **des**. |

Copyright © 2013, Juniper Networks, Inc.

Table 147: show security group-vpn server ipsec security-associations *(continued)*

| Field Name | Field Description |
|---|---|
| **SPI** | Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI. |
| **Lifetime** | The lifetime of the SA, after which it expires, expressed in seconds. |
| **Policy Name** | Group policy associated with the IPsec SA. The source address, destination address, source port, destination port, and protocol defined for the policy are displayed. |

## Sample Output

show security group-vpn server ipsec security-associations

```
user@host> show security group-vpn server ipsec security-associations
Group: g2, Group Id: 2
  Total IPsec SAs: 2
  IPsec SA          Algorithm        SPI              Lifetime
  g2-gsa-1          ESP:aes-256/sha1 91f16f54         66
  g2-gsa-1          ESP:3des/sha1    39f8604a         1798
  g2-gsa-2          ESP:aes-256/sha1 e9450698         66
  g2-gsa-2          ESP:3des/sha1    99e3ead9         1798
Group: g3, Group Id: 3
  Total IPsec SAs: 2
  IPsec SA          Algorithm        SPI              Lifetime
  g2-gsa-1          ESP:aes-256/sha1 c81b4eba         66
  g2-gsa-1          ESP:3des/sha1    6696c219         1798
  g2-gsa-2          ESP:aes-256/sha1 e9230079         66
  g2-gsa-2          ESP:3des/sha1    710a231f         1798
```

In the output shown above, note that the encapsulation algorithm for the IPsec SAs changed from aes-256 to 3des. When this happened, the lifetime of the old key was reduced and the lifetime of the new key was set to 1800 seconds. When the **show** command was executed, 2 seconds had passed; therefore, the lifetime shown for the new keys is 1798 seconds.

## Sample Output

show security group-vpn server ipsec

```
user@host> show security group-vpn server ipsec security-associations detail
Group: g2, Group Id: 2
Total IPsec SAs: 2
```


Copyright © 2013, Juniper Networks, Inc.

security-associations detail

```
  IPsec SA: g2-gsa-1
    Protocol: ESP, Authentication: sha1, Encryption: aes-256
    SPI: 91f16f54
    Lifetime left: 52
    Policy Name: gsa-pol-1
      Source: 0.0.0.0/0
      Destination: 1.1.2.0/24
      Source Port: 5
      Destination Port: 0
      Protocol: 0
    Policy Name: gsa-pol-2
      Source: 0.0.0.0/0
      Destination: 2.1.2.0/24
      Source Port: 5
      Destination Port: 0
      Protocol: 0
  IPsec SA: g2-gsa-1
    Protocol: ESP, Authentication: sha1, Encryption: 3des
    SPI: 39f8604a
    Lifetime left: 1784
    Policy Name: gsa-pol-1
      Source: 0.0.0.0/0
      Destination: 1.1.2.0/24
      Source Port: 5
      Destination Port: 0
      Protocol: 0
    Policy Name: gsa-pol-2
      Source: 0.0.0.0/0
      Destination: 2.1.2.0/24
      Source Port: 5
      Destination Port: 0
      Protocol: 0
  IPsec SA: g2-gsa-2
    Protocol: ESP, Authentication: sha1, Encryption: aes-256
    SPI: e9450698
    Lifetime left: 52
  IPsec SA: g2-gsa-2
    Protocol: ESP, Authentication: sha1, Encryption: 3des
    SPI: 99e3ead9
    Lifetime left: 1784
Group: g3, Group Id: 3
Total IPsec SAs: 2
  IPsec SA: g2-gsa-1
    Protocol: ESP, Authentication: sha1, Encryption: aes-256
    SPI: c81b4eba
    Lifetime left: 52
    Policy Name: gsa-pol-1
      Source: 0.0.0.0/0
      Destination: 1.1.2.0/24
      Source Port: 5
      Destination Port: 0
      Protocol: 0
    Policy Name: gsa-pol-2
      Source: 0.0.0.0/0
      Destination: 2.1.2.0/24
      Source Port: 5
      Destination Port: 0
      Protocol: 0
  IPsec SA: g2-gsa-1
    Protocol: ESP, Authentication: sha1, Encryption: 3des
    SPI: 6696c219
```

Copyright © 2013, Juniper Networks, Inc.

```
  Lifetime left: 1784
  Policy Name: gsa-pol-1
    Source: 0.0.0.0/0
    Destination: 1.1.2.0/24
    Source Port: 5
    Destination Port: 0
    Protocol: 0
  Policy Name: gsa-pol-2
    Source: 0.0.0.0/0
    Destination: 2.1.2.0/24
    Source Port: 5
    Destination Port: 0
    Protocol: 0
IPsec SA: g2-gsa-2
  Protocol: ESP, Authentication: sha1, Encryption: aes-256
  SPI: e9230079
  Lifetime left: 52
IPsec SA: g2-gsa-2
  Protocol: ESP, Authentication: sha1, Encryption: 3des
  SPI: 710a231f
  Lifetime left: 1784
```


Copyright © 2013, Juniper Networks, Inc.

## show security group-vpn server kek security-associations

**Syntax** show security group-vpn server kek security-associations [brief | detail] [group *group-name* | group-id *group-id* | index *sa-index*]

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display configured server-member communications.

**Options**
- none—Display server-member communications configured for all groups.
- **brief**—(Optional) Display summary output.
- **detail**—(Optional) Display detailed output.
- **group**—(Optional) Display server-member communications configured for the specified group.
- **group-id**—(Optional) Display server-member communications configured for the specified group.
- **index**—(Optional) Display information for a particular SA based on the index number of the SA. To obtain the index number for a particular SA, display the list of existing SAs by using the command with no options.

**Required Privilege Level** view

**Related Documentation**
- show security group-vpn member kek security-associations on page 1990

**List of Sample Output**
show security group-vpn server kek security-associations on page 2003
show security group-vpn server kek security-associations detail on page 2003

**Output Fields** Table 148 on page 2001 lists the output fields for the **show security group-vpn server kek security-assocations** command. Output fields are listed in the approximate order in which they appear.

### Table 148: show security group-vpn server kek security-associations Output Fields

| Field Name | Field Description |
|---|---|
| **Index** | Index number of an SA. This number is an internally generated number you can use to display information about a single SA. |
| **Remote Address** | Identifier of the remote/peer. Because there could be multiple members, the remote address always contains the IP address 0.0.0.0. |
| **State** | State of the KEK security associations:<br>• **DOWN**—SA is not active.<br>• **UP**—SA is active. |

Copyright © 2013, Juniper Networks, Inc.

Table 148: show security group-vpn server kek security-associations Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Initiator cookie** | Random number generated by the server. This is used when the server needs to push data to a member or send heartbeats to a member, or a member needs to reply to the server. |
| **Responder cookie** | Random number generated by the server. This is used when the server needs to push data to a member or send heartbeats to a member, or a member needs to reply to the server. |
| **GroupId** | Group identifier. |
| **KEK Peer** | IP address of the destination peer with which the local peer communicates. For KEK SAs, it always contains 0.0.0.0 which means any IP address. |
| **Role** | For the server, it is always initiator. |
| **Authentication method** | RSA is the supported authentication method. |
| **Local** | Address of the local peer. |
| **Remote** | Address of the remote peer. |
| **Lifetime** | Number of seconds remaining until the IKE SA expires. |
| **Algorithms** | Internet Key Exchange (IKE) algorithms used to encrypt and secure exchanges between the peers during the Phase 2 process:<br>• **Sig-hash**—Type of authentication algorithm used.<br>  ◦ **sha1**—Secure Hash Algorithm 1(sha1) authentication.<br>  ◦ **md5**—MD5 authentication.<br>• **Encryption**—Type of encryption algorithm used.<br>  ◦ **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption.<br>  ◦ **aes-192-cbc**— AES192-bit encryption<br>  ◦ **aes-128-cbc**—AES 128-bit encryption.<br>  ◦ **3des-cbc**—3 Data Encryption Standard (DES) encryption.<br>  ◦ **des-cbc**—DES encryption. |
| **Traffic statistics** | • **Input bytes**—Number of bytes received.<br>• **Output bytes**—Number of bytes transmitted.<br>• **Input packets**—Number of packets received.<br>• **Output packets**—Number of packets transmitted. |
| **Server Info Version** | Identify the latest set of information maintained in the server. |
| The following fields are the configured **server-member-communication** options: | |
| **Server Heartbeat Interval** | Interval in seconds at which the server sends heartbeats to group members. |


Copyright © 2013, Juniper Networks, Inc.

Table 148: show security group-vpn server kek security-associations Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Server Activation Delay** | Number of seconds before a group member can use a new key when the member reregisters with the server. |
| **Server Multicast Group** | Multicast IP address to which the server sends rekey messages. |
| **Server Replay Window** | Antireplay time in seconds. This is 0 if antireplay is disabled. |
| **Retransmission Period** | Number of seconds between a rekey transmission and the first retransmission when there is no reply from the member. |
| **Number of Retransmissions** | For unicast communications, the number of times the server retransmits rekey messages to a member when there is no reply. For multicast communications, the number of copies of a message the server sends to members. |
| **Lifetime Seconds** | Configured lifetime, in seconds, for the KEK. |
| **Group Key Push sequence number** | Sequence number of the KEK SA groupkey-push message. This number is incremented with every groupkey-push message, including heartbeats. |

## Sample Output

show security group-vpn server kek security-associations

```
user@host> show security group-vpn server kek security-associations
Index   Remote Address  State  Initiator cookie  Responder cookie  GroupId
2051    0.0.0.0         UP     e3ead57303ae393d  d97290c9a91b6a2a  2
2052    0.0.0.0         UP     39985f6e9878d4fe  8ad3cabd99918841  3
```

## Sample Output

show security group-vpn server kek

```
user@host> show security group-vpn server kek security-associations detail
KEK peer 0.0.0.0, Index 2051
  Role: Initiator, State: UP
```

Copyright © 2013, Juniper Networks, Inc.

**security-associations detail**

```
  Initiator cookie: e3ead57303ae393d, Responder cookie: d97290c9a91b6a2a
  Authentication method: RSA
  Local: 10.1.1.11:848, Remote: 0.0.0.0:848
  Lifetime: Expires in 934 seconds
  Algorithms:
   Sig-hash             : sha1
   Encryption           : 3des-cbc
  Traffic statistics:
   Input  bytes  :                   0
   Output bytes  :                2652
   Input  packets:                   0
   Output packets:                  13
  Group Id: 2, Group Name: g2
  Server Info Version: 135
  Server Heartbeat Interval: 60
  Server Activation Delay: 17
  Server Multicast Group: Unicast, Server Replay Window: 100
  Retransmission Period: 4, Number of Retransmissions: 2
  Lifetime Seconds: 1800
  Group Key Push sequence number: 13

KEK peer 0.0.0.0, Index 2052
  Role: Initiator, State: UP
  Initiator cookie: 39985f6e9878d4fe, Responder cookie: 8ad3cabd99918841
  Authentication method: RSA
  Local: 10.1.1.11:848, Remote: 0.0.0.0:848
  Lifetime: Expires in 934 seconds
  Algorithms:
   Sig-hash             : sha1
   Encryption           : 3des-cbc
  Traffic statistics:
   Input  bytes  :                   0
   Output bytes  :                   0
   Input  packets:                   0
   Output packets:                   0
  Group Id: 3, Group Name: g3
  Server Info Version: 135
  Server Heartbeat Interval: 60
  Server Activation Delay: 17
  Server Multicast Group: Unicast, Server Replay Window: 100
  Retransmission Period: 4, Number of Retransmissions: 2
  Lifetime Seconds: 1800
  Group Key Push sequence number: 0
```


Copyright © 2013, Juniper Networks, Inc.

## show security group-vpn server registered-members

**Syntax** show security group-vpn server registered-members [group *group-name* | group-id *group-id*]

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display currently registered group members.

**Options**
- none—Display all group members for all groups.
- **group**—(Optional) Display group members for the specified group.
- **group-id**—(Optional) Display group members for the specified group.

**Required Privilege Level** view

**Related Documentation**
- clear security group-vpn server on page 1433

**List of Sample Output** show security group-vpn server registered-members on page 2006

**Output Fields** Table 149 on page 2005 lists the output fields for the **show security group-vpn server registered-members**command. Output fields are listed in the approximate order in which they appear.

Table 149: show security group—vpn server registered-members Output Fields

| Field Name | Field Description |
|---|---|
| **Group** | Group name. |
| **Group Id** | Group identifier. |
| **Member Gateway** | IP address of the gateway for the group member. |
| **Member IP** | IP address of the group member. |
| **Last Update** | The last time that members registered or sent acknowledgements to the server. |
| **Vsys** | The root system. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security group-vpn server registered-members

```
user@host> show security group-vpn server registered-members
Group: GroupA, Group Id: 1
  Member Gateway    Member IP   Last Update              Vsys
  gw-dn1            10.1.1.13   Tue Oct 20 2009 17:41:56 root
  gw-dn2            10.1.1.14   Tue Oct 20 2009 17:43:03 root

Group: GroupB, Group Id: 2
  Member Gateway    Member IP   Last Update              Vsys
  gw-enterprise     10.1.1.15   Tue Oct 20 2009 17:43:50 root
```


Copyright © 2013, Juniper Networks, Inc.

## show security idp active-policy

**Syntax** show security idp active-policy

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Display information about the policy name and running detector version with which the policy is compiled from IDP data plane module.

**Required Privilege Level** view

**Related Documentation**

- request security idp security-package download on page 1502
- request security idp security-package install on page 1504
- IDP Policies for Security Devices
- IDP Class of Service Action for Security Devices

**List of Sample Output** show security idp active-policy on page 2007

**Output Fields** Table 150 on page 2007 lists the output fields for the **show security idp active-policy** command. Output fields are listed in the approximate order in which they appear.

### Table 150: show security idp active-policy Output Fields

| Field Name | Field Description |
|---|---|
| **Policy Name** | Name of the running policy. |
| **Running Detector Version** | Current version of the running detector. |

## Sample Output

show security idp active-policy

```
user@host> show security idp active-policy
  Policy Name : viking-policy
  Running Detector Version : 9.1.140080300
```

Copyright © 2013, Juniper Networks, Inc.

## show security idp application-ddos application

**Syntax** show security idp application-ddos application

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Display basic statistics for the servers being protected by the IDP application–level DDoS feature.

**Options**

- ***application–name*** —Display information on a specific application-level DDoS application profile.
- **context**—Name of the application context for *application–name*
- **detail**—Display a detailed view of the protected servers.
- **server**—IP address of protected server.
- **zone**—Zone name where the protected server resides.

**Required Privilege Level** view

**Related Documentation**

- Application-Level Distributed Denial of Service
- IDP Policies for Security Devices

**List of Sample Output**
show security idp application-ddos application on page 2009
show security idp application-ddos application detail on page 2009

**Output Fields** Table 151 on page 2008 lists the output fields for the **show security idp application-ddos application** command.

### Table 151: show security idp application-ddos Output Fields

| Field Name | Field Description |
|---|---|
| **Zone** | Security zone where the protected server resides. |
| **Server** | IP address of the protected server. |
| **Application** | Name of the application-level DDoS application. |
| **Conn/sec** | Number of client connections to the protected server. |
| **Context** | Protocol context that is being monitored. |
| **Contexts/tick** | Number of protocol context hits measured per tick. One tick equals 60 seconds by default. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security idp application-ddos application

```
user@host> show security idp application-ddos application

Zone    Server      Application     Conn/sec    Context                 Contexts/tick
trust   81.0.3.1    http-server-1   2648/sec    http-header-user-agent    35746/60sec
trust   81.1.0.2    dns-server-1    4517/sec    dns-type-name            263234/60sec
trust   81.1.0.2    dns-server-1    1497/sec    dns-type-name             88061/60sec
trust   81.0.3.1    http-server1    1496/sec    http-url-parsed           81177/60sec

...
```

## Sample Output

### show security idp application-ddos application detail

```
user@host> show security idp application-ddos application detail

Zone: trust Server: 81.1.0.2 Application: dns-server-1 Connections/sec:
1499/secContext: dns-type-name Contexts/tick: 88061/60sec
Value: 00 05 74 65 73 74 6e 61 6d 65 2e 6a 75 6e 69 70 testname.juniper.net
Value: 65 72 2e 6e 65 74
Context values/tick : 29143/60sec

Zone: trust Server: 81.0.3.1 Application: http-server-1 Connections/sec:
2615/secContext: http-url contexts/tick: 148196/60sec
Value: 2f 6e 65 74 73 63 72 65 65 6e 2e 68 746d 6c /netscreen.htm
Context values/tick : 26809/60sec

...
```

Copyright © 2013, Juniper Networks, Inc.

## show security idp attack description

**Syntax** **show security idp attack description *attack-name***

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Display description of a specified IDP attack.

**Options**
- ***attack-name*** —IDP attack name.

**Required Privilege Level** view

**Related Documentation**
- clear security idp attack table on page 1436
- IDP Policies for Security Devices

**List of Sample Output** show security idp attack description on page 2010

**Output Fields** Table 152 on page 2010 lists the output fields for the **show security idp attack description** command. Output fields are listed in the approximate order in which they appear.

Table 152: show security idp attack description Output Fields

| Field Name | Field Description |
|---|---|
| **Description** | IDP attack description. |

### Sample Output

show security idp attack description

```
user@host> show security idp attack description FTP:USER:ROOT
Description: This signature detects attempts to login to an FTP server using the
 "root" account.  This can indicate an attacker trying to gain root-level access,
 or it can indicate poor security practices. FTP typically uses plain-text
passwords, and using the root account to FTP could expose sensitive data over the
 network.
```


Copyright © 2013, Juniper Networks, Inc.

## show security idp attack detail

**Syntax** **show security idp attack detail *attack-name***

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Display details of a specified IDP attack.

**Options**
- ***attack-name*** —IDP attack name.

**Required Privilege Level** view

**Related Documentation**
- clear security idp attack table on page 1436
- IDP Policies for Security Devices

**List of Sample Output** show security idp attack detail on page 2012

**Output Fields** Table 153 on page 2011 lists the output fields for the **show security idp attack detail** command. Output fields are listed in the approximate order in which they appear.

### Table 153: show security idp attack detail Output Fields

| Field Name | Field Description |
|---|---|
| **Display Name** | Display name of the IDP attack. |
| **Severity** | Severity level of the IDP attack. |
| **Category** | IDP attack category. |
| **Recommended** | Specifies whether a default action for the IDP attack is recommended by Juniper Networks (true or false). |
| **Recommended Action** | Recommended action for the IDP attack. |
| **Type** | Type of IDP attack. |
| **Direction** | Direction of the IDP attack. |
| **False Positives** | Specifies whether the IDP attack produces false positive on the network. |
| **Service** | IDP service configured for the IDP attack. If a service is configured for the IDP attack, the IDP service name is displayed. Otherwise, **Not available** is displayed. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security idp attack detail

```
user@host> show security idp attack detail FTP:USER:ROOT
Display Name: FTP: "root" Account Login
Severity: Minor
Category: FTP
Recommended: false
Recommended Action: None
Type: signature
Direction: CTS
False Positives: unknown
Service: Not available
```


Copyright © 2013, Juniper Networks, Inc.

## show security idp attack table

**Syntax** show security idp attack table

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Display detailed information of IDP attack table.

**Required Privilege Level** view

**Related Documentation**
- clear security idp attack table on page 1436
- IDP Policies for Security Devices

**List of Sample Output** show security idp attack table on page 2013

**Output Fields** Table 154 on page 2013 lists the output fields for the **show security idp attack table** command. Output fields are listed in the approximate order in which they appear.

### Table 154: show security idp attack table Output Fields

| Field Name | Field Description |
|---|---|
| **Attack name** | Name of the attack that you want to match in the monitored network traffic. |
| **Hits** | Total number of attack matches.<br><br>On SRX Series and J Series devices, for brute force and time-binding-related attacks, the logging is to be done only when the match **count** is equal to the **threshold**. That is, only one log is generated within the 60-second period in which the threshold is measured. This process prevents repetitive logs from being generated and ensures consistency with other IDP platforms, such as IDP-standalone.<br><br>When no attack is seen within the 60-second period and the BFQ entry is flushed out, the match count starts over the new attack match shows up in the attack table, and the log is generated. |

## Sample Output

**show security idp attack table**

```
user@host> show security idp attack table
IDP attack statistics:
  Attack name                                   #Hits
  HTTP:OVERFLOW:PI3WEB-SLASH-OF                 1
```

Copyright © 2013, Juniper Networks, Inc.

## show security idp counters application-ddos

**Syntax** show security idp counters application-ddos

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Display the status of all IDP application-ddos counter values.

**Required Privilege Level** view

**Related Documentation**
- Application-Level Distributed Denial of Service
- IDP Policies for Security Devices

**List of Sample Output** show security idp counters application-ddos on page 2016

**Output Fields** Table 155 on page 2014 lists the output fields for the **show security idp counters application-ddos** command. Output fields are listed in the approximate order in which they appear.

### Table 155: show security idp counters application-ddos Output Fields

| Field Name | Field Description |
|---|---|
| **App-DDOS inspected flows** | Number of client-to-server flows inspected for application-ddos. |
| **App-DDOS failed flows** | Number of client-to-server flows that failed during application-ddos processing. |
| **App-DDOS ignored flows** | Number of client-to-server flows ignored for application-ddos. |
| **App-DDOS first path failed** | Number of client-to-server flow initialization failures during first path. |
| **App-DDOS first path succeeded** | Number of successful client-to-server flow initialization during first path. |
| **App-DDOS dropped packets** | Number of packets dropped in the application-level DDoS module. |
| **App-DDOS processed packets** | Number of total packets processed in the application-level DDoS module. |
| **App-DDOS connection table process succeeded** | Number of times connection processing succeeded. |
| **App-DDOS connection table process failed** | Number of times connection processing failed. |
| **App-DDOS context process succeeded** | Number of times the context processing succeeded. |
| **App-DDOS context process failed** | Number of times context processing failed. |
| **App-DDOS ignore context** | Number of contexts ignored if the flow is not client-to-server or if the application-level DDoS module is disabled. |


Copyright © 2013, Juniper Networks, Inc.

Table 155: show security idp counters application-ddos Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **App-DDOS context values excluded** | Number of context values excluded for actions, reporting, or both. |
| **App-DDOS context value process succeeded** | Number of times context value processing succeeded, including action and logging events if configured. |
| **App-DDOS context value process failed** | Number of times context value processing failed, including action and logging events if configured. |
| **App-DDOS context value prune failed** | Number of times context value pruning failed. |
| **App-DDOS no action** | Number of times an attack is detected and no action is taken. |
| **App-DDOS drop connection action** | Number of times an attack is detected and a drop connection action is taken. |
| **App-DDOS drop packet action** | Number of times an attack is detected and a drop packet action is taken. |
| **App-DDOS close server action** | Number of times an attack is detected and a close server action is taken. |
| **App-DDOS IP Action block** | Number of times an ip-action block entry is created and installed. |
| **App-DDOS IP Action close** | Number of times an ip-action close entry is created and installed. |
| **App-DDOS Action notify** | Number of times an ip-action notify entry is created and installed. |
| **App-DDOS logs sent** | Number of attack logs sent. |
| **App-DDOS logs report failed** | Number of attack log reports that failed. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security idp counters application-ddos

```
user@host> show security idp counters application-ddos

App-DDOS inspected flows                                447172
App-DDOS failed flows                                   0
App-DDOS ignored flows                                  12267
App-DDOS first path failed                              0
App-DDOS first path succeeded                           459439
App-DDOS dropped packets                                0
App-DDOS processed packets                              449118
App-DDOS connection table process succeeded             459439
App-DDOS connection table process failed                0
App-DDOS context process succeeded                      449118
App-DDOS context process failed                         0
App-DDOS ignore context                                 0
App-DDOS context values excluded                        0
App-DDOS context value process succeeded                449118
App-DDOS context value process failed                   0
App-DDOS context value prune failed                     0
App-DDOS no action                                      275996
App-DDOS drop connection action                         0
App-DDOS drop packet action                             0
App-DDOS close server action                            0
App-DDOS IP Action block                                0
App-DDOS IP Action close                                0
App-DDOS IP Action notify                               275996
App-DDOS logs sent                                      238
App-DDOS logs report failed                             0
```


Copyright © 2013, Juniper Networks, Inc.

## show security idp counters application-identification

**Syntax** show security idp counters application-identification

**Release Information** Command introduced in Release 9.2 of Junos OS. Updated in Release 12.1 of Junos OS.

**Description** Display the status of all IDP application identification (AI) counter values.

**Required Privilege Level** view

**Related Documentation**
- clear security idp counters application-identification on page 1437
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

**List of Sample Output** show security idp counters application-identification on page 2018

**Output Fields** Table 156 on page 2017 lists the output fields for the **show security idp counters application-identification** command. Output fields are listed in the approximate order in which they appear.

### Table 156: show security idp counters application-identification Output Fields

| Field Name | Field Description |
|---|---|
| **AI matches** | Number of sessions with an AI signature match. |
| **AI no-matches** | Number of sessions with no AI signature match. |
| **AI-enabled sessions** | Number of sessions with AI enabled. |
| **AI-disabled sessions** | Number of sessions with AI disabled. |
| **AI-disabled sessions due to ssl encapsulated flows** | Number of sessions with AI disabled due to SSL encapsulated flows. |
| **AI-disabled sessions due to cache hit** | Number of sessions with AI disabled due to a cache match. |
| **AI-disabled sessions due to configuration** | Number of sessions with AI disabled because the configured session limit was reached. |
| **AI-disabled sessions due to protocol remapping** | Number of sessions with AI disabled due to protocol remapping. |
| **AI-disabled sessions due to RPC match** | Number of sessions with AI disabled due to an RPC match. |
| **AI-disabled sessions due to non-TCP/UDP flows** | Number of sessions with AI disabled due to non-TCP or non-UDP flows. |

Copyright © 2013, Juniper Networks, Inc.

Table 156: show security idp counters application-identification Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **AI-disabled sessions due to session limit** | Number of sessions with AI disabled because the maximum session limit was reached. |
| **AI-disabled sessions due to session packet memory limit** | Number of sessions with AI disabled because the memory usage limit per session was reached. |
| **AI-disabled sessions due to global packet memory limit** | Number of sessions with AI disabled because the global memory usage limit was reached. |
| **Packets cloned for AI** | Number of packets cloned for application identification. |
| **Policy update** | Number of times the IDP policy has been updated. |

## Sample Output

### show security idp counters application-identification

```
user@host> show security idp counters application-identification
IDP counters:
IDP counter type                                                Value
 AI matches                                                       4
 AI no-matches                                                    0
 AI-enabled sessions                                              4
 AI-disabled sessions                                             0
 AI-disabled sessions due to gate match                           0
 AI-disabled sessions due to ssl encapsulated flows               0
 AI-disabled sessions due to cache hit                            0
 AI-disabled sessions due to configuration                        0
 AI-disabled sessions due to protocol remapping                   0
 AI-disabled sessions due to RPC match                            0
 AI-disabled sessions due to non-TCP/UDP flows                    0
 AI-disabled sessions due to session limit                        0
 AI-disabled sessions due to session packet memory limit          0
 AI-disabled sessions due to global packet memory limit           0
 Packets cloned for AI                                           12
 Policy update                                                    0
```


Copyright © 2013, Juniper Networks, Inc.

## show security idp counters dfa

**Syntax** show security idp counters dfa

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Display the status of all DFA counter values.

**Required Privilege Level** view

**Related Documentation**
- clear security idp counters dfa on page 1438
- IDP Policies for Security Devices

**List of Sample Output** show security idp counters dfa on page 2019

**Output Fields** Table 157 on page 2019 lists the output fields for the **show security idp counters dfa** command. Output fields are listed in the approximate order in which they appear.

### Table 157: show security idp counters dfa Output Fields

| Field Name | Field Description |
|---|---|
| DFA Group Merged Usage | Number of DFA groups merged. |
| DFA Matches | Number of DFA matches found. |

### Sample Output

show security idp counters dfa

```
user@host> show security idp counters dfa
IDP counters:
IDP counter type                                                Value
 DFA Group Merged Usage                                             0
 DFA Matches                                                        1
```

Copyright © 2013, Juniper Networks, Inc.

## show security idp counters flow

**Syntax** show security idp counters flow

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Display the status of all IDP flow counter values.

**Required Privilege Level** view

**Related Documentation**
- flow (Security IDP) on page 597
- clear security idp counters flow on page 1439
- IDP Policies for Security Devices

**List of Sample Output** show security idp counters flow on page 2022

**Output Fields** Table 158 on page 2020 lists the output fields for the **show security idp counters flow** command. Output fields are listed in the approximate order in which they appear.

### Table 158: show security idp counters flow Output Fields

| Field Name | Field Description |
|---|---|
| **Fast-path packets** | Number of packets that are set through fast path after completing idp policy lookup. |
| **Slow-path packets** | Number of packet that are sent through slow path during idp policy lookup. |
| **ICMP-error packets**<br>(Unsupported) | Number of ICMP error packets. |
| **Session construction failed**<br>(Unsupported) | Number of times the packet failed to establish the session. |
| **Session limit reached** | Number of sessions that reached idp sessions limit. |
| **Not a new session**<br>(Unsupported) | Number of session that extended from its time limit. |
| **Invalide index at age-out**<br>(Unsupported) | Invalid session index in session age-out message. |
| **Packet logging** | Number of packets saved for packet logging. |
| **Busy packets**<br>(Unsupported) | Number of packets saved as the one or more packets of this session are handed off for async processing. |


Copyright © 2013, Juniper Networks, Inc.

Table 158: show security idp counters flow Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Policy cache hits** | Number of sessions that matched policy cache. |
| **Policy cache misses** | Number of sessions that did not match policy cache. |
| **Maximum flow hash collisions** | Maximum number of packets of one flow that share the same hash value. |
| **Bad-UDP-checksumpackets**<br>(Unsupported) | Number of packets that received with bad UDP checksum error. |
| **Gates added** | Number of gate entries added for dynamic port identification. |
| **Gate matches**<br>(Unsupported) | Number of times a gate is matched. |
| **Sessions deleted** | Number of sessions deleted. |
| **Sessions aged-out**<br>(Unsupported) | Number of sessions are aged out if no traffic is received within session timeout value. |
| **Sessions in-use while aged-out**<br>(Unsupported) | Number of sessions in use during session age-out. |
| **TCP flows marked dead on RST/FIN** | Number of session marked dead on TCP RST/FIN. |
| **Sessions constructed** | Number of sessions established. |
| **Sessions destructed** | Number of sessions destructed. |
| **SM Session Create** | Number of SM sessions created. |
| **SM Packet Process** | Number of packets processed from SM. |
| **SM Session close** | Number of SM sessions closed. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security idp counters flow

```
user@host> show security idp counters flow
IDP counters:
 IDP counter type                                  Value
 Fast-path packets                                     0
 Slow-path packets                                     1
 ICMP-error packets                                    0
 Session construction failed                           0
 Session limit reached                                 0
 Not a new session                                     0
 Invalide index at ageout                              0
 Packet logging                                        0
 Busy packets                                          0
 Policy cache hits                                     0
 Policy cache misses                                   1
 Maximum flow hash collisions                          0
 Flow hash collisions                                  0
 Bad-UDP-checksum packets                              0
 Gates added                                           0
 Gate matches                                          0
 Sessions deleted                                      1
 Sessions aged-out                                     0
 Sessoins in-use while aged-out                        0
 TCP flows marked dead on RST/FIN                      1
 Sessions constructed                                  1
 Sessions destructed                                   1
 SM Session Create                                     1
 SM Packet Process                                    28
 SM Session close                                      1
```


Copyright © 2013, Juniper Networks, Inc.

## show security idp counters http-decoder

**Syntax** show security idp counters http-decoder

**Release Information** Command introduced in Release 11.2 of Junos OS.

**Description** Display the status of all HTTP decoders.

**Required Privilege Level** view

**Related Documentation**
- clear security idp counters http-decoder on page 1440
- IDP Policies for Security Devices

**List of Sample Output** show security idp counters http-decoder on page 2023

**Output Fields** Table 159 on page 2023 lists the output fields for the **show security idp counters http-decoder** command. Output fields are listed in the approximate order in which they appear.

### Table 159: show security idp counters http-decoder Output Fields

| Field Name | Field Description |
|---|---|
| **No of file decoder requests from MIME over HTTP** | Number of active file decoder requests sent over HTTP from MIME. |
| **No of pending file decoder requests from MIME over HTTP** | Number of pending file decoder requests sent over HTTP from MIME. |
| **No of completed file decoder requests from MIME over HTTP** | Number of completed file decoder requests sent over HTTP from MIME. |
| **No of unrecognized file type from MIME over HTTP** | Number of unrecognized file types sent over HTTP from MIME. |
| **No of compressed payload transferred over HTTP** | Number of compressed files transferred over HTTP from MIME. |

## Sample Output

**show security idp counters http-decoder**

```
user@host> show security idp counters http-decoder
IDP counters:
IDP counter type                                                  Value
No of file decoder requests from MIME over HTTP                       0
No of pending file decoder requests from MIME over HTTP               0
No of completed file decoder requests from MIME over HTTP             0
No of unrecognized file type from MIME over HTTP                      0
No of compressed payload transferred over HTTP                        0
```

Copyright © 2013, Juniper Networks, Inc.

## show security idp counters ips

**Syntax** show security idp counters ips

**Release Information** Command modified in Release 11.2 of Junos OS.

**Description** Display the status of all IPS counter values.

**Required Privilege Level** view

**Related Documentation**

- ips on page 698
- clear security idp counters ips on page 1441
- IDP Policies for Security Devices

**List of Sample Output** show security idp counters ips on page 2026

**Output Fields** Table 160 on page 2024 lists the output fields for the **show security idp counters ips** command. Output fields are listed in the approximate order in which they appear.

### Table 160: show security idp counters ips Output Fields

| Field Name | Field Description |
|---|---|
| **TCP fast path** | Number of TCP packets skipped for IDS processing. |
| **Layer-4 anomalies** | Number of Layer-4 protocol error or anomaly. |
| **Anomaly hash misses** | Number of times look failed on anomaly hash. |
| **Line context matches** | Number of attempts to match line based attacks in traffic stream. |
| **Stream256 context matches** | Number of attempts to match stream based attacks in first 256 bytes of traffic stream. |
| **Stream context matches** | Number of attempts to match stream based attacks in traffic stream. |
| **Packet context matches** | Number of attempts to match packet based attacks in traffic packet. |
| **Packet header matches** | Number of attempts to match packet header based attacks in traffic packet. |
| **Context matches** | Number of attempts to match protocol context based attacks in traffic stream. |
| **Regular expression matches** | Number of attempts to match PCRE expressions in traffic stream. |
| **Tail DFAs** | Number of attempts to match an attack on tail DFA group matches. |
| **Exempted attacks** | Number of attacks exempted from match as per exempt rulebase. |
| **Out of order chains** | Number of times attack is excluded from match due to member attacks in an attack group did not complete chain. |


Copyright © 2013, Juniper Networks, Inc.

Table 160: show security idp counters ips Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Partial chain matches** | Number of attacks in partial chain match with attack scope as transaction. |
| **IDS device FIFO size** | Number of IDS contexts in virtual IDS device. |
| **IDS device FIFO overflows** | Number of times an IDS context can not be written as the IDS device is full. |
| **Brute force queue size** | Number of entries in the brute force queue. |
| **IDS cache hits**<br>(Unsupported) | Number of sessions those found attack instance in IDS cache. |
| **IDS cache misses**<br>(Unsupported) | Number of sessions those did not find attack instance in IDS cache. |
| **Shellcode detection invocations** | Number of times shell code match is attempted. |
| **Wrong offsets** | Number of times attack's offset is not within the service offset range. |
| **No peer MAC**<br>(Unsupported) | Number of times flow peer MAC address is not available. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security idp counters ips

```
user@host> show security idp counters ips
IDP counters:
 IDP counter type                                                Value
 TCP fast path                                                      15
 Layer-4 anomalies                                                   0
 Anomaly hash misses                                                 3
 Line context matches                                                5
 Stream256 context matches                                           5
 Stream context matches                                              5
 Packet context matches                                              0
 Packet header matches                                               0
 Context matches                                                    12
 Regular expression matches                                          0
 Tail DFAs                                                           0
 Exempted attacks                                                    0
 Out of order chains                                                 0
 Partial chain matches                                               0
 IDS device FIFO size                                                0
 IDS device FIFO overflows                                           0
 Brute force queue size                                              0
 IDS cache hits                                                      0
 IDS cache misses                                                    0
 Shellcode detection invocations                                     0
 Wrong offsets                                                       0
 No peer MAC                                                         0
 Content-decompression memory usage in KB                            0
 Content-decompression memory over limit                             0
 Content-decompression gunzip called                                 0
 Content-decompression gunzip failed                                 0
 Content-decompression others called                                 0
 Content-decompression others failed                                 0
 Content-decompression input bytes                                   0
 Content-decompression output bytes                                  0
 Content-decompression ratio over limit                              0
 Content-decompression type mismatch                                 0
```


Copyright © 2013, Juniper Networks, Inc.

## show security idp counters log

**Syntax** show security idp counters log

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Display the status of all IDP log counter values.

**Required Privilege Level** view

**Related Documentation**
- event-rate on page 566
- clear security idp counters log
- IDP Policies for Security Devices

**List of Sample Output** show security idp counters log on page 2029

**Output Fields** Table 161 on page 2027 lists the output fields for the **show security idp counters log** command. Output fields are listed in the approximate order in which they appear.

### Table 161: show security idp counters log Output Fields

| Field Name | Field Description |
|---|---|
| **Logs dropped** | Number of logs that are dropped. |
| **Suppressed log count** | Number of logs that are suppressed. |
| **Logs waiting for post-window packets** (Unsupported) | Number of logs waiting for post-window packets. |
| **Logs ready to be sent** (Unsupported) | Number of logs ready to be sent. |
| **Logs in suppression list** (Unsupported) | Number of logs considered for suppression list. |
| **Log timers created** | Number of times the log timer is created. |
| **Logs timers expired** | Number of times the log timer is expired. |
| **Log timers cancelled** | Number of times the log timer is canceled. |
| **Logs ready to be sent high watermark** (Unsupported) | Number of packets that are ready to be sent with high degree watermark. |

Copyright © 2013, Juniper Networks, Inc.

Table 161: show security idp counters log Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Log receive buffer full**<br>(Unsupported) | Number of times the buffer is full. |
| **Packet log too big**<br>(Unsupported) | Number of packet logs that exceeded allowed packet log size. |
| **Reads per second**<br>(Unsupported) | Number of packets that are read per second. |
| **Logs in read buffer high watermark**<br>(Unsupported) | Number of high watermark packets that are in read buffer. |
| **Packets logged** | Number of packets that are logged, |
| **Packets lost**<br>(Unsupported) | Number of packets that are failed to log. |
| **Packets copied**<br>(Unsupported) | Number of packets copied during packet log. |
| **Packets held**<br>(Unsupported) | Number of packets held for packet log. |
| **Packets released** | Number of packets that are released from hold. |
| **IP Action Messages**<br>(Unsupported) | Number of IP action messages. |
| **IP Action Drops**<br>(Unsupported) | Number of IP action messages dropped. |
| **IP Action Exists**<br>(Unsupported) | Number of exits during IP action creation. |
| **NWaits**<br>(Unsupported) | Number of logs waiting for post window packets. |
| **Match vectors** | Number of attacks in IDS match vector. |
| **Supercedes** | Number of attacks in supercede vector. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security idp counters log

```
user@host> show security idp counters log
IDP counters:
 IDP counter type                                                Value
 Logs dropped                                                        0
 Suppressed log count                                                0
 Logs waiting for post-window packets                                0
 Logs ready to be sent                                               0
 Logs in suppression list                                            0
 Log timers created                                                  0
 Logs timers expired                                                 0
 Log timers cancelled                                                0
 Logs ready to be sent high watermark                                0
 Log receive buffer full                                             0
 Packet log too big                                                  0
 Reads per second                                                    1
 Logs in read buffer high watermark                                  0
 Log Bytes in read buffer high watermark                             0
 Packets logged                                                      0
 Packets lost                                                        0
 Packets copied                                                      0
 Packets held                                                        0
 Packets released                                                    0
 IP Action Messages                                                  0
 IP Action Drops                                                     0
 IP Action Exists                                                    0
 NWaits                                                              0
 Match vectors                                                       0
 Supercedes                                                          0
 Kpacket too big                                                     0
```

Copyright © 2013, Juniper Networks, Inc.

## show security idp counters packet

**Syntax** show security idp counters packet

**Release Information** Command introduced in Release 9.2 of Junos OS. **Dropped by IDP policy** and **Dropped by Error** added in Release 10.1 of Junos OS.

**Description** Display the status of all IDP packet counter values.

**Required Privilege Level** view

**Related Documentation**
- clear security idp counters packet on page 1443
- IDP Policies for Security Devices

**List of Sample Output** show security idp counters packet on page 2032

**Output Fields** Table 162 on page 2030 lists the output fields for the **show security idp counters packet** command. Output fields are listed in the approximate order in which they appear.

Table 162: show security idp counters packet Output Fields

| Field Name | Field Description |
|---|---|
| **Processed packets** | Number of packets processed by the IDP service. |
| **Dropped packets** | Number of packets dropped by the IDP service. |
| **Dropped by IDP policy** | Number of packets dropped by the IDP policy. |
| **Dropped by Error** | Number of packets dropped by error. |
| **Dropped sessions**<br>(Unsupported) | Number of sessions dropped. |
| **Bad IP headers** | Number of packets that fail IP header length validity check. |
| **Packets with IP options** | Number of packets that contain the optional header fields. |
| **Decapsulated packets** | Number of packets that are decapsulated. |
| **GRE decapsulations**<br>(Unsupported) | Number of packets that are generic routing encapsulation (GRE) decapsulated. |
| **PPP decapsulations**<br>(Unsupported) | Number of packets that are Point-to-Point Protocol (PPP) decapsulated. |


Copyright © 2013, Juniper Networks, Inc.

Table 162: show security idp counters packet Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **GTP decapsulations**<br><br>(Unsupported) | Number of packets that are GPRS tunneling protocol (GTP) decapsulated. |
| **GTP flows**<br><br>(Unsupported) | Number of GTP flows. |
| **TCP decompression uncompressed IP**<br><br>(Unsupported) | Number of uncompressed IP headers that are to be TCP decompressed. |
| **TCP decompression compressed IP**<br><br>(Unsupported) | Number of compressed IP headers that are to be TCP decompressed. |
| **Deferred-send packets**<br><br>(Unsupported) | Number of deferred IP packets that are sent out. |
| **IP-in-IP packets**<br><br>(Unsupported) | Number of packets that are IP-in-IP encapsulated. |
| **TTL errors**<br><br>(Unsupported) | Number of packets with TTL error in the header. |
| **Routing loops**<br><br>(Unsupported) | Number of packets that continue to be routed in an endless circle due to an inconsistent routing state. |
| **No-route packets**<br><br>(Unsupported) | Number of packets that could not be routed further. |
| **Flood IP**<br><br>(Unsupported) | Number of packets that are identified as IP flood packets. |
| **Invalid ethernet headers**<br><br>(Unsupported) | Number of packets that are identified with an invalid Ethernet header. |
| **Packets attached** | Number of packets attached. |
| **Packets cloned** | Number of packets that are cloned. |
| **Packets allocated** | Number of packets allocated. |
| **Packets destructed** | Number of packets destructed. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security idp counters packet

```
user@host> show security idp counters packet
IDP counters:
 IDP counter type                                                Value
 Processed packets                                                  27
 Dropped packets                                                     0
 Dropped by IDP policy                                               0
 Dropped by error                                                    0
 Dropped sessions                                                    0
 Bad IP headers                                                      0
 Packets with IP options                                             0
 Decapsulated packets                                                0
 GRE decapsulations                                                  0
 PPP decapsulations                                                  0
 GTP decapsulations                                                  0
 GTP flows                                                           0
 TCP decompression uncompressed IP                                   0
 TCP decompression compressed IP                                     0
 Deferred-send packets                                               0
 IP-in-IP packets                                                    0
 TTL errors                                                          0
 Routing loops                                                       0
 STP drops                                                           0
 No-route packets                                                    0
 Flood IP                                                            0
 Invalid ethernet headers                                            0
 Packets attached                                                   28
 Packets cloned                                                     28
 Packets allocated                                                   0
 Packets destructed                                                 55
```


Copyright © 2013, Juniper Networks, Inc.

## show security idp counters packet-log

**Syntax** show security idp counters packet-log

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display the values of all IDP packet-log counters.

**Required Privilege Level** view

**Related Documentation**
- IDP Policies for Security Devices

**Output Fields** The following table lists the output fields for the **show security idp counters packet-log** command. Output fields are listed in the approximate order in which they appear.

| Field Name | Field Description |
|---|---|
| **Total packets captured since packet capture was activated** | Number of packets captured by the device by the IDP service. |
| **Total sessions enabled since packet capture was activated** | Number of sessions that have performed packet capture since the capture facility was activated. |
| **Sessions currently enabled for packet capture** | Number of sessions that are actively capturing packets at this time. |
| **Packets currently captured for enabled sessions** | Number of packets that have been captured by active sessions. |
| **Packet clone failures** | Number of packet capture failures due to cloning error. |
| **Session log object failures** | Number of objects containing log messages generated during packet capture that were not successfully transmitted to the host. |
| **Session packet log object failures** | Number of objects containing captured packets that were not successfully transmitted to the host. |
| **Sessions skipped because session limit exceeded** | Number of sessions that could not initiate packet capture because the maximum number of sessions specified for the device were conducting captures at that time. |
| **Packets skipped because packet limit exceeded** | Number of packets not captured because the packet limit specified for this device was reached. |
| **Packets skipped because total memory limit exceeded** | Number of packets not captured because the memory allocated for packet capture on this device was exceeded. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security idp counters packet-log

```
user@host> show security idp counters packet-log
IDP counters:                                                   Value
 Total packets captured since packet capture was activated          0
 Total sessions enabled since packet capture was activated          0
 Sessions currently enabled for packet capture                      0
 Packets currently captured for enabled sessions                    0
 Packet clone failures                                              0
 Session log object failures                                        0
 Session packet log object failures                                 0
 Sessions skipped because session limit exceeded                    0
 Packets skipped because packet limit exceeded                      0
 Packets skipped because total memory limit exceeded                0
```


Copyright © 2013, Juniper Networks, Inc.

## show security idp counters policy-manager

**Syntax** show security idp counters policy-manager

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Display the status of all IDP policies counter values.

**Required Privilege Level** view

**Related Documentation**
- clear security idp counters policy-manager on page 1444
- IDP Policies for Security Devices

**List of Sample Output** show security idp counters policy-manager on page 2035

**Output Fields** Table 163 on page 2035 lists the output fields for the **show security idp counters policy-manager** command. Output fields are listed in the approximate order in which they appear.

Table 163: show security idp counters policy-manager Output Fields

| Field Name | Field Description |
|---|---|
| **Number of policies** | Number of policies installed. |
| **Number of aged out policies** | Number of IDP policies that are expired. |

### Sample Output

show security idp counters policy-manager

```
user@host> show security idp counters policy-manager
IDP counters:
 IDP counter type                                    Value
 Number of policies                                      0
 Number of aged out policies                             0
```

Copyright © 2013, Juniper Networks, Inc.

## show security idp counters tcp-reassembler

**Syntax** show security idp counters tcp-reassembler

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Display the status of all TCP reassembler counter values.

**Required Privilege Level** view

**Related Documentation**
- re-assembler on page 873
- clear security idp counters tcp-reassembler on page 1445
- IDP Policies for Security Devices

**List of Sample Output** show security idp counters tcp-reassembler on page 2038

**Output Fields** Table 164 on page 2036 lists the output fields for the **show security idp counters tcp-reassembler** command. Output fields are listed in the approximate order in which they appear.

### Table 164: show security idp counters tcp-reassembler Output Fields

| Field Name | Field Description |
|---|---|
| **Bad TCP checksums**<br>(Unsupported) | Number of packets that have incorrect TCP checksums. |
| **Bad TCP headers** | Number of bad TCP headers detected. |
| **Slow path segments** | Number of segments that are sent through the slow path if the TCP segment does not pass fast-path segment validation. |
| **Fast path segments** | Number of segments that are sent through the fast path after passing a predefined TCP validation sequence. |
| **Sequence number wrap around errors** | Number of packets that wrap around of the sequence number. |
| **Session reuses** | Number of sessions that reused an already established TCP session. |
| **SYN retransmissions** | Number of SYN packets that are retransmitted. |
| **Bad three way handshake acknowledgements** | Number of packets that have incorrect three-way handshake acknowledgements (ACK packet). |
| **Sequence number out of sync flows** | Number of packets that have out-of-sync sequence numbers. |
| **Fast path pattern matches in queued up streams** | Number of queued packets that have fast path pattern match. |


Copyright © 2013, Juniper Networks, Inc.

Table 164: show security idp counters tcp-reassembler Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **New segments with no overlaps with old segment** | Number of new segments that do not overlap with old segment. |
| **New segment overlaps with beginning of old segment** | Number of new segments that overlap with beginning of old segment. |
| **New segment overlaps completely with old segment** | Number of new segments that overlap completely with old segment. |
| **New segment is contained in old segment** | Number of new segments contained in old segment. |
| **New segment overlaps with end of old segment** | Number of new segments that overlap with the end of old segment. |
| **New segment begins after end of old segment** | Number of new segments that overlap after the end of old segment. |
| **Memory consumed by new segment** | Memory that is consumed by the new segment. |
| **Segments in memory** | Number of segments that are stored in memory for processing. |
| **Per-flow memory overflows** | Number of segments dropped after reaching per flow memory limit. |
| **Global memory overflows** | Number of segments dropped after reaching reassembler global memory limit. |
| **Overflow drops** | Number of packets that are dropped due to memory overflow. |
| **Copied packets**<br>(Unsupported) | Number of packets copied in reassembler. |
| **Closed Acks** | Number of Ack packets seen without having seen SYN on the same session. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security idp counters tcp-reassembler

```
user@host> show security idp counters tcp-reassembler
IDP counters:
 IDP counter type                                                Value
 Bad TCP checksums                                                   0
 Bad TCP headers                                                     0
 Slow path segments                                                  4
 Fast path segments                                                 23
 Sequence number wrap around errors                                  0
 Session reuses                                                      0
 SYN retransmissions                                                 0
 Bad three way handshake acknowledgements                            0
 Sequence number out of sync flows                                   0
 Fast path pattern matches in queued up streams                      0
 New segments with no overlaps with old segment                      0
 New segment overlaps with beginning of old segment                  0
 New segment overlaps completely with old segment                    0
 New segment is contained in old segment                             0
 New segment overlaps with end of old segment                        0
 New segment begins after end of old segment                         0
 Memory consumed by new segment                                      0
 Segments in memory                                                  0
 Per-flow memory overflows                                           0
 Global memory overflows                                             0
 Overflow drops                                                      0
 Copied packets                                                      0
 Closed Acks                                                         0
```


Copyright © 2013, Juniper Networks, Inc.

## show security idp logical-system policy-association

**Syntax** show security idp logical-system policy-association

**Release Information** Command introduced in Release 11.3 of Junos OS.

**Description** Display the IDP policy assigned to a logical system. The IDP policy is assigned to a logical system through the security profile.

**Required Privilege Level** view

**Related Documentation**
- security-profile on page 1278
- IDP Policies for Security Devices
- Master Administrator for Logical Systems on Security Devices

**List of Sample Output** show security idp logical-system policy-association on page 2039

**Output Fields** Table 165 on page 2039 lists the output fields for the **show security idp logical-system policy-association** command.

Table 165: show security idp logical-system policy-association Output Fields

| Field Name | Field Description |
|---|---|
| **Logical system** | Name of the logical system to which an IDP policy is assigned. |
| **IDP policy** | Name of the IDP policy that is specified in the security profile that is bound to the logical system. |

### Sample Output

show security idp logical-system policy-association

```
user@host> show security idp logical-system policy-association
Logical system          IDP policy
root-logical-system     idp-policy1
lsys1                   idp-policy2
```

Copyright © 2013, Juniper Networks, Inc.

## show security idp memory

**Syntax** show security idp memory

**Release Information** Command introduced in Release 9.2 of Junos OS. Percentage outputs added in Release 10.1 of Junos OS.

**Description** Display the status of all IDP data plane memory.

**Required Privilege Level** view

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

**List of Sample Output** show security idp memory on page 2040

**Output Fields** Table 166 on page 2040 lists the output fields for the **show security idp memory** command. Output fields are listed in the approximate order in which they appear.

### Table 166: show security idp memory Output Fields

| Field Name | Field Description |
|---|---|
| **PIC** | Name of the PIC. |
| **Total IDP data plane memory** | Total memory space that is allocated for the IDP data plane.<br>NOTE: IDP requires a minimum of 5 MB of memory for session inspection. |
| **Used** | Used memory space in the data plane. |
| **Available** | Available memory space in the data plane. |

## Sample Output

**show security idp memory**

```
user@host> show security idp memory
    IDP data plane memory statistics:
                              PIC : FPC 0 PIC 0:
  Total IDP data plane memory : 196 MB
                         Used : 8 MB ( 8192 KB ) ( 4.08% )
                    Available : 188 MB ( 192512 KB ) (95.91%)
```


Copyright © 2013, Juniper Networks, Inc.

## show security idp policies

**Syntax** show security idp policies

**Release Information** Command introduced in Release 10.1 of Junos OS.

**Description** Display the list of currently installed policies.

**Required Privilege Level** view

**Related Documentation**

- show security idp active-policy on page 2007
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices
- IDP Class of Service Action for Security Devices

**Output Fields** user@host> show security idp policies

### Sample Output

```
Subscriber:  s0,        Installed policies:  1

  ID     Name    Sessions    Memory    detector

  0      new1      0         10179       9.2.160090324
```

Copyright © 2013, Juniper Networks, Inc.

## show security idp policy-commit-status

**Syntax** show security idp policy-commit-status

**Release Information** Command introduced in Release 10.4 of JUNOS OS.

**Description** Display the IDP policy commit status. For example, status of policy compilation or load.

**Required Privilege Level** view

**Related Documentation**

- show security idp status on page 2051
- show security idp policy-commit-status clear on page 2043
- IDP Policies for Security Devices

### Sample Output

```
user@host> show security idp policy-commit-status
Reading prereq sensor config...
```


Copyright © 2013, Juniper Networks, Inc.

## show security idp policy-commit-status clear

**Syntax** show security idp policy-commit-status clear

**Release Information** Command introduced in Release 10.4 of JUNOS OS.

**Description** Clear the IDP policy commit status.

**Required Privilege Level** clear

**Related Documentation**
- show security idp policy-commit-status on page 2042
- IDP Policies for Security Devices

**Output Fields** This command produces no output.

Copyright © 2013, Juniper Networks, Inc.

## show security idp policy-templates

**Syntax** show security idp policy-templates

**Release Information** Command introduced in Release 10.1 of Junos OS.

**Description** Display the list of available policy templates.

**Required Privilege Level** view

**Related Documentation**
- show security idp active-policy on page 2007
- IDP Policies for Security Devices

**Output Fields** user@host> show security idp policy-templates

### Sample Output

```
DMZ_Services
DNS_Service
File_Server
Getting_Started
IDP_Default
Recommended
Web_Server
```


Copyright © 2013, Juniper Networks, Inc.

## show security idp predefined-attacks

**Syntax** show security idp predefined-attacks
filters ( category | severity | direction)

**Release Information** Command introduced in Release 10.1 of Junos OS.

**Description** Display information about predefined attacks using optional filters.

**Options** filters (Optional)

- **category**—Show predefined attacks in different categories.
- **severity**—Show predefined attacks based on different severities.
  - **critical**
  - **info**
  - **major**
  - **minor**
  - **warning**
- **direction** — Show predefined attacks for different directions.
  - **any**
  - **client-to-server**
  - **exclude-any**
  - **exclude-client-to-server**
  - **exclude-server-to-client**
  - **server-to-client**

**Required Privilege Level** view

**Related Documentation**
- IDP Policies for Security Devices
- IDP Application Identification for Security Devices

**Output Fields** **user@host> show security idp predefined-attacks filters category APP**

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

```
APP:AMANDA:AMANDA-ROOT-OF1
APP:AMANDA:AMANDA-ROOT-OF2
APP:ARKEIA:TYPE-77-OF
APP:CA:ALERT-SRV-OF
APP:CA:ARCSRV:TCP-BOF
APP:CA:ARCSRV:UA-OF
APP:CA:IGATEWAY-BOF
APP:CA:LIC-COMMAND-OF
APP:CA:LIC-GCR-OF
APP:CA:LIC-GETCONFIG-OF
APP:CA:LIC-GETCONFIG-OF2
APP:CA:LIC-PUTOLF-OF
APP:CDE-DTSPCD-OF
APP:DOUBLETAKE
APP:ETHEREAL:DISTCC-OF
APP:HPOVNNM:HPOVTRACE-OF
APP:KERBEROS:GSS-ZERO-TOKEN
APP:KERBEROS:KBR-DOS-TCP-2
APP:MDAEMON:FORM2RAW-OF
APP:MERCURY-BOF
APP:MISC:MCAFFEE-SRV-HDR
APP:NTOP-WEB-FS1
APP:PPTP:MICROSOFT-PPTP
APP:REMOTE:TIMBUKTU-AUTH-OF
```

**user@host> show security idp security-package predefined-attacks filters category FTP severity critical direction client-to-server**

```
FTP:COMMAND:WZ-SITE-EXEC
FTP:DIRECTORY:TILDE-ROOT
FTP:EXPLOIT:OPENFTPD-MSG-FS
FTP:OVERFLOW:OPENBSD-FTPD-GLOB
FTP:OVERFLOW:PATH-LINUX-X86-3
FTP:OVERFLOW:WFTPD-MKD-OVERFLOW
FTP:OVERFLOW:WUBSD-SE-RACE
FTP:PROFTP:OVERFLOW1
FTP:PROFTP:PPC-FS2
FTP:SERVU:CHMOD-OVERFLOW
FTP:SERVU:LIST-OVERFLOW
FTP:SERVU:MDTM-OVERFLOW
FTP:WU-FTP:IREPLY-FS
```


Copyright © 2013, Juniper Networks, Inc.

## show security idp security-package-version

**Syntax** show security idp security-package-version

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Display information of the currently installed security package version and detector version.

**Required Privilege Level** view

**Related Documentation**
- IDP Policies for Security Devices
- IDP Signature Database for Security Devices
- security-package on page 922
- request security idp security-package download on page 1502
- request security idp security-package install on page 1504

**List of Sample Output** show security idp security-package-version on page 2047

**Output Fields** Table 167 on page 2047 lists the output fields for the **show security idp security-package-version** command. Output fields are listed in the approximate order in which they appear.

### Table 167: show security idp security-package-version Output Fields

| Field Name | Field Description |
|---|---|
| **Attack database version** | Attack database version number that are currently installed on the system. |
| **Detector version** | Detector version number that are currently installed on the system. |
| **Policy template version** | Policy template version that are currently installed on the system. |

## Sample Output

show security idp security-package-version

```
user@host> show security idp security-package-version
  Attack database version:1154(Mon Apr 28 15:08:42 2008)
  Detector version :9.1.140080400
  Policy template version :7
```

Copyright © 2013, Juniper Networks, Inc.

## show security idp ssl-inspection key

**Syntax** **show security idp ssl-inspection key** [*<key-name>* **[server** *<server-ip>***]]**

**Release Information** Command introduced in Release 9.3 of Junos OS.

**Description** Display SSL keys added to the system along with their associated server IP addresses.

**Options**
- ***key-name*** —(Optional) Name of SSL private key.
- **server** ***server-ip*** —(Optional) Server IP address associated for specified key.

**Required Privilege Level** view

**Related Documentation**
- IDP Policies for Security Devices

**List of Sample Output**
show security idp ssl-inspection key on page 2049
show security idp ssl-inspection key key2 on page 2049

**Output Fields** Table 168 on page 2048 lists the output fields for the **show security idp ssl-inspection key** command. Output fields are listed in the approximate order in which they appear.

### Table 168: show security idp ssl-inspection key Output Fields

| Field Name | Field Description |
|---|---|
| **Total SSL keys** | Total number of SSL keys. |
| **key** | Name of the SSL private key. |
| **server** | Server IP address associated with the SSL keys. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security idp ssl-inspection key

```
user@host> show security idp ssl-inspection key
Total SSL keys : 4

SSL Server key and ip address:

  Key : key1, server : 1.1.0.1
  Key : key1, server : 1.1.0.2
  Key : key2, server : 2.2.0.1
  key : key3
```

## Sample Output

show security idp ssl-inspection key key2

```
user@host> show security idp ssl-inspection key key2
SSL Server key and ip address:

  Key : key2, server : 2.2.0.1
```

Copyright © 2013, Juniper Networks, Inc.

## show security idp ssl-inspection session-id-cache

**Syntax** show security idp ssl-inspection session-id-cache

**Release Information** Command introduced in Release 9.3 of Junos OS.

**Description** Display all the SSL session IDs in the session ID cache. Each cache entry is 32 bytes long.

**Required Privilege Level** view

**Related Documentation**
- clear security idp ssl-inspection session-id-cache on page 1446
- IDP Policies for Security Devices

**List of Sample Output** show security idp ssl-inspection session-id-cache on page 2050

**Output Fields** Table 169 on page 2050 lists the output fields for the **show security idp ssl-inspection session-id-cache** command. Output fields are listed in the approximate order in which they appear.

Table 169: show security idp ssl-inspection session-id-cache Output Fields

| Field Name | Field Description |
|---|---|
| **Total SSL session identifiers** | Total number of SSL session identifiers stored in the session ID cache. |

### Sample Output

show security idp ssl-inspection session-id-cache

```
user@host> show security idp ssl-inspection session-id-cache
SSL session identifiers :

c98396c768f983b515d93bb7c421fb6b8ce5c2c5c230b8739b7fcf8ce9c0de4e
a211321a3242233243c3dc0d421fb6b8ce5e4e983b515d932c5c230b87392c

Total SSL session identifiers : 2
```


Copyright © 2013, Juniper Networks, Inc.

## show security idp status

**Syntax** show security idp status

**Release Information** Command introduced in Release 9.2 of Junos OS. Multiple detector information introduced in Release 10.1 of Junos OS. Output changed to support IDP dedicated mode in Release 11.2 of Junos OS.

**Description** Display the status of the current IDP policy.

**Required Privilege Level** view

**Related Documentation**
- IDP Policies for Security Devices

**List of Sample Output** show security idp status on page 2052

**Output Fields** Table 170 on page 2051 lists the output fields for the **show security idp status** command. Output fields are listed in the approximate order in which they appear.

### Table 170: show security idp status Output Fields

| Field Name | Field Description |
|---|---|
| **State of IDP** | Status of current IDP policy. |
| **Packets/second** | The aggregated throughput (packets per second) for the system. |
| **KBits/second** | The aggregated throughput (kbits per second) for the system. |
| **Latency** | • min—Minimum delay for a packet to receive and return by a node in microseconds.<br>• max—Maximum delay for a packet to receive and return by a node in microseconds.<br>• ave—Average delay for a packet to receive and return by a node in microseconds. |
| **Packet Statistics** | Statistics for ICMP, TCP, and UDP packets. |
| **Flow Statistics** | Flow-related system statistics for ICMP, TCP, and UDP packets. |
| **Session Statistics** | Session-related system statistics for ICMP, TCP, and UDP packets. |
| **Number of SSL Sessions** | Number of current SSL sessions. |
| **Policy Name** | Name of the running policy. If IDP is configured for logical systems, **idp-policy-combined** is displayed. |
| **Running Detector Version** | Current version of the running detector. |
| **Forwarding process mode** | IDP dedicated mode: **default**, **equal**, **idp**, or **firewall**. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security idp status

```
user@host> show security idp status
State of IDP: 2-default,  Up since: 2010-02-04 13:37:16 UTC (17:15:02 ago)

Packets/second: 5               Peak: 11 @ 2010-02-05 06:51:58 UTC
KBits/second  : 2               Peak: 5 @ 2010-02-05 06:52:06 UTC
Latency (microseconds): [min: 0] [max: 0] [avg: 0]

Packet Statistics:
[ICMP: 0] [TCP: 82] [UDP: 0] [Other: 0]

Flow Statistics:
  ICMP: [Current: 0] [Max: 0 @ 2010-02-05 06:49:51 UTC]
  TCP: [Current: 2] [Max: 6 @ 2010-02-05 06:52:08 UTC]
  UDP: [Current: 0] [Max: 0 @ 2010-02-05 06:49:51 UTC]
  Other: [Current: 0] [Max: 0 @ 2010-02-05 06:49:51 UTC]

Session Statistics:
[ICMP: 0] [TCP: 1] [UDP: 0] [Other: 0]

Policy Name : sample
Running Detector Version : 10.4.160091104
```


Copyright © 2013, Juniper Networks, Inc.

## show security idp status detail

**Syntax** show security idp status detail

**Release Information** Command introduced in Release 10.1 of Junos OS. Output changed to support IDP dedicated mode in Release 11.2 of Junos OS.

**Description** Display statistics for each Services Processing Unit (SPU), including multiple detector information for each SPU.

**Required Privilege Level** view

**Related Documentation**

- IDP Policies for Security Devices

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security idp status detail

```
user@host> show security idp status detail
  PIC : FPC 1 PIC 1:
State of IDP: Default,  Up since: 2011-03-29 17:25:07 UTC (00:02:48 ago)

Packets/second: 0               Peak: 0 @ 2011-03-29 17:25:07 UTC
KBits/second  : 0               Peak: 0 @ 2011-03-29 17:25:07 UTC
Latency (microseconds): [min: 0] [max: 0] [avg: 0]


Packet Statistics:
[ICMP: 0] [TCP: 0] [UDP: 0] [Other: 0]

Flow Statistics:
  ICMP: [Current: 0] [Max: 0 @ 2011-03-29 17:25:07 UTC]
  TCP: [Current: 0] [Max: 0 @ 2011-03-29 17:25:07 UTC]
  UDP: [Current: 0] [Max: 0 @ 2011-03-29 17:25:07 UTC]
  Other: [Current: 0] [Max: 0 @ 2011-03-29 17:25:07 UTC]

Session Statistics:
 [ICMP: 0] [TCP: 0] [UDP: 0] [Other: 0]

Number of SSL Sessions : 0

 PIC : FPC 1 PIC 0:

State of IDP: Default,  Up since: 2011-03-29 17:25:08 UTC (00:02:47 ago)

Packets/second: 0               Peak: 0 @ 2011-03-29 17:25:08 UTC
KBits/second  : 0               Peak: 0 @ 2011-03-29 17:25:08 UTC
Latency (microseconds): [min: 0] [max: 0] [avg: 0]

Packet Statistics:
 [ICMP: 0] [TCP: 0] [UDP: 0] [Other: 0]

Flow Statistics:
  ICMP: [Current: 0] [Max: 0 @ 2011-03-29 17:25:08 UTC]
  TCP: [Current: 0] [Max: 0 @ 2011-03-29 17:25:08 UTC]
  UDP: [Current: 0] [Max: 0 @ 2011-03-29 17:25:08 UTC]
  Other: [Current: 0] [Max: 0 @ 2011-03-29 17:25:08 UTC]

Session Statistics:
 [ICMP: 0] [TCP: 0] [UDP: 0] [Other: 0]

Number of SSL Sessions : 0

 PIC : FPC 0 PIC 1:

State of IDP: Default,  Up since: 2011-03-29 17:25:04 UTC (00:02:51 ago)


Packets/second: 0               Peak: 0 @ 2011-03-29 17:25:04 UTC
KBits/second  : 0               Peak: 0 @ 2011-03-29 17:25:04 UTC
Latency (microseconds): [min: 0] [max: 0] [avg: 0]

Packet Statistics:
 [ICMP: 0] [TCP: 0] [UDP: 0] [Other: 0]

Flow Statistics:
```


Copyright © 2013, Juniper Networks, Inc.

```
  ICMP: [Current: 0] [Max: 0 @ 2011-03-29 17:25:04 UTC]
  TCP: [Current: 0] [Max: 0 @ 2011-03-29 17:25:04 UTC]
  UDP: [Current: 0] [Max: 0 @ 2011-03-29 17:25:04 UTC]
  Other: [Current: 0] [Max: 0 @ 2011-03-29 17:25:04 UTC]

Session Statistics:
 [ICMP: 0] [TCP: 0] [UDP: 0] [Other: 0]


Number of SSL Sessions : 0

  PIC : FPC 1 PIC 1:

  Policy Name : none

  PIC : FPC 1 PIC 0:

  Policy Name : none

  PIC : FPC 0 PIC 1:

  Policy Name : none

Forwarding process mode : maximizing sessions  firewall
```

## show security ike active-peer

**Syntax** show security ike active-peer

**Release Information** Command introduced in Release 10.4 of Junos OS.

**Description** This command is used to display the list of connected active users with details about the peer addresses and ports they are using.

**Required Privilege Level** view

**List of Sample Output** show security ike active-peer on page 2056

### Sample Output

show security ike active-peer

```
user@host> show security ike active-peer

Remote Address   Port     Peer IKE-ID        XAUTH username   Assigned IP
172.27.6.136     8034     tleungjtac@650a     tleung          10.123.80.225
```


Copyright © 2013, Juniper Networks, Inc.

## show security ike debug-status

**Syntax** **show security ike debug-status**

**Release Information** Command introduced in Release 11.4R3 of Junos OS.

**Description** Display debug information for currently enabled Internet Key Exchange (IKE).

**Required Privilege Level** view

**Related Documentation**
- request security ike debug-disable on page 1511
- request security ike debug-enable on page 1512

**List of Sample Output** show security ike debug-status on page 2057

### Sample Output

show security ike debug-status

```
user@host> show security ike debug-status
Enabled
flag: all
level: 15
```

## show security ike pre-shared-key

**Syntax** **show security ike pre-shared key**
**<master-key** ***master-key*** **>**
**<user-id** ***user-id*** **>**

**Release Information** Command introduced in Release 8.5 of Junos OS.

**Description** Display the Internet Key Exchange (IKE) preshared key used by the Virtual Private network (VPN) gateway to authenticate the remote access user.

**Options**
- **master-key** ***master-key*** —(Optional) Master preshared key.
- **user-id** ***user-id*** —(Optional) IKE user ID value.

**Required Privilege Level** view

**Related Documentation**
- pre-shared-key (Security IKE Policy) on page 831

**List of Sample Output** show security ike pre-shared-key on page 2058

### Sample Output

show security ike pre-shared-key

```
user@host> show security ike pre-shared-key user-id a@juniper.net master-key juniper
Preshared Key:3b33ec3631a561ec5a710f5d02f208033b108bb4
```


Copyright © 2013, Juniper Networks, Inc.

## show security ike security-associations

**Syntax**

**show security ike security-associations**
*peer-address*
brief | detail
fpc *slot-number*
index *SA-index-number*
kmd-instance (all | *kmd-instance-name*)
pic *slot-number*
family (inet | inet6)

**Release Information**

Command introduced in Release 8.5 of Junos OS. The **fpc**, **pic**, and **kmd-instance** options added in Release 9.3 of Junos OS. The **family** option added in Release 11.1 of Junos OS.

**Description**

Display information about Internet Key Exchange security associations (IKE SAs).

**Options**

- none—Display standard information about existing IKE SAs, including index numbers.
- ***peer-address***—(Optional) Display details about a particular SA based on the IPv4 or IPv6 address of the destination peer. This option and **index** provide the same level of output.
- **brief**—(Optional) Display standard information about all existing IKE SAs. (Default)
- **detail**—(Optional) Display detailed information about all existing IKE SAs.
- **fpc *slot-number***—(Optional) Specific to SRX Series devices. Display information about existing IKE SAs in this Flexible PIC Concentrator (FPC) slot. This option is used to filter the output.
- **index *SA-index-number***—(Optional) Display information for a particular SA based on the index number of the SA. For a particular SA, display the list of existing SAs by using the command with no options. This option and ***peer-address*** provide the same level of output.
- **kmd-instance** —(Optional) Specific to SRX Series devices. Display information about existing IKE SAs in the key management process (in this case, it is KMD) identified by FPC *slot-number* and PIC *slot-number*. This option is used to filter the output.
  - **all**—All KMD instances running on the Services Processing Unit (SPU).
  - ***kmd-instance-name***—Name of the KMD instance running on the SPU.
- **pic *slot-number*** —(Optional) Specific to SRX Series devices. Display information about existing IKE SAs in this PIC slot. This option is used to filter the output.
- **family**—(Optional) Display IKE SAs by family. This option is used to filter the output.
  - **inet**—IPv4 address family.
  - **inet6**—IPv6 address family.

**Required Privilege Level**

view

Copyright © 2013, Juniper Networks, Inc.

**Related Documentation**

- clear security ike security-associations on page 1448
- VPN for Security Devices
- Master Administrator for Logical Systems on Security Devices

**List of Sample Output**

show security ike security-associations (IPv4) on page 2063
show security ike security-associations (IPv6) on page 2063
show security ike security-associations detail (Branch SRX Series Devices) on page 2063
show security ike security-associations detail (For High-End SRX Series Devices) on page 2063
show security ike security-associations family inet6 on page 2064
show security ike security-associations index 8 detail on page 2064
show security ike security-associations 1.1.1.2 on page 2065
show security ike security-associations fpc 6 pic 1 kmd-instance all (SRX Series Devices) on page 2065

**Output Fields**

Table 171 on page 2060 lists the output fields for the **show security ike security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 171: show security ike security-associations Output Fields

| Field Name | Field Description |
|---|---|
| **IKE Peer or Remote Address** | IP address of the destination peer with which the local peer communicates. |
| **Index** | Index number of an SA. This number is an internally generated number you can use to display information about a single SA. |
| **Gateway Name** | Name of the IKE gateway. |
| **Location** | • **FPC**—Flexible PIC Concentrator (FPC) slot number.<br>• **PIC**—PIC slot number.<br>• **KMD-Instance**—The name of the KMD instance running on the SPU, identified by FPC *slot-number* and PIC *slot-number*. Currently, 4 KMD instances are running on each SPU, and any particular IKE negotiation is carried out by a single KMD instance. |
| **Role** | Part played in the IKE session. The device triggering the IKE negotiation is the initiator, and the device accepting the first IKE exchange packets is the responder. |
| **State** | State of the IKE SAs:<br>• **DOWN**—SA has not been negotiated with the peer.<br>• **UP**—SA has been negotiated with the peer. |
| **Initiator cookie** | Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered. |
| **Responder cookie** | Random number generated by the remote node and sent back to the initiator as a verification that the packets were received.<br><br>A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity. |


Copyright © 2013, Juniper Networks, Inc.

Table 171: show security ike security-associations Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Mode or Exchange type** | Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between one another. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are:<br>• **main**—The exchange is done with six messages. This mode or exchange type encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate.<br>• **aggressive**—The exchange is done with three messages. This mode or exchange type does not encrypt the payload, leaving the identity of the neighbor unprotected.<br>NOTE: IKEv2 protocol does not use the mode configuration for negotiation. Therefore, mode displays the version number of the security association. |
| **Local** | Address of the local peer. |
| **Remote** | Address of the remote peer. |
| **Lifetime** | Number of seconds remaining until the IKE SA expires. |
| **Algorithms** | IKE algorithms used to encrypt and secure exchanges between the peers during the IPsec Phase 2 process:<br>• **Authentication**—Type of authentication algorithm used:<br>  ◦ **sha1**—Secure Hash Algorithm 1 authentication.<br>  ◦ **md5**—MD5 authentication.<br>• **Encryption**—Type of encryption algorithm used:<br>  ◦ **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption.<br>  ◦ **aes-192-cbc**— AES192-bit encryption.<br>  ◦ **aes-128-cbc**—AES 128-bit encryption.<br>  ◦ **3des-cbc**—3 Data Encryption Standard (DES) encryption.<br>  ◦ **des-cbc**—DES encryption. |
| **Diffie-Hellman group** | Specifies the IKE Diffie-Hellman group. |
| **Traffic statistics** | • **Input bytes**—Number of bytes received.<br>• **Output bytes**—Number of bytes transmitted.<br>• **Input packets**—Number of packets received.<br>• **Output packets**—Number of packets transmitted. |

Copyright © 2013, Juniper Networks, Inc.

Table 171: show security ike security-associations Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Flags** | Notification to the key management process of the status of the IKE negotiation:<br>• **caller notification sent**—Caller program notified about the completion of the IKE negotiation.<br>• **waiting for done**—Negotiation is done. The library is waiting for the remote end retransmission timers to expire.<br>• **waiting for remove**—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation.<br>• **waiting for policy manager**—Negotiation is waiting for a response from the policy manager. |
| **IPSec security associations** | • ***number* created:** The number of SAs created.<br>• ***number* deleted**: The number of SAs deleted. |
| **Phase 2 negotiations in progress** | Number of Phase 2 IKE negotiations in progress and status information:<br>• **Negotiation type**—Type of Phase 2 negotiation. Junos OS currently supports quick mode.<br>• **Message ID**—Unique identifier for a Phase 2 negotiation.<br>• **Local identity**—Identity of the local Phase 2 negotiation. The format is *id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation)*.<br>• **Remote identity**—Identity of the remote Phase 2 negotiation. The format is *id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation)*.<br>• **Flags**—Notification to the key management process of the status of the IKE negotiation:<br>  ◦ **caller notification sent**—Caller program notified about the completion of the IKE negotiation.<br>  ◦ **waiting for done**—Negotiation is done. The library is waiting for the remote end retransmission timers to expire.<br>  ◦ **waiting for remove**—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation.<br>  ◦ **waiting for policy manager**—Negotiation is waiting for a response from the policy manager. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security ike security-associations (IPv4)

```
user@host> show security ike security-associations
Index  Remote Address    State  Initiator cookie     Responder cookie     Mode
8  1.1.1.2    UP  3a895f8a9f620198     9040753e66d700bb     Main
Index  Remote Address    State  Initiator cookie     Responder cookie     Mode
9  1.2.1.3     UP  5ba96hfa9f65067   1  70890755b65b80b   d  Main
```

## Sample Output

show security ike security-associations (IPv6)

```
user@host> show security ike security-associations
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address

5       UP     e48efd6a444853cf  0d09c59aafb720be  Aggressive     1212::1112
```

## Sample Output

show security ike security-associations detail (Branch SRX Series Devices)

```
user@host> show security ike security-associations detail
IKE peer 25.191.134.245, Index 2577565, Gateway Name: tropic
  Role: Initiator, State: UP
  Initiator cookie: b869b3424513340a, Responder cookie: 4cb3488cb19397c3
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 25.191.134.241:500, Remote: 25.191.134.245:500
  Lifetime: Expires in 169 seconds
  Peer ike-id: 25.191.134.245
  Xauth assigned IP: 0.0.0.0
  Algorithms:
   Authentication        : hmac-sha1-96
   Encryption            : aes128-cbc
   Pseudo random function: hmac-sha1
  Diffie-Hellman group  : DH-group-5
  Traffic statistics:
   Input  bytes  :                 1012
   Output bytes  :                 1196
   Input  packets:                    4
   Output packets:                    5
  Flags: IKE SA is created
  IPSec security associations: 1 created, 0 deleted
  Phase 2 negotiations in progress: 0

    Negotiation type: Quick mode, Role: Initiator, Message ID: 0
    Local: 25.191.134.241:500, Remote: 25.191.134.245:500
    Local identity: 25.191.134.241
    Remote identity: 25.191.134.245
    Flags: IKE SA is created
```

## Sample Output

show security ike security-associations

```
user@host> show security ike security-associations detail
IKE peer 1.1.1.2, Index 914039858, Gateway Name: tropic
  Location: FPC 3, PIC 1, KMD-Instance 3
```

Copyright © 2013, Juniper Networks, Inc.

detail (For High-End SRX Series Devices)

```
  Role: Initiator, State: UP
  Initiator cookie: 219a697652bdde37, Responder cookie: b49c30b229d36bcd
  Exchange type: Aggressive, Authentication method: Pre-shared-keys
  Local: 1.1.1.1:500, Remote: 1.1.1.2:500
  Lifetime: Expires in 26297 seconds
  Peer ike-id: 1.1.1.2
  Xauth user-name: not available
  Xauth assigned IP: 0.0.0.0
  Algorithms:
   Authentication        : hmac-sha1-96
   Encryption            : 3des-cbc
   Pseudo random function: hmac-sha1
  Diffie-Hellman group  : DH-group-5
  Traffic statistics:
   Input  bytes  :                   0
   Output bytes  :                   0
   Input  packets:                   0
   Output packets:                   0
  IPSec security associations: 0 created, 0 deleted
  Phase 2 negotiations in progress: 1
```

## Sample Output

show security ike security-associations family inet6

```
user@host> show security ike security-associations family inet6
  IKE peer 1212::1112, Index 5, Gateway Name: tropic
  Role: Initiator, State: UP
  Initiator cookie: e48efd6a444853cf, Responder cookie: 0d09c59aafb720be
  Exchange type: Aggressive, Authentication method: Pre-shared-keys
  Local: 1212::1111:500, Remote: 1212::1112:500
  Lifetime: Expires in 19518 seconds
  Peer ike-id: not valid
  Xauth assigned IP: 0.0.0.0
  Algorithms:
   Authentication        : sha1
   Encryption            : 3des-cbc
   Pseudo random function: hmac-sha1
   Diffie-Hellman group  : DH-group-5
  Traffic statistics:
   Input  bytes  :                1568
   Output bytes  :                2748
   Input  packets:                   6
   Output packets:                  23
  Flags: Caller notification sent
  IPSec security associations: 5 created, 0 deleted
  Phase 2 negotiations in progress: 1

    Negotiation type: Quick mode, Role: Initiator, Message ID: 2900338624
    Local: 1212::1111:500, Remote: 1212::1112:500
    Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
    Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
    Flags: Caller notification sent, Waiting for done
```

## Sample Output

show security ike security-associations index 8 detail

```
user@host> show security ike security-associations index 8 detail
IKE peer 1.1.1.2, Index 8, Gateway Name: tropic
 Role: Responder, State:UP
 Initiator cookie: 3a895f8a9f620198, Responder cookie: 9040753e66d700bb
 Exchange type; main, Authentication method: Pre-shared-keys
 Local: 1.1.1.1:500, Remote: 1.1.1.2:500
```


Copyright © 2013, Juniper Networks, Inc.

```
Lifetime: Expired in 381 seconds
Algorithms:
 Authentication:       md5
 Encryption:      3des-cbc
 Pseudo random function      hmac-md5
    Diffie-Hellman group  : DH-group-5
   Traffic statistics:
 Input bytes:       11268
 Output bytes:        6940
 Input packets:        57
 Output packets:        57
Flags: Caller notification sent
IPsec security associations: 0 created, 0 deleted
Phase 2 negotiations in progress: 1

 Negotiation type: Quick mode, Role: Responder, Message ID: 1765792815
 Local: 1.1.1.1:500, Remote: 1.1.1.2:500
 Local identity: No Id
 Remote identity: No Id
 Flags: Caller notification sent, Waiting for remove
```

## Sample Output

show security ike security-associations 1.1.1.2

```
user@host> show security ike security-associations 1.1.1.2
Index     State  Initiator cookie  Responder cookie  Mode Remote Address
   8        UP     3a895f8a9f620198  9040753e66d700bb  Main 1.1.1.2
```

## Sample Output

show security ike security-associations fpc 6 pic 1 kmd-instance all (SRX Series Devices)

```
user@host> show security ike security-associations fpc 6 pic 1 kmd-instance all
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode

1728053250 1.1.1.2      UP     fc959afd1070d10b  bdeb7e8c1ea99483  Main
```

Copyright © 2013, Juniper Networks, Inc.

## show security ike tunnel-map

**Syntax** **show security ike tunnel-map <brief | summary>**

**Release Information** Command introduced in Junos OS Release 12.1x44-D10.

**Description** Display the tunnel mapping on different Services Processing Units (SPUs).

**Options**
- **brief | summary** —(Optional) Display the specified level of output.

**Required Privilege Level** view

**List of Sample Output**
show security ike tunnel-map on page 2066
show security ike tunnel-map summary on page 2066

### Sample Output

show security ike tunnel-map

```
user@host> show security ike tunnel-map
node0:
Gateway ID   Gateway Name FPC  PIC  IKED Instance
    2        ike_gw1       4    0       1
    3        ike_gw2       7    0       1
    4        ike_gw3       7    0       2
    5        ike_gw4       4    0       2
```

show security ike tunnel-map summary

```
user@host> show security ike tunnel-map summary
node0:
FPC  PIC  SPU Load
 4    0      2
 7    0      2
```


Copyright © 2013, Juniper Networks, Inc.

## show security ipsec inactive-tunnels

**Syntax** **show security ipsec inactive-tunnels**
brief | detail
family (inet | inet6)
fpc *slot-number*
index *index-number*
kmd-instance (all | *kmd-instance-name*)
pic *slot-number*
vpn-name *vpn-name*

**Release Information** Command introduced in Release 11.4R3 of Junos OS.

**Description** Display security information about the inactive tunnel.

**Options**

- none—Display information about all inactive tunnels.
- **brief** | **detail**—(Optional) Display the specified level of output.
- **family**—(Optional) Display the inactive tunnel by family. This option is used to filter the output.
  - **inet**—IPv4 address family.
  - **inet6**—IPv6 address family.
- **fpc** ***slot-number***—(Optional) Specific to SRX Series devices. Display information about inactive tunnels in the Flexible PIC Concentrator (FPC) slot.
- **index** ***index-number***—(Optional) Display detailed information about the specified inactive tunnel identified by this index number. For a list of all inactive tunnels with their index numbers, use the command with no options.
- **kmd-instance** —(Optional) Specific to SRX Series devices. Display information about inactive tunnels in the key management process (in this case, it is KMD) identified by FPC *slot-number* and PIC *slot-number*.
  - **all**—All KMD instances running on the Services Processing Unit (SPU).
  - ***kmd-instance-name***—Name of the KMD instance running on the SPU.
- **pic** ***slot-number***—Specific to SRX Series devices. Display information about inactive tunnels in the PIC slot.
- **vpn-name** ***vpn-name***—(Optional) Name of the VPN.



NOTE: The **fpc** ***slot-number***, **kmd-instance (all | *kmd-instance-name*)**, and **pic** ***slot-number*** parameters apply to SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices only.

Copyright © 2013, Juniper Networks, Inc.

**Required Privilege Level** view

**Related Documentation**
- show security ipsec security-associations in the *CLI Reference*

**List of Sample Output**
show security ipsec inactive-tunnels on page 2069
show security ipsec inactive-tunnels index 131073 on page 2069

**Output Fields** Table 172 on page 2068 lists the output fields for the **show security ipsec inactive-tunnels** command. Output fields are listed in the approximate order in which they appear.

### Table 172: show security ipsec inactive-tunnels Output Fields

| Field Name | Field Description |
|---|---|
| **Total inactive tunnels** | Total number of inactive IPsec tunnels. |
| **Total inactive tunnels which establish immediately** | Total number of inactive IPsec tunnels that can establish a session immediately. |
| **ID** | Identification number of the inactive tunnel. You can use this number to get more information about the inactive tunnel. |
| **Gateway** | IP address of the remote gateway. |
| **Port** | If Network Address Translation (NAT) is used, this value is 4500. Otherwise, it is the standard IKE port, 500. |
| **Nego#** | Number of IPsec negotiations. |
| **Fail#** | Number of IPsec negotiation failures. |
| **Def-Del#** | Number of deferred deletions of a dial-up IPsec VPN. |
| **Flag** | Internal flag depicting the state of the tunnel, used for debugging purposes. |
| **Virtual system** | Virtual system to which the VPN belongs. |
| **VPN name** | Name of the IPsec VPN. |
| **Local gateway** | Gateway address of the local system. |
| **Remote gateway** | Gateway address of the remote system. |
| **Local identity** | Identity of the local peer so that its partner destination gateway can communicate with it. The value is specified as an IP address, fully qualified domain name, e-mail address, or distinguished name (DN). |
| **Remote identity** | IP address of the destination peer gateway. |
| **Version** | Version of IKE. |


Copyright © 2013, Juniper Networks, Inc.

Table 172: show security ipsec inactive-tunnels Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **DF-bit** | State of the don't fragment bit: **set** or **clear**. |
| **Bind-interface** | The tunnel interface to which the route-based VPN is bound. |
| **Policy-name** | Name of the applicable policy. |
| **Tunnel Down Reason** | Reason for which the tunnel is inactive. |

## Sample Output

### show security ipsec inactive-tunnels

```
user@host> show security ipsec inactive-tunnels
Total inactive tunnels: 5
  Total inactive tunnels with establish immediately: 1
  ID     Port  Nego#  Fail#  Flag      Gateway          Tunnel Down Reason
  2      500   0      0      604829                     SA not initiated
  3      500   0      0      600829    12.2.3.110       SA not initiated
  131073 500   419    0      600a29    12.2.2.110       P1 SA deleted
  131074 500   0      0      600a29    12.2.2.110       SA not initiated
  131075 500   0      0      600a29    12.2.4.110       SA not initiated
```

## Sample Output

### show security ipsec inactive-tunnels index 131073

```
user@host> show security ipsec inactive-tunnels index 131073
ID: 131073 Virtual-system: root, VPN Name: tropic
  Local Gateway: 12.2.2.109, Remote Gateway: 12.2.2.110
  Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote Identity: ipv4_subnet(any:0,[0..7]=30.1.1.0/24)
  Version: IKEv1
    DF-bit: clear
    Bind-interface: st0.3

  Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 600a29
  Tunnel Down Reason: SA not initiated
```

Copyright © 2013, Juniper Networks, Inc.

## show security ipsec next-hop-tunnels

**Syntax** **show security ipsec next-hop-tunnels**
**< interface-name** ***interface-name*** **>**

**Release Information** Command introduced in Release 8.5 of Junos OS.

**Description** Display security information about the secure tunnel interface.

**Options**
- none—Display information about all secure tunnel interface.
- **interface-name** ***interface-name*** —(Optional) Name of the secure tunnel logical interface.

**Required Privilege Level** view

**List of Sample Output** show security ipsec next-hop-tunnels on page 2070

**Output Fields** Table 173 on page 2070 lists the output fields for the **show security ipsec next-hop-tunnels** command. Output fields are listed in the approximate order in which they appear.

### Table 173: show security ipsec next-hop-tunnels Output Fields

| Field Name | Field Description |
|---|---|
| **Next-hop gateway** | IP address of the next gateway. |
| **Interface** | Name of the secure tunnel logical interface. |
| **IPsec VPN name** | Name of the IPsec VPN tunnel. |
| **Flag** | • **Static**—IP address manually configured.<br>• **Auto**—IP address obtained from the remote peer automatically. |

## Sample Output

### show security ipsec next-hop-tunnels

```
user@host> show security ipsec next-hop-tunnels
Next-hop gateway  interface   IPsec VPN name                 Flag
11.1.1.2          st0.0       autokey                        Static
11.1.1.3          st0.0       pbd-4-6                        Auto
```


Copyright © 2013, Juniper Networks, Inc.

## show security ipsec security-associations

**Syntax**

**show security ipsec security-associations**
brief | detail
fpc *slot-number*
index *SA-index-number*
kmd-instance (all | *kmd-instance-name*)
pic *slot-number>*
family (inet | inet6)
vpn-name *vpn-name*

**Release Information**

Command introduced in Release 8.5 of Junos OS. The **fpc**, **pic**, and **kmd-instance** options added in Release 9.3 of Junos OS. The **family** option added in Release 11.1 of Junos OS. The **vpn-name** option added in Release 11.4R3 of Junos OS.

**Description**

Display information about the IPsec security associations (SAs).

**Options**

- none—Display information about all SAs.
- **brief** | **detail**—(Optional) Display the specified level of output.
- **fpc** ***slot-number***—(Optional) Specific to SRX Series devices. Display information about existing IPsec SAs in this Flexible PIC Concentrator (FPC) slot. This option is used to filter the output.
- **index** ***SA-index-number***—(Optional) Display detailed information about the specified SA identified by this index number. To obtain a list of all SAs that includes their index numbers, use the command with no options.
- **kmd-instance**—(Optional) Specific to SRX Series devices. Display information about existing IPsec SAs in the key management process (in this case, it is KMD) identified by the FPC *slot-number* and PIC *slot-number*. This option is used to filter the output.
  - **all**—All KMD instances running on the Services Processing Unit (SPU).
  - ***kmd-instance-name***—Name of the KMD instance running on the SPU.
- **pic** ***slot-number***—(Optional) Specific to SRX Series devices. Display information about existing IPsec SAs in this PIC slot. This option is used to filter the output.
  - **family**—(Optional) Display SAs by family. This option is used to filter the output.
    - **inet**—IPv4 address family.
    - **inet6**—IPv6 address family.
- **vpn-name** ***vpn-name***—Name of the VPN.

**Required Privilege Level**

view

**Related Documentation**

- MPLS for Security Devices
- clear security ipsec security-associations on page 1450

Copyright © 2013, Juniper Networks, Inc.

- VPN for Security Devices
- Master Administrator for Logical Systems on Security Devices

**List of Sample Output**

show security ipsec security-associations (IPv4) on page 2075
show security ipsec security-associations (IPv6) on page 2075
show security ipsec security-associations index 5 on page 2075
show security ipsec security-associations brief on page 2075
show security ipsec security-associations detail on page 2076
show security ipsec security-associations detail (SRX Series Devices) on page 2076
show security ipsec security-associations family inet6 on page 2077
show security ipsec security-associations fpc 6 pic 1 kmd-instance all (SRX Series Devices) on page 2077

**Output Fields**

Table 174 on page 2072 lists the output fields for the **show security ipsec security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 174: show security ipsec security-associations

| Field Name | Field Description |
|---|---|
| **Total active tunnels** | Total number of active IPsec tunnels. |
| **ID** | Index number of the SA. You can use this number to get additional information about the SA. |
| **VPN name** | IPsec name for VPN. |
| **Gateway** | IP address of the remote gateway. |
| **Port** | If Network Address Translation (NAT) is used, this value is 4500. Otherwise, it is the standard IKE port, 500. |
| **Algorithm** | Cryptography used to secure exchanges between peers during the IKE Phase 2 negotiations includes:<br>• An authentication algorithm used to authenticate exchanges between the peers. Options are **hmac-md5-95**, **hmac-sha1-96,** or **ESP**.<br>• An encryption algorithm used to encrypt data traffic. Options are **3des-cbc, aes-128-cbc, aes-192-cbc**, **aes-256-cbc**, or **des-cbc.** |
| **SPI** | Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI. Each entry includes the name of the VPN, the remote gateway address, the SPIs for each direction, the encryption and authentication algorithms, and keys. The peer gateways each have two SAs, one resulting from each of the two phases of negotiation: Phase 1 and Phase 2. |
| **Life: sec/kb** | The lifetime of the SA, after which it expires, expressed either in seconds or kilobytes. |


Copyright © 2013, Juniper Networks, Inc.

Table 174: show security ipsec security-associations *(continued)*

| Field Name | Field Description |
|---|---|
| **Sta** | State has two options, **Installed** and **Not Installed**.<br>• **Installed**—The SA is installed in the SA database.<br>• **Not Installed**—The SA is not installed in the SA database.<br>For transport mode, the value of State is always **Installed**. |
| **Mon** | The Mon field refers to VPN monitoring status. If VPN monitoring is enabled, then this field displays **U** (up) or **D** (down). A hyphen (-) means VPN monitoring is not enabled for this SA. |
| **vsys or Virtual-system** | The root system. |
| **Tunnel index** | Numeric identifier of the specific IPsec tunnel for the SA. |
| **Local gateway** | Gateway address of the local system. |
| **Remote gateway** | Gateway address of the remote system. |
| **Local identity** | Identity of the local peer so that its partner destination gateway can communicate with it. The value is specified as an IP address, fully qualified domain name, e-mail address, or distinguished name (DN). |
| **Remote identity** | IP address of the destination peer gateway. |
| **DF-bit** | State of the don't fragment bit: **set** or **cleared**. |
| **Bind interface** | The tunnel interface to which VPN is bound. |
| **Policy-name** | Name of the applicable policy. |
| **Location** | **FPC**—Flexible PIC Concentrator (FPC) slot number.<br>**PIC**—PIC slot number.<br>**KMD-Instance**—The name of the KMD instance running on the SPU, identified by FPC *slot-number* and PIC *slot-number*. Currently, 4 KMD instances running on each SPU, and any particular IPsec negotiation is carried out by a single KMD instance. |
| **Direction** | Direction of the SA; it can be inbound or outbound. |
| **AUX-SPI** | Value of the auxiliary security parameter index(SPI).<br>• When the value is **AH** or **ESP**, **AUX-SPI** is always 0.<br>• When the value is **AH+ESP**, **AUX-SPI** is always a positive integer. |
| **Mode** | Mode of the SA:<br>• **transport**—Protects host-to-host connections.<br>• **tunnel—**Protects connections between security gateways. |

Copyright © 2013, Juniper Networks, Inc.

Table 174: show security ipsec security-associations *(continued)*

| Field Name | Field Description |
|---|---|
| **Type** | Type of the SA:<br>• **manual**—Security parameters require no negotiation. They are static and are configured by the user.<br>• **dynamic**—Security parameters are negotiated by the IKE protocol. Dynamic SAs are not supported in transport mode. |
| **State** | State of the SA:<br>• **Installed**—The SA is installed in the SA database.<br>• **Not Installed**—The SA is not installed in the SA database.<br>For transport mode, the value of State is always **Installed**. |
| **Protocol** | Protocol supported.<br>• Transport mode supports Encapsulation Security Protocol (ESP) and Authentication Header (AH).<br>• Tunnel mode supports ESP and AH.<br>  ◦ **Authentication**—Type of authentication used.<br>  ◦ **Encryption**—Type of encryption used. |
| **Soft lifetime** | The soft lifetime informs the IPsec key management system that the SA is about to expire.<br>Each lifetime of an SA has two display options, hard and soft, one of which must be present for a dynamic SA. This allows the key management system to negotiate a new SA before the hard lifetime expires.<br>• **Expires in seconds**—Number of seconds left until the SA expires. |
| **Hard lifetime** | The hard lifetime specifies the lifetime of the SA.<br>• **Expires in seconds**—Number of seconds left until the SA expires. |
| **Lifesize Remaining** | The lifesize remaining specifies the usage limits in kilobytes. If there is no lifesize specified, it shows unlimited.<br>• **Expires in kilobytes**—Number of kilobytes left until the SA expires. |
| **Anti-replay service** | State of the service that prevents packets from being replayed. It can be **Enabled** or **Disabled**. |
| **Replay window size** | Configured size of the antireplay service window. It can be 32 or 64 packets. If the replay window size is 0, the antireplay service is disabled.<br>The antireplay window size protects the receiver against replay attacks by rejecting old or duplicate packets. |
| **Bind-interface** | The tunnel interface to which the route-based VPN is bound. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security ipsec security-associations (IPv4)

```
user@host> show security ipsec security-associations
Total active tunnels: 1
ID    Gateway          Port  Algorithm       SPI      Life:sec/kb  Mon vsys
  131075 11.0.28.241    500   ESP:3des/sha1   86758ff0 6918/ unlim   -   0
  131075 11.0.28.241    500   ESP:3des/sha1   3183ff26 6918/ unlim   -   0
```

## Sample Output

show security ipsec security-associations (IPv6)

```
user@host> show security ipsec security-associations
Total active tunnels: 1
ID    Algorithm       SPI      Life:sec/kb  Mon vsys Port  Gateway
  131074 ESP:3des/sha1 14caf1d9 3597/ unlim   -   root 500   1212::1112
  131074 ESP:3des/sha1 9a4db486 3597/ unlim   -   root 500   1212::1112
```

## Sample Output

show security ipsec security-associations index 5

```
user@host> show security ipsec security-associations index 5
ID: 131073 Virtual-system: root, VPN Name: tropic
Local gateway: 1.1.1.1, Remote gateway: 1.1.1.2
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0...7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear
Bind-interface: st0.3
Policy-name: my-policy

Direction: inbound, SPI: 494001027, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expired
Hard lifetime: Expired in 130 seconds
Lifesize Remaining: Unlimited
Anti-replay service: Enabled, Replay window size: 64

Direction: inbound, SPI: 1498711950, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 40 seconds
Hard lifetime: Expires in 175 seconds
Lifesize Remaining: Unlimited
Anti-replay service: Enabled, Replay window size: 64

Direction: outbound, SPI: 4038397695, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 40 seconds
Hard lifetime: Expires in 175 seconds
Lifesize Remaining: Unlimited
Anti-replay service: Enabled, Replay window size: 64
```

## Sample Output

Copyright © 2013, Juniper Networks, Inc.

show security ipsec security-associations brief

```
user@host> show security ipsec security-associations brief
Total active tunnels: 2
ID Gateway Port Algorithm SPI Life:sec/kb Mon vsys
<16384 1.1.1.1 500 ESP:3des/sha1 af88baa 28795/unlim D 0
>16384 1.1.1.1 500 ESP:3des/sha1 f4e3e5f4 28795/unlim D 0
```

## Sample Output

show security ipsec security-associations detail

```
user@host> show security ipsec security-associations detail
ID: 131073 Virtual-system: root, VPN Name: tropic
Local Gateway: 1.1.1.2, Remote Gateway: 1.1.1.1
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear
Bind-interface: st0.3
Direction: inbound, SPI: 184060842, AUX-SPI: 0
Hard lifetime: Expires in 28785 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expired
Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: DOWN
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Anti-replay service: enabled, Replay window size: 32

Direction: outbound, SPI: 4108576244, AUX-SPI: 0
Hard lifetime: Expires in 28785 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expired
Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: DOWN
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Anti-replay service: enabled, Replay window size: 32
```

## Sample Output

show security ipsec security-associations

```
user@host> show security ipsec security-associations detail
ID: 131073 Virtual-system: root, VPN Name: tropic
  Local Gateway: 20.0.0.4, Remote Gateway: 30.0.0.2
```


Copyright © 2013, Juniper Networks, Inc.

detail (SRX Series Devices)

```
  Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote Identity: ipv4(any:0,[0..3]=20.0.0.4)
    Version: IKEv2
    DF-bit: clear
    Policy-name: p1
    Bind-interface: st0.3
    Location: FPC 1, PIC 2, KMD-Instance 3
    Direction: inbound, SPI: 3727011331, AUX-SPI: 0
    Hard lifetime: Expires in 3570 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 3525 seconds
    Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: -
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128 bits)
    Anti-replay service: enabled, Replay window size: 32

    Location: FPC 1, PIC 2, KMD-Instance 3
    Direction: outbound, SPI: 4212479378, AUX-SPI: 0
    Hard lifetime: Expires in 3570 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 3525 seconds
    Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: -
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128 bits)
    Anti-replay service: enabled, Replay window size: 32
```

## Sample Output

show security ipsec security-associations family inet6

```
user@host> show security ipsec security-associations family inet6
  Virtual-system: root
  Local Gateway: 1212::1111, Remote Gateway: 1212::1112
  Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
    DF-bit: clear
    Direction: inbound, SPI: 14caf1d9, AUX-SPI: 0
                              , VPN Monitoring: -
    Hard lifetime: Expires in 3440 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 2813 seconds
    Mode: tunnel, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Anti-replay service: counter-based enabled, Replay window size: 64

    Direction: outbound, SPI: 9a4db486, AUX-SPI: 0
                              , VPN Monitoring: -
    Hard lifetime: Expires in 3440 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 2813 seconds
    Mode: tunnel, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Anti-replay service: counter-based enabled, Replay window size: 64
```

## Sample Output

show security ipsec security-associations fpc 6 pic 1

```
user@host> show security ipsec security-associations fpc 6 pic 1 kmd-instance all
  Total active tunnels: 1

ID    Gateway          Port  Algorithm       SPI      Life:sec/kb  Mon vsys
```

Copyright © 2013, Juniper Networks, Inc.

kmd-instance all (SRX Series Devices)

```
<2    1.1.1.2          500   ESP:3des/sha1   67a7d25d 28280/unlim   -   0
>2    1.1.1.2          500   ESP:3des/sha1   a23cbcdc 28280/unlim   -   0
```


Copyright © 2013, Juniper Networks, Inc.

## show security ipsec statistics

**Syntax**

**show security ipsec statistics**
<**fpc** *slot-number* >
<**index** *SA-index-number* >
<**kmd-instance** *kmd-instance-name* >
**pic** *slot-number*

**Release Information**

Command introduced in Release 8.5 of Junos OS; **fpc** and **pic** options added in Release 9.3 of Junos OS ;**kmd-instance** option added in Release 10.4 of Junos OS.

**Description**

Display standard IPsec statistics.

**Options**

- none—Display statistics about all IPsec security associations (SAs).
- **fpc** *slot-number* —Specific to SRX Series devices. Display statistics about existing IPsec SAs in this Flexible PIC Concentrator (FPC) slot. This option is used to filter the output.
- **index** *SA-index-number* —(Optional) Display statistics for the SA with this index number.
- **kmd-instance** *kmd-instance-name* —Specific to SRX Series devices. Display information about existing IKE SAs in the key management process (the daemon, which in this case is KMD) identified by FPC *slot-number* and PIC *slot-number*. This option is used to filter the output.
  - **all**—All KMD instances running on the Services Processing Unit (SPU).
  - ***kmd-instance-name***—Name of the KMD instance running on the SPU.
- **pic** *slot-number* —Specific to SRX Series devices. Display statistics about existing IPsec SAs in this PIC slot. This option is used to filter the output.

**Required Privilege Level**

view

**Related Documentation**

- MPLS for Security Devices
- clear security ipsec statistics on page 1452

**List of Sample Output**

show security ipsec statistics on page 2081
show security ipsec statistics index 5 on page 2081
show security ipsec statistics fpc 6 pic 1 (SRX Series devices) on page 2081

**Output Fields**

Table 175 on page 2079 lists the output fields for the **show security ipsec statistics** command. Output fields are listed in the approximate order in which they appear.

### Table 175: show security ipsec statistics Output Fields

| Field Name | Field Description |
|---|---|
| **Virtual-system** | The root system. |

Copyright © 2013, Juniper Networks, Inc.

Table 175: show security ipsec statistics Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **ESP Statistics** | • **Encrypted bytes**—Total number of bytes encrypted by the local system across the IPsec tunnel.<br>• **Decrypted bytes**—Total number of bytes decrypted by the local system across the IPsec tunnel.<br>• **Encrypted packets**—Total number of packets encrypted by the local system across the IPsec tunnel.<br>• **Decrypted packets**—Total number of packets decrypted by the local system across the IPsec tunnel. |
| **AH Statistics** | • **Input bytes**—Total number of bytes received by the local system across the IPsec tunnel.<br>• **Output bytes**—Total number of bytes transmitted by the local system across the IPsec tunnel.<br>• **Input packets**—Total number of packets received by the local system across the IPsec tunnel.<br>• **Output packets**—Total number of packets transmitted by the local system across the IPsec tunnel. |
| **Errors** | • **AH authentication failures**—Total number of authentication header (AH) failures. An AH failure occurs when there is a mismatch of the authentication header in a packet transmitted across an IPsec tunnel.<br>• **Replay errors**—Total number of replay errors. A replay error is generated when a duplicate packet is received within the replay window.<br>• **ESP authentication failures**—Total number of Encapsulation Security Payload (ESP) failures. An ESP failure occurs when there is an authentication mismatch in ESP packets.<br>• **ESP decryption failures**—total number of ESP decryption errors.<br>• **Bad headers**—Total number of invalid headers detected.<br>• **Bad trailers**—Total number of invalid trailers detected. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security ipsec statistics

```
user@host> show security ipsec statistics
Virtual-system: Root
ESP Statistics:
  Encrypted bytes:                0
  Decrypted bytes:                0
  Encrypted packets:              0
  Decrypted packets:              0
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```

## Sample Output

### show security ipsec statistics index 5

```
user@host> show security ipsec statistics index 5
Virtual-system: Root
SA index: 5
ESP Statistics:
  Encrypted bytes:                0
  Decrypted bytes:                0
  Encrypted packets:              0
  Decrypted packets:              0
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```

## Sample Output

### show security ipsec statistics fpc 6 pic 1 (SRX Series devices)

```
user@host> show security ipsec statistics fpc 6 pic 1
ESP Statistics:
Encrypted bytes:           536408
Decrypted bytes:           696696
Encrypted packets:           1246
Decrypted packets:            888
AH Statistics:
Input bytes:                    0
Output bytes:                   0
Input packets:                  0
Output packets:                 0
Errors:
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
```

Copyright © 2013, Juniper Networks, Inc.

## show security log

**Syntax** show security log {*all*| *destination-address*| *destination-port*| *event-id*| *failure*|*interface-name*| *newer-than*| *older-than*| *process*| *protocol*| *severity*| *sort-by*| *source-address*| *source-port*| *success*| *user*}

**Release Information** Command introduced in Release 11.2 of Junos OS.

**Description** Display security event logs. This command continuously displays security events on the screen. To stop the display, press Ctrl+c.

**Options**

**all**—Displays all audit event logs stored in the device memory.

**destination-address**—Displays audit event logs with the specified destination address.

**destination-port**—Displays audit event logs with the specified destination port.

**event-id**—Displays audit event logs with the specified event identification number.

**failure**—Displays failed audit event logs.

**interface-name**—Displays audit event logs with the specified interface.

**newer-than**—Displays audit event logs newer than the specified date and time.

**older-than**—Displays audit event logs older than the specified date and time.

**process**—Displays audit event logs with the specified process that generated the event.

**protocol**—Displays audit event logs generated through the specified protocol.

**severity**—Displays audit event logs generated with the specified severity.

**sort-by**—Displays audit event logs generated sorted with the specified options.

**source-address**—Displays audit event logs with the specified source address.

**source-port**—Displays audit event logs with the specified source port.

**success**—Displays successful audit event logs.

**username**—Displays audit event logs generated for the specified user.

**Required Privilege Level** view

**Related Documentation**

- exclude (Security Log) on page 568
- clear security log on page 1454
- Log File Formats

**List of Sample Output** show security log on page 2084


Copyright © 2013, Juniper Networks, Inc.

**Output Fields** Table 176 on page 2083 lists the output fields for the **show security log** command. Output fields are listed in the approximate order in which they appear.

### Table 176: show security log Output Fields

| Field Name | Field Description |
|---|---|
| **Event time** | The timestamp of the events received.<br><br>On SRX Series devices, security logs were always timestamped using the UTC time zone by running **set system time-zone utc** and **set security log utc-timestamp** CLI commands. Now, time zone can be defined using the local time zone by running the **set system time-zone time-zone** command to specify the local time zone that the system should use when timestamping the security logs. |
| **Message** | Security events are listed. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security log

```
user@host> show security log
Event time               Message
2010-10-22 13:28:37 CST  session created 1.1.1.2/1->2.2.2.2/1308 icmp
1.1.1.2/1->2.2.2.2/1308 None None 1 policy1 trustZone untrustZone 52 N/A(N/A)
ge-0/0/1.0
2010-10-22 13:28:38 CST  session created 1.1.1.2/2->2.2.2.2/1308 icmp
1.1.1.2/2->2.2.2.2/1308 None None 1 policy1 trustZone untrustZone 54 N/A(N/A)
ge-0/0/1.0

...

2010-10-22 13:36:12 CST  session denied 1.1.1.2/1->2.2.2.2/54812 icmp 1(8) policy1
 trustZone untrustZone N/A(N/A) ge-0/0/1.0
2010-10-22 13:36:14 CST  session denied 1.1.1.2/2->2.2.2.2/54812 icmp 1(8) policy1
 trustZone untrustZone N/A(N/A) ge-0/0/1.0

...

2010-10-27 15:50:11 CST  IP spoofing! source: 2.2.2.20, destination: 2.2.2.2,
protocol-id: 17, zone name: trustZone, interface name: ge-0/0/1.0, action: drop
2010-10-27 15:50:11 CST  IP spoofing! source: 2.2.2.20, destination: 2.2.2.2,
protocol-id: 17, zone name: trustZone, interface name: ge-0/0/1.0, action: drop

...

2011-02-18 15:53:34 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/certification-authority/ca-profile1-ca1.cert
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/crl/ca-profile1.crl
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/system-key-pair/system-generated.priv
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/system-cert/system-generated.cert
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/key-pair/cert1.priv
2011-02-18 15:53:42 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/key-pair/test2.priv

...

2011-03-14 23:00:40 PDT  IDP_COMMIT_COMPLETED: IDP policy commit is complete.
                         IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]

 ,failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT  ]
                         IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]

 ,failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT  ]
                         IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]

 ,failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT  ]

...

Event time               Message
```


Copyright © 2013, Juniper Networks, Inc.

```
2011-03-21 14:21:49 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
 9.9.9.1 source-address 6.6.6.1 '
2011-03-21 14:23:01 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
 9.9.9.1 source-address 6.6.6.1 '
2011-03-21 14:23:05 CST  KMD_PM_SA_ESTABLISHED: Local gateway: 7.7.7.1, Remote
gateway: 8.8.8.1, Local ID: ipv4(any:0,[0..3]=6.6.6.1), Remote ID:
ipv4(any:0,[0..3]=9.9.9.1), Direction: inbound, SPI: 37a2a179, AUX-SPI: 0, Mode:
 tunnel, Type: dynamic
2011-03-21 14:23:05 CST  KMD_PM_SA_ESTABLISHED: Local gateway: 7.7.7.1, Remote
gateway: 8.8.8.1, Local ID: ipv4(any:0,[0..3]=6.6.6.1), Remote ID:
ipv4(any:0,[0..3]=9.9.9.1), Direction: outbound, SPI: b2231c1f, AUX-SPI: 0, Mode:
 tunnel, Type: dynamic
2011-03-21 14:23:08 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
 9.9.9.1 source-address 6.6.6.1 '
2011-03-21 14:23:13 CST  UI_CMDLINE_READ_LINE: User 'root', command 'show security
 log '
```

Copyright © 2013, Juniper Networks, Inc.

## show security log file

**Syntax** show security log file

**Release Information** Command introduced in Release 12.1 of Junos OS.

**Description** Enables customers to view event-mode log files stored on the device in binary format.

**Required Privilege Level** view

**Related Documentation**

- System Log Messages
- Security Logs
- CLI Statements and Commands
- show security log on page 2082

**List of Sample Output** show security log file on page 2087

**Output Fields** Table 177 on page 2086 lists the output fields for the **show security log file** command. Output fields are listed in the approximate order in which they appear.

Table 177: show security log file Output Fields

| Field Name | Field Description |
|---|---|
| **Event time** | The timestamp when the security event was received. |
| **Message** | The message describing the security event. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security log file

```
user@host> show security log file
<14>1 2011-08-28T21:14:43 topstar RT_FLOW - RT_FLOW_SESSION_CREATE
[junos@2636.1.1.1.2.34 source-address="7.7.7.2" source-port="1"
destination-address="8.8.8.2" destination-port="5636" service-name="icmp"
nat-source-address="7.7.7.2" nat-source-port="1" nat-destination-address="8.8.8.2"
 nat-destination-port="5636" src-nat-rule-name="None" dst-nat-rule-name="None"
protocol-id="1" policy-name="client-to-server" source-zone-name="client"
destination-zone-name="server" session-id-32="60000442" username="N/A" roles="N/A"
 packet-incoming-interface="ge-0/0/0.0"]

<14>1 2011-08-28T21:14:45 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.34 reason="response received" source-address="7.7.7.2"
source-port="0" destination-address="8.8.8.2" destination-port="5636"
service-name="icmp" nat-source-address="7.7.7.2" nat-source-port="0"
nat-destination-address="8.8.8.2" nat-destination-port="5636"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="1"
policy-name="client-to-server" source-zone-name="client"
destination-zone-name="server" session-id-32="60000441" packets-from-client="1"
bytes-from-client="84" packets-from-server="1" bytes-from-server="84"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/0.0"]

...

user@host> show security log file
<14>1 2011-11-17T23:41:46 topstar RT_FLOW - RT_FLOW_SESSION_CREATE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" username="N/A"
roles="N/A" packet-incoming-interface="ge-0/0/2.0"]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.34 reason="response received" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218"
packets-from-client="1" bytes-from-client="104" packets-from-server="1"
bytes-from-server="104" elapsed-time="3" application="UNKNOWN"
nested-application="UNKNOWN" username="N/A" roles="N/A"
packet-incoming-interface="ge-0/0/2.0" encrypted="No "]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" reason="response received"
source-address="3001::2" source-port="0" destination-address="5001::2"
destination-port="17420" service-name="icmpv6" nat-source-address="3001::2"
nat-source-port="0" nat-destination-address="5001::2" nat-destination-port="17420"
 src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218"
packets-from-client="1" bytes-from-client="104" packets-from-server="1"
```

Copyright © 2013, Juniper Networks, Inc.

```
bytes-from-server="104" elapsed-time="3" application="UNKNOWN"
nested-application="UNKNOWN" username="N/A" roles="N/A"
packet-incoming-interface="ge-0/0/2.0" encrypted="No "]

 ...
```


Copyright © 2013, Juniper Networks, Inc.

## show security match-policies

**Syntax**

**show security match-policies**
**destination-ip** *ip-address*
**destination-port** *port-number*
**from-zone** *zone-name*
**protocol** *protocol-name* | *protocol-number*
**result-count** *number*
**source-identity** *role-name*
**source-ip** *ip-address*
**source-port** *port-number*
**to-zone** *zone-name*

**Release Information**

Command introduced in Release 10.3 of Junos OS.
Command updated in Release 10.4 of Junos OS.
Command updated in Release 12.1 of Junos OS.

**Description**

The **show security match-policies** command allows you to troubleshoot traffic problems using the match criteria: source port, destination port, source IP address, destination IP address, and protocol. For example, if your traffic is not passing because either an appropriate policy is not configured or the match criteria is incorrect, then the **show security match-policies** command allows you to work offline and identify where the problem actually exists. It uses the search engine to identify the problem and thus enables you to use the appropriate match policy for the traffic.

The **result-count** option specifies how many policies to display. The first enabled policy in the list is the policy that is applied to all matching traffic. Other policies below it are "shadowed" by the first and are never encountered by matching traffic.



NOTE: **The show security match-policies command is applicable only to security policies; IDP policies are not supported.**

**Options**

- **destination-ip** ***destination-ip***—Destination IP address of the traffic.
- **destination-port** ***destination-port***—Destination port number of the traffic. Range is 1 through 65,535
- **from-zone** ***from-zone***—Name or ID of the source zone of the traffic.
- **protocol** ***protocol-name*** **|** ***protocol-number***—Protocol name or numeric value of the traffic.
  - **ah** or **51**
  - **egp** or **8**
  - **esp** or **50**
  - **gre** or **47**
  - **icmp** or **1**
  - **igmp** or **2**

Copyright © 2013, Juniper Networks, Inc.

- **igp** or **9**
- **ipip** or **94**
- **ipv6** or **41**
- **ospf** or **89**
- **pgm** or **113**
- **pim** or **103**
- **rdp** or **27**
- **rsvp** or **46**
- **sctp** or **132**
- **tcp** or **6**
- **udp** or **17**
- **vrrp** or **112**

- **result-count** ***number***—(Optional) The number of policy matches to display. Valid range is from 1 through 16. The default value is 1.
- **source-identity** ***role-name***—Source identity of the traffic determined by the user role.
- **source-ip** ***source-ip***—Source IP address of the traffic.
- **source-port** ***source-port***—Source port number of the traffic. Range is 1 through 65,535.
- **to-zone** ***to-zone***—Name or ID of the destination zone of the traffic.

**Required Privilege Level** view

**Related Documentation**
- clear security policies statistics on page 1467
- Logical Systems for Security Devices

**List of Sample Output**
Example 1: show security match-policies on page 2093
Example 2: show security match policies ... result-count on page 2093
Example 3: show security match policies ... source-identity on page 2093

**Output Fields** Table 178 on page 2090 lists the output fields for the **show security match-policies** command. Output fields are listed in the approximate order in which they appear.

### Table 178: show security match-policies Output Fields

| Field Name | Field Description |
|---|---|
| **Policy:** | Name of the applicable policy. |


Copyright © 2013, Juniper Networks, Inc.

Table 178: show security match-policies Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Action** or **Action-type:** | The action to be taken for traffic that matches the policy's match criteria. Actions include the following:<br>• **permit**<br>• **firewall-authentication**<br>• **tunnel ipsec-vpn** *vpn-name*<br>• **pair-policy** *pair-policy-name*<br>• **source-nat pool** *pool-name*<br>• **pool-set** *pool-set-name*<br>• **interface**<br>• **destination-nat** *name*<br>• **deny**<br>• **reject** |
| **State:** | Status of the policy:<br>• **enabled**: The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it.<br>• **disabled**: The policy cannot be used in the policy lookup process, and therefore it is not available for access control. |
| **Index:** | An internal number associated with the policy. |
| **Sequence number:** | Number of the policy within a given context. For example, three policies that are applicable in a from-zoneA-to-zoneB context might be ordered with sequence numbers 1, 2, and 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, and 4. |
| **From zone:** | Name of the source zone. |
| **To zone:** | Name of the destination zone. |
| **Source addresses:** | The names and corresponding IP addresses of the source addresses for a policy. Address sets are resolved to their individual address name-IP address pairs. |
| **Destination addresses:** | The names and corresponding IP addresses of the destination addresses (or address sets) for a policy as entered in the destination zone's address book. A packet's destination address must match one of these addresses for the policy to apply to it. |
| **Application** | Name of a preconfigured or custom application, or **any** if no application is specified. |
| **IP protocol:** | Numeric value for the IP protocol used by the application, such as 6 for TCP or 1 for ICMP. |
| **ALG:** | If an ALG is associated with the session, the name of the ALG. Otherwise, 0. |
| **Inactivity timeout:** | Elapsed time without activity after which the application is terminated. |
| **Source-port range:** | Range of matching source ports defined in the policy. |

Copyright © 2013, Juniper Networks, Inc.

Table 178: show security match-policies Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Destination-port range:** | Range of matching destination ports defined in the policy. |
| **Source identites** | One or more user roles defined in the matching policy. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### Example 1: show security match-policies

```
user@host> show security match-policies from-zone z1 to-zone z2 source-ip 10.10.10.1
destination-ip 30.30.30.1 source-port 1 destination-port 21 protocol tcp
Policy: p1, action-type: permit, State: enabled, Index: 4
  Sequence number: 1
  From zone: z1, To zone: z2
  Source addresses:
    a2: 20.20.0.0/16
    a3: 10.10.10.1/32
  Destination addresses:
    d2: 40.40.0.0/16
    d3: 30.30.30.1/32
  Application: junos-ftp
    IP protocol: tcp, ALG: ftp, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination port range: [21-21]
```

### Example 2: show security match policies ... result-count

```
user@host> show security match-policies source-ip 10.10.10.1 destination-ip 20.20.20.5
source_port 1004 destination_port 80 protocol tcp result_count 5
Policy: p1, action-type: permit, State: enabled, Index: 4
  Sequence number: 1
  From zone: zone-A, To zone: zone-B
  Source addresses:
    sa1: 10.10.0.0/16
  Destination addresses:
    da5: 20.20.0.0/16
  Application: any
    IP protocol: 1, ALG: 0, Inactivity timeout: 0
      Source port range: [1000-1030]
    Destination port range: [80-80]

Policy: p15, action-type: deny, State: enabled, Index: 18
  Sequence number: 15
  From zone: zone-A, To zone: zone-B
  Source addresses:
    sa11: 10.10.10.1/32
  Destination addresses:
    da15: 20.20.20.5/32
  Application: any
    IP protocol: 1, ALG: 0, Inactivity timeout: 0
      Source port range: [1000-1030]
    Destination port range: [80-80]
```

### Example 3: show security match policies ... source-identity

```
user@host> show security match-policies from-zone untrust to-zone trust source-ip 10.10.10.1
destination-ip 20.20.20.5 destination_port 21 protocol 6 source-port 1234 source-identity role1
Policy: p1, action-type: permit, State: enabled, Index: 40
      Policy Type: Configured
      Sequence number: 1
      From zone: untrust, To zone: trust
      Source addresses:
        a1: 20.0.0.0/8
      Destination addresses:
        d1: 21.0.0.0/8
      Application: junos-ftp
        IP protocol: tcp, ALG: ftp, Inactivity timeout: 1800
          Source port range: [0-0]
          Destination port range: [21-21]
```

Copyright © 2013, Juniper Networks, Inc.

```
Source identities: role1
Per policy TCP Options: SYN check: No, SEQ check: No
```


Copyright © 2013, Juniper Networks, Inc.

## show security monitoring fpc fpc-number

**Syntax** **show security monitoring fpc** *fpc-number*
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 9.2 of Junos OS.

**Description** Display security monitoring information about the FPC slot.

**Options**

- ***fpc-number*** —Display security monitoring information for the specified FPC slot. It can be in the range from 0 to 11.
- **node**—(Optional) For chassis cluster configurations, display security monitoring information for the specified FPC on a specific node (device) in the cluster.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Additional Information** For complete list of slot numbering, physical port, and logical interface numbering for SRX Series devices in chassis cluster, see Chassis Cluster for Security Devices.

**Required Privilege Level** view

**Related Documentation**

- Device and Routing Operations Monitoring

**List of Sample Output**

show security monitoring fpc 0 on page 2097
show security monitoring fpc 1 on page 2097
show security monitoring fpc 8 on page 2097

**Output Fields** Table 179 on page 2095 lists the output fields for the **show security monitoring fpc** *fpc-number* command. Output fields are listed in the approximate order in which they appear.

### Table 179: show security monitoring fpc fpc-number Output Fields

| Field Name | Field Description |
|---|---|
| FPC | Slot number in which the FPC is installed. |
| PIC | Slot number in which the PIC is installed. |
| CPU Utilization (%) | Total percentage of CPU being used by the PIC's processors. |
| Memory Utilization (%) | Percentage of heap space (dynamic memory) being used by the PIC's processor. If this number exceeds 80 percent, there may be a software problem (memory leak). |

Copyright © 2013, Juniper Networks, Inc.

Table 179: show security monitoring fpc fpc-number Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Current flow session** | The current number of flow sessions. When SRX Series devices operate in packet mode, flow sessions will not be created and this field will remain zero. |
| **Max flow session** | The maximum number of flow sessions allowed. This number will differ from one device to another. |
| **SPU current cp session** | The current number of cp sessions for the SPU (on SRX3400, SRX3600, SRX5600, and SRX5800 devices only). |
| **SPU max cp session** | The maximum number of cp sessions allowed for the SPU (on SRX3400, SRX3600, SRX5600, and SRX5800 devices only). |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security monitoring fpc 0

```
user@host> show security monitoring fpc 0
FPC 0
  PIC 0
    CPU utilization      :    0 %
    Memory utilization   :   82 %
    Current flow session :    0
    Max flow session     :    0
    Current CP session   :    0
    Max CP session       : 12000000
Session Creation Per Second (for last 96 seconds on average):    0
  PIC 1
    CPU utilization      :    0 %
    Memory utilization   :   54 %
    Current flow session :    0
    Max flow session     : 819200
    Current CP session   :    0
    Max CP session       :    0
Session Creation Per Second (for last 96 seconds on average):    0
```

## Sample Output

### show security monitoring fpc 1

```
user@host> show security monitoring fpc 1
FPC 1
  PIC 0
    CPU utilization      :    0 %
    Memory utilization   :   21 %
    Current flow session :    0
    Max flow session     : 524288
    Current CP session   :    0
    Max CP session       : 1048576
Session Creation Per Second (for last 96 seconds on average):    0
```

## Sample Output

### show security monitoring fpc 8

```
user@host> show security monitoring fpc 5
FPC 5
  PIC 0
    CPU utilization      :    0 %
    Memory utilization   :   64 %
    Current flow session :    0
    Max flow session     : 524288
    Current CP session   :    0
    Max CP session       : 2359296
Session Creation Per Second (for last 96 seconds on average):    0
  PIC 1
    CPU utilization      :    0 %
    Memory utilization   :   65 %
    Current flow session :    0
    Max flow session     : 1048576
    Current CP session   :    0
    Max CP session       :    0
Session Creation Per Second (for last 96 seconds on average):    0
```

Copyright © 2013, Juniper Networks, Inc.

## show security monitoring performance session

**Syntax** show security monitoring performance session

```
<fpc slot-number>

<pic slot-number>
```

**Release Information** Command introduced in Release of 10.2 of Junos OS.

**Description** Display the number of sessions added (ramp-up rate) for the last 60 seconds. Output of this command does not display the total number of sessions or the number of deleted sessions.

**Options**

- **fpc slot-number** — Display information about the FPC slot. Use this option to filter the output based on the slot number.
- **pic slot-number** — Display information about existing PIMs or Mini-PIMs in a particular PIC slot. Use this option to filter the output based on PIC slot.



NOTE: The fpc slot-number and pic slot-number options are not available on SRX100, SRX210, SRX240, and SRX650 devices.

**Required Privilege Level** View

**Related Documentation**

- Device and Routing Operations Monitoring

## show security monitoring performance session

**user@host> show security monitoring performance session**

```
fpc  0  pic  0
Last 60 seconds:
 0:       8   1:       8   2:       8   3:       8   4:       8   5:       7
 6:       7   7:       7   8:       7   9:       7  10:       7  11:       8
12:       8  13:       8  14:       7  15:       7  16:       7  17:       7
18:       7  19:       7  20:       7  21:       5  22:       5  23:       5
24:       5  25:       5  26:       5  27:       5  28:       5  29:       4
30:       4  31:       4  32:       3  33:       3  34:       3  35:       3
36:       5  37:       5  38:       6  39:       6  40:       5  41:       5
42:       5  43:       5  44:       5  45:       5  46:       5  47:       5
48:       7  49:       7  50:       6  51:       8  52:       8  53:       6
54:       5  55:       7  56:       7  57:       5  58:       5  59:       8
```


Copyright © 2013, Juniper Networks, Inc.

## show security monitoring performance spu

**Syntax** show security monitoring performance spu

```
<fpc slot-number>

<pic slot-number>
```

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display the services processing unit (SPU) statistics for all FPC slots over the last 60 seconds.

**Options**

- **fpc slot-number** — Display information about the FPC slot. Use this option to filter the output based on the slot number.
- **pic slot-number** — Display information about existing PIMs or Mini-PIMs in a particular PIC slot. Use this option to filter the output based on PIC slot.



NOTE: The fpc slot-number and pic slot-number options are not available on SRX100, SRX210, SRX240, and SRX650 devices.

**Required Privilege Level** View

**Related Documentation**

- Device and Routing Operations Monitoring

## show security monitoring performance spu

**user@host>show security monitoring performance spu**

```
fpc  0  pic  0
Last 60 seconds:
 0:  48   1:  48   2:  48   3:  48   4:  48   5:  48
 6:  48   7:  48   8:  49   9:  48  10:  48  11:  48
12:  48  13:  48  14:  48  15:  48  16:  48  17:  48
18:  48  19:  48  20:  48  21:  48  22:  49  23:  48
24:  49  25:  49  26:  48  27:  48  28:  48  29:  48
30:  48  31:  48  32:  48  33:  48  34:  48  35:  48
36:  46  37:  47  38:  46  39:  46  40:  46  41:  46
42:  46  43:  46  44:  46  45:  46  46:  46  47:  46
48:  46  49:  46  50:  46  51:  46  52:  46  53:  46
54:  46  55:  46  56:  46  57:  46  58:  46  59:  46
```

Copyright © 2013, Juniper Networks, Inc.

## show security nat destination pool

**Syntax**

show security nat destination pool
< *pool-name* >
all
logical-system *logical-system-name*
root-logical-system

**Release Information**

Command introduced in Junos OS Release 9.2. The **Description** output field added in Junos OS Release 12.1.

**Description**

Display information about the specified Network Address Translation (NAT) destination address pool.

**Options**

- ***pool-name*** —Name of the destination address pool.
- **all**—Display information about all the destination NAT address pools.
- **logical-system *logical-system-name***—Display information about the destination NAT pools for the specified logical system.
- **root-logical-system**—Display information about the destination NAT pools for the master (root) logical system.

**Required Privilege Level**

view

**Related Documentation**

- pool (Security Destination NAT) on page 818
- Network Address Translation for Security Devices

**List of Sample Output**

show security nat destination pool dst-nat-pool1 on page 2101
show security nat destination pool all on page 2101

**Output Fields**

Table 180 on page 2100 lists the output fields for the **show security nat destination pool** command. Output fields are listed in the approximate order in which they appear.

### Table 180: show security nat destination pool Output Fields

| Field Name | Field Description |
|---|---|
| **Pool name** | Name of the destination pool. |
| **Description** | Description of the destination pool. |
| **Pool id** | Pool identification number. |
| **Routing instance** | Name of the routing instance. |
| **Total address** | Number of IP addresses that are in use. |
| **Translation hits** | Number of translation hits. |


Copyright © 2013, Juniper Networks, Inc.

Table 180: show security nat destination pool Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Address range** | IP address or IP address range for the pool. |

## Sample Output

### show security nat destination pool dst-nat-pool1

```
user@host> show security nat destination pool dst-p1

Pool name       : dst-p1
Description     : The destination pool dst-p1 is for the sales team
Pool id         : 1
Routing instance: default
Total address   : 1
Translation hits: 0
Address range                       Port
     1.1.1.1 - 1.1.1.1              0
```

## Sample Output

### show security nat destination pool all

```
user@host> show security nat destination pool all

Total destination-nat pools: 2

Pool name       : dst-p1
Description     : The destination pool dst-p1 is for the sales team
Pool id         : 1
Routing instance: default
Total address   : 1
Translation hits: 0
Address range                       Port
     1.1.1.1 - 1.1.1.1              0

Pool name       : dst-p2
Description     : The destination pool dst-p2 is for the sales team
Pool id         : 2
Routing instance: default
Total address   : 1
Translation hits: 0
Address range                       Port
     2001::1 - 2001::1              0
```

Copyright © 2013, Juniper Networks, Inc.

## show security nat destination rule

**Syntax**

show security nat destination rule
*<rule-name>*
all
logical-system *logical-system-name*
root-logical-system

**Release Information**

Command introduced in Junos OS Release 9.2. The **Description** output field added in Junos OS Release 12.1.

**Description**

Display information about the specified destination Network Address Translation (NAT) rule.

**Options**

- ***rule-name***—Name of the rule.
- **all**—Display information about all the destination NAT rules.
- **logical-system *logical-system-name***—Display information about the destination NAT rules for the specified logical system.
- **root-logical-system**—Display information about the destination NAT rules for the master (root) logical system.

**Required Privilege Level**

view

**Related Documentation**

- rule (Security Destination NAT) on page 896
- Network Address Translation for Security Devices
- Logical Systems for Security Devices

**List of Sample Output**

show security nat destination rule dst2-rule on page 2104
show security nat destination rule all on page 2104

**Output Fields**

Table 181 on page 2102 lists the output fields for the **show security nat destination rule** command. Output fields are listed in the approximate order in which they appear.

### Table 181: show security nat destination rule Output Fields

| Field Name | Field Description |
|---|---|
| **Destination NAT rule** | Name of the destination NAT rule. |
| **Description** | Description of the destination NAT rule. |
| **Rule-Id** | Rule identification number. |
| **Rule position** | Position of the destination NAT rule. |
| **From routing instance** | Name of the routing instance from which the packets flow. |


Copyright © 2013, Juniper Networks, Inc.

Table 181: show security nat destination rule Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **From interface** | Name of the interface from which the packets flow. |
| **From zone** | Name of the zone from which the packets flow. |
| **Source addresses** | Name of the source addresses which match the rule. The default value is any. |
| **Destination addresses** | Name of the destination addresses which match the rule. The default value is any. |
| **Action** | The action taken when a packet matches the rule's tuples. Actions include the following:<br>• **destination NAT pool**—Use user-defined destination NAT pool to perform destination NAT.<br>• **off**—Do not perform destination NAT. |
| **Destination port** | Destination ports number which match the rule. The default value is any. |
| **Translation hits** | Number of translation hits. |
| **Total destination-nat rules** | Number of destination NAT rules. |
| **Total referenced IPv4/IPv6 ip-prefixes** | Number of IP prefixes referenced in source, destination, and static NAT rules. This total includes the IP prefixes configured directly as address names and as address set names in the rule. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security nat destination rule dst2-rule

```
user@host>show security nat destination rule dst2-rule

 Destination NAT rule: dst2-rule            Rule-set: dst2
  Description               : The destination rule dst2-rule is for the sales
team
  Rule-Id                   : 1
  Rule position             : 1
  From routing instance     : ri1
                            : ri2
  Match
    Source addresses        : add1
                              add2
    Destination addresses   : add9
  Action                    : off

  Destination port          : 0
  Translation hits          : 0
```

## Sample Output

### show security nat destination rule all

```
user@host>  show security nat destination rule all

Total destination-nat rules: 171
Total referenced IPv4/IPv6 ip-prefixes: 6725/258

Destination NAT rule: dst2-rule            Rule-set: dst2
  Description               : The destination rule dst2-rule is for the sales
team
  Rule-Id                   : 1
  Rule position             : 1
  From routing instance     : ri1
                            : ri2
  Match
    Source addresses        : add1
                              add2
    Destination addresses   : add9
  Action                    : off

...
```


Copyright © 2013, Juniper Networks, Inc.

## show security nat destination summary

**Syntax** show security nat destination summary
logical-system *logical-system-name*

**Release Information** Command introduced in Junos OS Release 9.2.

**Description** Display a summary of Network Address Translation (NAT) destination pool information.

**Options**
- none—Display summary information about the destination NAT pool.
- **logical-system** *logical-system-name*—Display summary information about the destination NAT pool for the specified logical system.

**Required Privilege Level** view

**Related Documentation**
- pool (Security Destination NAT) on page 818
- rule (Security Destination NAT) on page 896
- Network Address Translation for Security Devices
- Logical Systems for Security Devices

**List of Sample Output** show security nat destination summary on page 2106

**Output Fields** Table 182 on page 2105 lists the output fields for the **show security nat destination summary** command. Output fields are listed in the approximate order in which they appear.

Table 182: show security nat destination summary Output Fields

| Field Name | Field Description |
|---|---|
| **Total destination nat pool number** | Number of destination NAT pools. |
| **Pool name** | Name of the destination address pool. |
| **Address range** | IP address or IP address range for the pool. |
| **Routing Instance** | Name of the routing instance. |
| **Port** | Port number. |
| **Total** | Number of IP addresses that are in use. |
| **Available** | Number of IP addresses that are free for use. |
| **Total destination nat rule number** | Number of destination NAT rules. |
| **Total hit times** | Number of times a translation in the translation table is used for all the destination NAT rules. |

Copyright © 2013, Juniper Networks, Inc.

Table 182: show security nat destination summary Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Total fail times** | Number of times a translation in the translation table failed to translate for all the destination NAT rules. |

## Sample Output

### show security nat destination summary

```
user@host> show security nat destination summary

Total pools: 2
Pool name           Address                  Routing        Port  Total
                    Range                    Instance             Address
dst-p1              1.1.1.1  - 1.1.1.1        default        0     1
dst-p2              2001::1  - 2001::1        default        0     1

Total rules: 171
Rule name           Rule set       From                           Action
dst2-rule           dst2           ri1
                                   ri2
                                   ri3
                                   ri4
                                   ri5
                                   ri6
                                   ri7
dst3-rule           dst3           ri9                            off
                                   ri1
                                   ri2
                                   ri3
                                   ri4
                                   ri5

...
```


Copyright © 2013, Juniper Networks, Inc.

## show security nat incoming-table

**Syntax** **show security nat incoming-table**
<node ( ***node-id*** | all | local | primary)>

**Release Information** Command introduced in Junos OS Release 8.5. The **node** options added in Junos OS Release 9.0.

**Description** Display Network Address Translation (NAT) table information.



NOTE: The incoming dip NAT table is replaced with ALG cone NAT binding table and the **show security nat incoming-table** command is obsolete from Junos OS Release 11.2 onward. The **show security nat incoming-table** command works as is in the previous releases.

**Options**

- none—Display all information NAT incoming table.
- **node**—(Optional) For chassis cluster configurations, display incoming table information on a specific node.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level** view

**Related Documentation**

- clear security nat incoming-table on page 1457
- Network Address Translation for Security Devices

**List of Sample Output** show security nat incoming-table on page 2108

**Output Fields** Table 183 on page 2107 lists the output fields for the **show security nat incoming-table** command. Output fields are listed in the approximate order in which they appear.

### Table 183: show security nat incoming-table Output Fields

| Field Name | Field Description |
|---|---|
| **In use** | Number of entries in the NAT table. |
| **Maximum** | Maximum number of entries possible in the NAT table. |
| **Entry allocation failed** | Number of entries failed for allocation. |

Copyright © 2013, Juniper Networks, Inc.

Table 183: show security nat incoming-table Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Destination** | Destination IP address and port number. |
| **Host** | Host IP address and port number that the destination IP address is mapped. |
| **References** | Number of sessions referencing the entry. |
| **Timeout** | Timeout, in seconds, of the entry in the NAT table. |
| **Source-pool** | Name of source pool where translation is allocated. |

## Sample Output

### show security nat incoming-table

```
user@host> show security nat incoming-table
In use: 1, Maximum: 1024, Entry allocation failed: 0
Destination           Host                  References Timeout Source-pool
10.1.1.26:1028        1.1.1.10:5060                  1    3600 p1
```


Copyright © 2013, Juniper Networks, Inc.

## show security nat interface-nat-ports

**Syntax**

**show security nat interface-nat-ports**
<node ( *node-id* | all | local | primary)>
logical-system *logical-system-name*

**Release Information**

Command modified in Junos OS Release 9.2. The **node** options added in Junos OS Release 9.0.

**Description**

Display port usage for an interface source pool for Network Address Translation (NAT).

**Options**

- none—Display all port usage information for an interface source pool.
- **node**—(Optional) For chassis cluster configurations, display interface NAT ports information on a specific node.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

  **logical-system *logical-system-name***—Display port usage information about an interface source pool for the specified logical system.

**Required Privilege Level**

view

**Related Documentation**

- Network Address Translation for Security Devices

**List of Sample Output**

show security nat interface-nat-ports on page 2110

**Output Fields**

Table 184 on page 2109 lists the output fields for the **show security nat interface-nat-ports** command. Output fields are listed in the approximate order in which they appear.

### Table 184: show security nat interface-nat-ports Output Fields

| Field Name | Field Description |
|---|---|
| **Pool Index** | Port pool index. |
| **Total Ports** | Total number of ports in a port pool. In SRX Series devices, 10 interface NAT ports are supported. |
| **Single Ports Allocated** | Number of ports allocated one at a time that are in use. |
| **Single Ports Available** | Number of ports allocated one at a time that are free for use. |
| **Twin Ports Allocated** | Number of ports allocated two at a time that are in use. |
| **Twin Ports Available** | Number of ports allocated two at a time that are free for use. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security nat interface-nat-ports

```
user@host> show security nat interface-nat-ports
Pool   Total  Single ports  Single ports  Twin ports  Twin ports
    index  ports     allocated     available   allocated   available
     0  64510             0         63486           0        1024
     1  64510             0         63486           0        1024
     2  64510             0         63486           0        1024
     3  64510             0         63486           0        1024
     4  64510             0         63486           0        1024
     5  64510             0         63486           0        1024
     6  64510             0         63486           0        1024
     7  64510             0         63486           0        1024
     8  64510             0         63486           0        1024
     9  64510             0         63486           0        1024
```


Copyright © 2013, Juniper Networks, Inc.

## show security nat source persistent-nat-table

**Syntax** show security nat source persistent-nat-table ( all | interface | internal-ip *ip-address* <internal-port *port*> | pool *poolname* )

**Release Information** Command introduced in Junos OS Release 9.6. Support for IPv6 addresses added in Junos OS Release 11.2.

**Description** Display a summary of persistent Network Address Translation (NAT) information.

**Options**

- **all**—Display all persistent NAT bindings.
- **interface**—Display persistent NAT bindings for the interface.
- **internal-ip *ip-address***—Display persistent NAT bindings for the specified internal IP address.
- **internal-ip *ip-address* internal-port *port***—Display persistent NAT bindings for the specified internal IP address and port.
- **pool**—Display persistent NAT bindings for the specified source NAT pool.

**Required Privilege Level** view

**Related Documentation**

- clear security nat source persistent-nat-table on page 1458
- Network Address Translation for Security Devices

**List of Sample Output**

show security nat source persistent–nat–table all on page 2112
show security nat source persistent–nat–table internal-ip 2000::1 on page 2112
show security nat source persistent–nat–table internal-ip 2000::1 internal-port 54281 on page 2112
show security nat source persistent–nat–table internal-ip 2000::1 internal-port 54281 internal-protocol 6 on page 2112
show security nat source persistent-nat-table summary on page 2113

**Output Fields** Table 185 on page 2111 lists the output fields for the **show security nat source persistent–nat–table** command. Output fields are listed in the approximate order in which they appear.

### Table 185: show security nat source persistent–nat–table Output Fields

| Field Name | Field Description |
|---|---|
| **Internal IP/Port** | Internal transport IP address and port number of the outgoing session from internal to external. |
| **Reflexive IP/Port** | Translated IP address and port number of the source IP address and port. |
| **Source NAT Pool** | The name of the source pool where persistent NAT is used. |

Copyright © 2013, Juniper Networks, Inc.

Table 185: show security nat source persistent–nat–table Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Type** | Persistent NAT type. |
| **Left_time/Conf_time** | The inactivity timeout period that remains and the configured timeout value. |
| **Current_Sess_Num/Max_Sess_Num** | The number of current sessions associated with the persistent NAT binding. |
| **Source NAT Rule** | Name of the source NAT rule to which this persistent NAT binding applies. |

## Sample Output

show security nat source persistent–nat–table all

```
user@host> show security nat source persistent–nat–table all
Persistent NAT Bindings on FPC4 PIC0:
Internal Reflective Source Type Left_time/ Curr_Sess_Num/ Source
In_IP In_Port I_Proto Ref_IP Ref_Port R_Proto NAT Pool Conf_time Max_Sess_Num NAT
 Rule
2000::1 54281 6 1.1.1.254 48240 6 interface any-remote-host -/300 1/30 pst_nat64
Persistent NAT Bindings on FPC5 PIC0:
```

## Sample Output

show security nat source persistent–nat–table internal-ip 2000::1

```
user@host> show security nat source persistent–nat–table internal-ip 2000::1
Persistent NAT Bindings on FPC4 PIC0:
Internal Reflective Source Type Left_time/ Curr_Sess_Num/ Source
In_IP In_Port I_Proto Ref_IP Ref_Port R_Proto NAT Pool Conf_time Max_Sess_Num NAT
 Rule
2000::1 54281 6 1.1.1.254 48240 6 interface any-remote-host -/300 1/30 pst_nat64
Persistent NAT Bindings on FPC5 PIC0:
```

## Sample Output

show security nat source persistent–nat–table internal-ip 2000::1 internal-port 54281

```
user@host> show security nat source persistent–nat–table internal-ip 2000::1 internal-port
54281
Persistent NAT Bindings on FPC4 PIC0:
Internal Reflective Source Type Left_time/ Curr_Sess_Num/ Source
In_IP In_Port I_Proto Ref_IP Ref_Port R_Proto NAT Pool Conf_time Max_Sess_Num NAT
 Rule
2000::1 54281 6 1.1.1.254 48240 6 interface any-remote-host -/300 1/30 pst_nat64
Persistent NAT Bindings on FPC5 PIC0:
```

## Sample Output

show security nat source persistent–nat–table internal-ip 2000::1

```
user@host> show security nat source persistent–nat–table internal-ip 2000::1 internal-port
54281 internal-protocol 6
Persistent NAT Bindings on FPC4 PIC0:
Internal Reflective Source Type Left_time/ Curr_Sess_Num/ Source
In_IP In_Port I_Proto Ref_IP Ref_Port R_Proto NAT Pool Conf_time Max_Sess_Num NAT
```


Copyright © 2013, Juniper Networks, Inc.

internal-port 54281 internal-protocol 6

```
 Rule
2000::1 54281 6 1.1.1.254 48240 6 interface any-remote-host -/300 1/30 pst_nat64
```

## Sample Output

show security nat source persistent-nat-table summary

```
user@host> show security nat source persistent-nat-table summary
Persistent NAT Table Statistics on FPC4 PIC0:
binding total : 65536
binding in use : 1
enode total : 524288
enode in use : 0
Persistent NAT Table Statistics on FPC5 PIC0:
binding total : 65536
binding in use : 0
enode total : 524288
enode in use : 0
```

Copyright © 2013, Juniper Networks, Inc.

## show security nat source pool

**Syntax**

show security nat source pool
< *pool-name* >
all
logical-system *logical-system-name*
root-logical-system

**Release Information**

Command introduced in Junos OS Release 9.2. **Description** output field added in Junos OS Release 12.1.

**Description**

Display information about the specified Network Address Translation (NAT) source address pool.

**Options**

- ***pool-name*** —Name of the source pool.
- **all**—Display information about all the source NAT address pools.
- **logical-system *logical-system-name***—Display information about the source NAT pools for the specified logical system.
- **root-logical-system**—Display information about the source NAT pools for the master (root) logical system.

**Required Privilege Level**

view

**Related Documentation**

- pool (Security Source NAT) on page 819
- Network Address Translation for Security Devices

**List of Sample Output**

show security nat source pool src-p1 on page 2116
show security nat source pool all on page 2116

**Output Fields**

Table 186 on page 2114 lists the output fields for the **show security nat source pool** command. Output fields are listed in the approximate order in which they appear.

### Table 186: show security nat source pool Output Fields

| Field Name | Field Description |
|---|---|
| **Pool name** | Name of the source pool. |
| **Description** | Description of the source pool. |
| **Pool id** | Pool identification number. |
| **Routing Instance** | Name of the routing instance. |
| **Host address base** | Base address of the original source IP address range. |
| **Port** | Port numbers used for the source pool. |


Copyright © 2013, Juniper Networks, Inc.

Table 186: show security nat source pool Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **port overloading** | Number of port overloading for the source pool. |
| **Total addresses** | Number of IP addresses that are in use. |
| **Translation hits** | Number of translation hits. |
| **Address range** | IP address or IP address range for the source pool. |
| **Single Ports** | Number of allocated single ports. |
| **Twin Ports** | Number of allocated twin ports. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security nat source pool src-p1

```
user@host> show security nat source pool src-p1

Pool name          : src-p1
Description        : The source pool src-p1 is for the sales team
Pool id            : 4
Routing instance   : default
Host address base  : 0.0.0.0
Port               : [1024, 63487]
port overloading   : 1
Total addresses    : 4
Translation hits   : 0
Address range                        Single Ports   Twin Ports
            3.3.3.0 - 3.3.3.3            0              0
```

## Sample Output

### show security nat source pool all

```
user@host> show security nat source pool all

Total pools: 4

Pool name          : src-p1
Description        : The source pool src-p1 is for the sales team
Pool id            : 4
Routing instance   : default
Host address base  : 0.0.0.0
Port               : [1024, 63487]
port overloading   : 1
Total addresses    : 4
Translation hits   : 0
Address range                        Single Ports   Twin Ports
            3.3.3.0 - 3.3.3.3            0              0

Pool name          : src-p2
Description        : The source pool src-p2 is for the sales team
Pool id            : 5
Routing instance   : default
Host address base  : 0.0.0.0
Port               : [1024, 63487]
port overloading   : 1
Total addresses    : 4
Translation hits   : 0
Address range                        Single Ports   Twin Ports
            4.4.4.0 - 4.4.4.3            0              0

Pool name          : src-p3
Description        : The source pool src-p3 is for the sales team
Pool id            : 6
Routing instance   : default
Host address base  : 0.0.0.0
Port               : [1024, 63487]
port overloading   : 1
Total addresses    : 1
Translation hits   : 0
Address range                        Single Ports   Twin Ports
            2003::1 - 2003::1            0              0

Pool name          : src-p4
```


Copyright © 2013, Juniper Networks, Inc.

```
Description        : The source pool src-p4 is for the sales team
Pool id            : 7
Routing instance   : default
Host address base  : 0.0.0.0
Port               : [1024, 63487]
port overloading   : 1
Total addresses    : 1
Translation hits   : 0
Address range                        Single Ports   Twin Ports
            2004::1 - 2004::1            0              0
```

Copyright © 2013, Juniper Networks, Inc.

## show security nat source rule

**Syntax**

show security nat source rule
*<rule-name>*
all
logical-system *logical-system-name*
root-logical-system

**Release Information**

Command introduced in Junos OS Release 9.2. Support for IPv6 addresses added in Junos OS Release 11.2. The **Description** output field added in Junos OS Release 12.1.

**Description**

Display information about the specified source Network Address Translation (NAT) rule.

**Options**

- ***rule-name***—Name of the rule.
- **all**—Display information about all the source NAT rules.
- **logical-system *logical-system-name***—Display information about the source NAT rules for the specified logical system.
- **root-logical-system**—Display information about the source NAT rules for the master (root) logical system.

**Required Privilege Level**

view

**Related Documentation**

- rule (Security Source NAT) on page 900
- Network Address Translation for Security Devices
- Logical Systems for Security Devices

**List of Sample Output**

show security nat source rule r2 on page 2120
show security nat source rule all on page 2120

**Output Fields**

Table 187 on page 2118 lists the output fields for the **show security nat source rule** command. Output fields are listed in the approximate order in which they appear

### Table 187: show security nat source rule Output Fields

| Field Name | Field Description |
|---|---|
| **Source NAT rule** | Name of the source NAT rule. |
| **Description** | Description of the source NAT rule. |
| **Rule-Id** | Rule identification number. |
| **Rule position** | Position of the source NAT rule. |
| **From zone** | Name of the zone from which the packets flow. |
| **To zone** | Name of the zone to which the packets flow. |


Copyright © 2013, Juniper Networks, Inc.

Table 187: show security nat source rule Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **From routing instance** | Name of the routing instance from which the packets flow. |
| **To routing instance** | Name of the routing instance to which the packets flow. |
| **From interface** | Name of the interface from which the packets flow. |
| **To interface** | Name of the interface to which the packets flow. |
| **Source addresses** | Name of the source addresses that match the rule. The default value is any. |
| **Destination address** | Name of the destination addresses that match the rule. The default value is any. |
| **Destination port** | Destination port numbers that match the rule. The default value is any. |
| **Action** | The action taken in regard to a packet that matches the rule's tuples. Actions include the following:<br>• **off**—Do not perform source NAT.<br>• **source NAT pool**—Use user-defined source NAT pool to perform source NAT<br>• **interface**—Use egress interface's IP address to perform source NAT. |
| **Persistent NAT type** | Persistent NAT type. |
| **Persistent NAT mapping type** | Persistent NAT mapping type. |
| **Inactivity timeout** | Inactivity timeout for persistent NAT binding. |
| **Max session number** | Maximum number of sessions. |
| **Translation hits** | Number of translation hits. |
| **Total rules** | Number of source NAT rules. |
| **Total referenced IPv4/IPv6 ip-prefixes** | Number of IP prefixes referenced in source, destination, and static NAT rules. This total includes the IP prefixes configured directly, as address names, and as address set names in the rule. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security nat source rule r2

```
user@host> show security nat source rule r2

 source NAT rule: r2        Rule-set: src-nat
  Description               : The source rule r2 is for the sales team
  Rule-Id                   : 1
  Rule position             : 1
  From zone                 : zone1
  To zone                   : zone9
  Match
   Source addresses         : add1
                              add2
   Destination addresses    : add9
                              add10
   Destination port         : 1002            - 1002
  Action                       : off
    Persistent NAT type        : N/A
    Persistent NAT mapping type : address-port-mapping
    Inactivity timeout         : 0
    Max session number         : 0
  Translation hits             : 0
```

## Sample Output

### show security nat source rule all

```
user@host> show security nat source rule all
  Total rules: 170
Total referenced IPv4/IPv6 ip-prefixes: 4437/835

source NAT rule: r2                  Rule-set: src-nat
  Description               : The source rule r2 is for the sales team
  Rule-Id                   : 1
  Rule position             : 1
  From zone                 : zone1
  To zone                   : zone9
  Match
    Source addresses        : add1
                              add2
    Destination addresses   : add9
                              add10
     Destination port        : 1002          - 1002
  Action                       : off
    Persistent NAT type        : N/A
    Persistent NAT mapping type : address-port-mapping
    Inactivity timeout         : 0
    Max session number         : 0
  Translation hits             : 0

...
```


Copyright © 2013, Juniper Networks, Inc.

## show security nat source summary

**Syntax**
show security nat source summary
logical-system *logical-system-name*

**Release Information**
Command introduced in Junos OS Release 9.2.

**Description**
Display a summary of Network Address Translation (NAT) source pool information.

**Options**
- none—Display summary information about the source NAT pool.
- **logical-system *logical-system-name***—Display summary information about the source NAT pool for the specified logical system.

**Required Privilege Level**
view

**Related Documentation**
- pool (Security Source NAT) on page 819
- rule (Security Source NAT) on page 900
- Network Address Translation for Security Devices
- Logical Systems for Security Devices

**List of Sample Output**
show security nat source summary on page 2122

**Output Fields**
Table 188 on page 2121 lists the output fields for the **show security nat source summary** command. Output fields are listed in the approximate order in which they appear.

Table 188: show security nat source summary Output Fields

| Field Name | Field Description |
|---|---|
| **Total source nat pool number** | Number of source NAT pools. |
| **Pool name** | Name of the source address pool. |
| **Address range** | IP address or IP address range for the pool. |
| **Routing Instance** | Name of the routing instance. |
| **PAT** | Whether Port Address Translation (PAT) is enabled (yes or no). |
| **Total Address** | Number of IP addresses that are in use. |
| **Total source nat rule number** | Number of source NAT rules. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security nat source summary

```
root@host> show security nat source summary logical-system all

Logical system: root-logical-system
Total port number usage for port translation pool: 67108864
Maximum port number for port translation pool: 134217728

Logical system: lsys1
Total port number usage for port translation pool: 193536
Maximum port number for port translation pool: 134217728
Total pools: 2

Logical system: root-logical-system
Pool              Address                   Routing   PAT   Total
Name              Range                     Instance        Address
pool1             1.1.1.0-1.1.4.255-        default   yes   2048
                  1.1.5.0-1.1.8.255


Logical system: lsys1
Pool              Address                    Routing   PAT   Total
Name              Range                      Instance        Address
pool2             30.1.1.1-30.1.1.3          default   yes   3


Total rules: 1

Logical system: root-logical-system
Rule name         Rule set      From         To             Action
rule 1            ruleset1      ge-2/2/2.0   ge-2/2/3.0     pool1
rule 1                          ge-2/2/4.0   ge-2/2/5.0
```


Copyright © 2013, Juniper Networks, Inc.

## show security nat static rule

**Syntax**

show security nat static rule
*<rule-name>*
*all*
logical-system *logical-system-name*
root-logical-system

**Release Information**

Command introduced in Junos OS Release 9.3. **Description** output field added in Junos OS Release 12.1.

**Description**

Display information about the specified static Network Address Translation (NAT) rule.

**Options**

- ***rule-name*** —Name of the rule.
- **all**—Display information about all the static NAT rules.
- **logical-system *logical-system-name***—Display information about the static NAT rules for the specified logical system.
- **root-logical-system**—Display information about the static NAT rules for the master (root) logical system.

**Required Privilege Level**

view

**Related Documentation**

- rule (Security Static NAT) on page 901
- Network Address Translation for Security Devices
- Logical Systems for Security Devices

**List of Sample Output**

show security nat static rule sta-r2 on page 2125
show security nat static rule all on page 2125

**Output Fields**

Table 189 on page 2123 lists the output fields for the **show security nat static rule** command. Output fields are listed in the approximate order in which they appear.

### Table 189: show security nat static rule Output Fields

| Field Name | Field Description |
|---|---|
| **Static NAT rule** | Name of the static NAT rule. |
| **Rule-set** | Name of the rule set. Currently, you can configure 8 rules within the same rule set. |
| **Description** | Description of the static NAT rule. |
| **Rule-Id** | Rule identification number. |
| **Rule position** | Position of the rule that indicates the order in which it applies to traffic. |
| **From interface** | Name of the interface from which the packets flow. |

Copyright © 2013, Juniper Networks, Inc.

Table 189: show security nat static rule Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **From routing instance** | Name of the routing instance from which the packets flow. |
| **From zone** | Name of the zone from which the packets flow. |
| **Destination addresses** | Name of the destination addresses that match the rule. |
| **Host addresses** | Name of the host addresses that match the rule. |
| **Netmask** | Subnet IP address. |
| **Host routing-instance** | Name of the host routing instance. |
| **Translation hits** | Number of times a translation in the translation table is used for a static NAT rule. |
| **Destination port** | Destination port numbers that match the rule. The default value is any. |
| **Total static-nat rules** | Number of static NAT rules. |
| **Total referenced IPv4/IPv6 ip-prefixes** | Number of IP prefixes referenced in source, destination, and static NAT rules. This total includes the IP prefixes configured directly, as address names, and as address set names in the rule. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security nat static rule sta-r2

```
user@host> show security nat static rule sta-r2

 Static NAT rule: sta-r2               Rule-set: sta-nat
  Description               : The static rule sta-r2 is for the sales team
  Rule-Id                   : 1
  Rule position             : 1
  From zone                 : zone9
  Destination addresses     : add3
  Host addresses            : add4
  Netmask                   : 24
  Host routing-instance     : N/A
  Translation hits          : 0
  Destination port          : 0
  Translation hits          : 0
```

## Sample Output

### show security nat static rule all

```
user@host> show security nat static rule all

Total static-nat rules: 170
Total referenced IPv4/IPv6 ip-prefixes: 170/170

Static NAT rule: sta-r2               Rule-set: sta-nat
  Description               : The static rule sta-r2 is for the sales team
  Rule-Id                   : 1
  Rule position             : 1
  From zone                 : zone9
  Destination addresses     : add3
  Host addresses            : add4
  Netmask                   : 24
  Host routing-instance     : N/A
  Translation hits          : 0

...
```

Copyright © 2013, Juniper Networks, Inc.

## show security pki ca-certificate (View)

**Syntax**

show security pki ca-certificate
<**brief** | **detail**>
<**ca-profile** *ca-profile-name* >

**Release Information**

Command modified in Junos OS Release 8.5. Subject string output field added in Junos OS Release 12.1X44-D10.

**Description**

Display information about the certificate authority (CA) public key infrastructure (PKI) digital certificates configured on the device.

NOTE: The FIPS image does not permit the use of MD5 fingerprints. Therefore, MD5 fingerprints are not included when a certificate is displayed using this command. The SHA-1 fingerprint (that is currently displayed) is retained in the FIPS image. The Simple Certificate Enrollment Protocol (SCEP) is disabled in the FIPS image.

**Options**

- none—Display basic information about all configured CA certificates.
- **brief** | **detail**—(Optional) Display the specified level of output.
- **ca-profile** ***ca-profile-name***- (Optional) Display information about only the specified CA certificate.

**Required Privilege Level**

view

**Related Documentation**

- ca-profile (Security) on page 448
- request security pki ca-certificate verify (Security)

**List of Sample Output**

show security pki ca-certificate ca-profile RootCA brief on page 2128
show security pki ca-certificate ca-profile RootCA detail on page 2128

**Output Fields**

Table 190 on page 2126 lists the output fields for the **show security pki ca-certificate** command. Output fields are listed in the approximate order in which they appear.

### Table 190: show security pki ca-certificate Output Fields

| Field Name | Field Description |
|---|---|
| **Certificate identifier** | Name of the digital certificate. |
| **Certificate version** | Revision number of the digital certificate. |
| **Serial number** | Unique serial number of the digital certificate. |
| **Issued to** | Device that was issued the digital certificate. |


Copyright © 2013, Juniper Networks, Inc.

Table 190: show security pki ca-certificate Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Issued by** | Authority that issued the digital certificate. |
| **Issuer** | Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are:<br>• **Organization**—Organization of origin.<br>• **Organizational unit**—Department within an organization.<br>• **Country**—Country of origin.<br>• **Locality**—Locality of origin.<br>• **Common name**—Name of the authority. |
| **Subject** | Details of the digital certificate holder organized using the distinguished name format. Possible subfields are:<br>• **Organization**—Organization of origin.<br>• **Organizational unit**—Department within an organization.<br>• **Country**—Country of origin.<br>• **Locality**—Locality of origin.<br>• **Common name**—Name of the authority.<br>If the certificate contains multiple subfield entries, all entries are displayed. |
| **Subject string** | Subject field as it appears in the certificate. |
| **Validity** | Time period when the digital certificate is valid. Values are:<br>• **Not before**—Start time when the digital certificate becomes valid.<br>• **Not after**—End time when the digital certificate becomes invalid. |
| **Public key algorithm** | Encryption algorithm used with the private key, such as **rsaEncryption**(**1024 bits**). |
| **Signature algorithm** | Encryption algorithm that the CA used to sign the digital certificate, such as **sha1WithRSAEncryption**. |
| **Fingerprint** | Secure Hash Algorithm (**SHA1**) and Message Digest 5 (**MD5**) hashes used to identify the digital certificate. |
| **Distribution CRL** | Distinguished name information and the URL for the certificate revocation list (CRL) server. |
| **Use for key** | Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Data encipherment**. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security pki ca-certificate ca-profile RootCA brief

```
user@host> show security pki ca-certificate ca-profile RootCA brief
Certificate identifier: RootCA
  Issued to: RootCA, Issued by: C = US, O = Juniper, CN = RootCA
  Validity:
    Not before: 05- 3-2012 07:15
    Not after: 05- 2-2017 07:15
  Public key algorithm: rsaEncryption(1024 bits)
```

## Sample Output

show security pki ca-certificate ca-profile RootCA detail

```
user@host> show security pki ca-certificate ca-profile RootCA detail
Certificate identifier: RootCA
  Certificate version: 3
  Serial number: 0712dc31
  Issuer:
    Organization: Juniper, Country: US, Common name: RootCA
  Subject:
    Organization: Juniper, Country: US, Common name: RootCA
  Subject string:
    C=US, O=Juniper, CN=RootCA
  Validity:
    Not before: 05- 3-2012 07:15
    Not after: 05- 2-2017 07:15
  Public key algorithm: rsaEncryption(1024 bits)
    30:81:89:02:81:81:00:ac:b0:c0:11:ac:0c:34:37:04:97:65:c2:b1
    ae:7e:68:e0:fa:37:23:a1:f0:eb:4d:eb:03:89:c9:d9:0d:34:f3:66
    91:97:8c:e9:9c:d4:b5:55:8d:c1:e2:8b:95:08:9d:29:f8:ab:ac:ff
    ae:af:f7:bc:4b:33:f2:eb:b9:e6:13:6d:18:d7:64:a7:85:78:99:41
    4e:b4:fa:bc:3e:1b:5c:26:25:89:03:af:e9:c6:e9:9e:7b:74:1a:1a
    5b:b4:2a:48:78:57:68:e2:5c:0b:71:71:78:ac:a2:23:5f:ca:d2:4a
    38:4c:35:5a:20:cc:44:39:96:26:20:43:bd:75:fd:02:03:01:00:01
  Signature algorithm: sha1WithRSAEncryption
  Use for key: CRL signing, Certificate signing, Key encipherment,
  Digital signature
  Fingerprint:
    eb:2a:2a:eb:d3:c7:cb:62:65:2e:6a:76:56:b8:af:88:51:8a:30:c9 (sha1)
    cd:43:ae:a4:b2:11:9e:cf:1a:47:fd:7f:0c:ce:d9:fd (md5)
  Auto-re-enrollment:
    Status: Disabled
    Next trigger time: Timer not started
```


Copyright © 2013, Juniper Networks, Inc.

## show security pki certificate-request (View)

**Syntax**
show security pki certificate-request
<**brief** | **detail**>
<certificate-id *certificate-id-name* >

**Release Information**
Command modified in Release 8.5 of Junos OS.

**Description**
Display information about manually generated local digital certificate requests that are stored on the device.

**Options**
- none—Display basic information about all local digital certificate requests.
- **brief** | **detail**—(Optional) Display the specified level of output.
- **certificate-id** ***certificate-id-name*** —(Optional) Display information about only the specified local digital certificate requests.

**Required Privilege Level**
view

**Related Documentation**
- clear security pki key-pair (Local Certificate) on page 1464

**List of Sample Output**
show security pki certificate-request certificate-id hassan brief on page 2130
show security pki certificate-request certificate-id hassan detail on page 2130

**Output Fields**
Table 191 on page 2129 lists the output fields for the **show security pki certificate-request** command. Output fields are listed in the approximate order in which they appear.

### Table 191: show security pki certificate-request Output Fields

| Field Name | Field Description |
|---|---|
| **Certificate identifier** | Name of the digital certificate. |
| **Certificate version** | Revision number of the digital certificate. |
| **Issued to** | Device that was issued the digital certificate. |
| **Subject** | Details of the digital certificate holder organized using the distinguished name format. Possible subfields are:<br>• **Organization**—Organization of origin.<br>• **Organizational unit**—Department within an organization.<br>• **Country**—Country of origin.<br>• **Locality**—Locality of origin.<br>• **Common name**—Name of the authority. |
| **Alternate subject** | Domain name or IP address of the device related to the digital certificate. |
| **Public key algorithm** | Encryption algorithm used with the private key, such as **rsaEncryption**(**1024 bits**). |

Copyright © 2013, Juniper Networks, Inc.

Table 191: show security pki certificate-request Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Public key verification status** | Public key verification status: **Failed** or **Passed**. The **detail** output also provides the verification hash. |
| **Fingerprint** | Secure Hash Algorithm (**SHA1**) and Message Digest 5 (**MD5**) hashes used to identify the digital certificate. |
| **Use for key** | Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Data encipherment**. |

## Sample Output

show security pki certificate-request certificate-id hassan brief

```
user@host> show security pki certificate-request certificate-id hassan brief
Certificate identifier: hassan
      Issued to: hassan@juniper.net
      Public key algorithm: rsaEncryption(1024 bits)
```

## Sample Output

show security pki certificate-request certificate-id hassan detail

```
user@host> show security pki certificate-request certificate-id hassan detail
    Certificate identifier: hassan
      Certificate version: 3
      Subject:
        Organization: juniper, Organizational unit: pepsi, Country: IN,
                      Common name: hassan
      Alternate subject: 102.168.72.124
      Public key algorithm: rsaEncryption(1024 bits)
      Public key verification status: Passed
        c7:a4:fb:e7:8c:4f:31:e7:eb:01:d8:32:65:21:f2:eb:6f:7d:49:1a:c3:9b
        63:47:e2:4f:f6:db:f6:c8:75:dd:e6:ec:0b:35:0a:62:32:45:6b:35:1f:65
        c9:66:b7:40:b2:f9:2a:ab:5b:60:f7:c7:73:36:da:68:25:fc:40:4b:12:3c
        d5:c8:c6:66:f6:10:1e:86:67:a8:95:9b:7f:1c:ae:a7:55:b0:28:95:a7:9a
        a2:24:28:e4:5a:b2:a9:06:7a:69:37:20:15:e1:b6:66:eb:22:b5:b6:77:f6
        65:88:b0:94:2b:91:4b:99:78:4a:e3:56:cc:14:45:d7:97:fd
      Fingerprint:
        8f:22:1a:f2:9f:27:b0:21:6c:da:46:64:31:34:1f:68:42:5a:39:e0 (sha1)
        09:15:11:aa:ea:f9:5a:b5:70:d7:0b:8e:be:a6:d3:cb (md5)
      Use for key: Digital signature
```


Copyright © 2013, Juniper Networks, Inc.

## show security pki crl (View)

**Syntax**
show security pki crl
< **brief** | **detail**>
<ca-profile *ca-profile-name* >

**Release Information**
Command modified in Release 8.5 of Junos OS.

**Description**
Display information about the certificate revocation lists (CRLs) configured on the device.

**Options**
- none—Display basic information about all CRLs.
- **brief** | **detail**—(Optional) Display the specified level of output.
- **ca-profile** *ca-profile-name*- (Optional) Display information about only the specified CA profile.

**Required Privilege Level**
view

**Related Documentation**
- crl (Security) on page 482

**List of Sample Output**
show security pki crl ca-profile ca2 on page 2133
show security pki crl ca-profile ca2 brief on page 2133
show security pki crl ca-profile ca2 detail on page 2133

**Output Fields**
Table 192 on page 2131 lists the output fields for the **show security pki crl** command. Output fields are listed in the approximate order in which they appear.

### Table 192: show security pki crl Output Fields

| Field Name | Field Description |
|---|---|
| **CA profile** | Name of the configured CA profile. |
| **CRL version** | Revision number of the certificate revocation list. |
| **CRL issuer** | Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are:<br>• **emailAddress**—Mail address of the issuing authority.<br>• **C**—Country of origin.<br>• **ST**—State of origin.<br>• **L**—Locality of origin.<br>• **O**—Organization of origin.<br>• **OU**—Department within an organization.<br>• **CN**—Name of the authority. |
| **Effective date** | Date and time the certificate revocation list becomes valid. |

Copyright © 2013, Juniper Networks, Inc.

Table 192: show security pki crl Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Next update** | Date and time the routing platform will download the latest version of the certificate revocation list. |
| **Revocation List** | List of digital certificates that have been revoked before their expiration date. Values are:<br>• **Serial number**—Unique serial number of the digital certificate.<br>• **Revocation date**—Date and time that the digital certificate was revoked. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security pki crl ca-profile ca2

```
user@host> show security pki crl ca-profile ca2
CA profile: ca2
  CRL version: V00000001
  CRL issuer: emailAddress = asaini@juniper.net, C = US, ST = ca, L = sunnyvale,
 O = Juniper networks, OU = SPG QA, CN = 2000-spg-juniper-net
  Effective date: 04-26-2007 18:47
  Next update: 05- 4-2007 07:07
```

## Sample Output

show security pki crl ca-profile ca2 brief

```
user@host> show security pki crl ca-profile ca2 brief
CA profile: ca2
  CRL version: V00000001
  CRL issuer: emailAddress = asaini@juniper.net, C = US, ST = ca, L = sunnyvale,
 O = Juniper networks, OU = SPG QA, CN = 2000-spg-juniper-net
  Effective date: 04-26-2007 18:47
  Next update: 05- 4-2007 07:07
```

## Sample Output

show security pki crl ca-profile ca2 detail

```
user@host> show security pki crl ca-profile ca2 detail
CA profile: ca2
  CRL version: V00000001
  CRL issuer: emailAddress = asaini@juniper.net, C = US, ST = ca, L = sunnyvale,
 O = Juniper networks, OU = SPG QA, CN = 2000-spg-juniper-net
  Effective date: 04-26-2007 18:47
  Next update: 05- 4-2007 07:07
  Revocation List:
    Serial number              Revocation date
    174e6399000000000506       03-16-2007 23:09
    174ef3f3000000000507       03-16-2007 23:09
    17529cd6000000000508       03-16-2007 23:09
    1763ac26000000000509       03-16-2007 23:09
    21904e5700000000050a       03-16-2007 23:09
    2191cf7900000000050b       03-16-2007 23:09
    21f10eb600000000050c       03-16-2007 23:09
    2253ca2a00000000050f       03-16-2007 23:09
    2478939b000000000515       03-16-2007 23:09
    24f35004000000000516       03-16-2007 23:09
    277ddfa8000000000517       03-16-2007 23:09
    277e97bd000000000518       03-16-2007 23:09
    27846a76000000000519       03-16-2007 23:09
    2785176f00000000051a       03-16-2007 23:09
```

Copyright © 2013, Juniper Networks, Inc.

## show security pki local-certificate (View)

**Syntax**

show security pki local-certificate
< **brief** | **detail** >
< certificate-id ***certificate-id-name*** >
<system-generated>

**Release Information**

Command modified in Junos OS Release 9.1. Subject string output field added in Junos OS Release 12.1X44-D10.

**Description**

Display information about the local digital certificates, corresponding public keys, and the automatically generated self-signed certificate configured on the device.

**Options**

- none—Display basic information about all configured local digital certificates, corresponding public keys, and the automatically generated self-signed certificate.
- **brief** | **detail**—(Optional) Display the specified level of output.
- certificate-id ***certificate-id-name*** —(Optional) Display information about only the specified local digital certificates and corresponding public keys.
- **system-generated**—Display information about the automatically generated self-signed certificate.

**Required Privilege Level**

view

**Related Documentation**

- clear security pki local-certificate (Device) on page 1465
- request security pki local-certificate generate-self-signed (Security) on page 1514

**List of Sample Output**

show security pki local-certificate certificate-id hello on page 2136
show security pki local-certificate certificate-id hello detail on page 2136
show security pki local-certificate system-generated on page 2137
show security pki local-certificate system-generated detail on page 2137

**Output Fields**

Table 193 on page 2134 lists the output fields for the **show security pki local-certificate** command. Output fields are listed in the approximate order in which they appear.

### Table 193: show security pki local-certificate Output Fields

| Field Name | Field Description |
|---|---|
| **Certificate identifier** | Name of the digital certificate. |
| **Certificate version** | Revision number of the digital certificate. |
| **Serial number** | Unique serial number of the digital certificate. |
| **Issued to** | Device that was issued the digital certificate. |
| **Issued by** | Authority that issued the digital certificate. |


Copyright © 2013, Juniper Networks, Inc.

Table 193: show security pki local-certificate Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Issuer** | Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are:<br>• **Organization**—Organization of origin.<br>• **Organizational unit**—Department within an organization.<br>• **Country**—Country of origin.<br>• **Locality**—Locality of origin.<br>• **Common name**—Name of the authority. |
| **Subject** | Details of the digital certificate holder organized using the distinguished name format. Possible subfields are:<br>• **Organization**—Organization of origin.<br>• **Organizational unit**—Department within an organization.<br>• **Country**—Country of origin.<br>• **Locality**—Locality of origin.<br>• **Common name**—Name of the authority.<br>If the certificate contains multiple subfield entries, all entries are displayed. |
| **Subject string** | Subject field as it appears in the certificate. |
| **Alternate subject** | Domain name or IP address of the device related to the digital certificate. |
| **Validity** | Time period when the digital certificate is valid. Values are:<br>• **Not before**—Start time when the digital certificate becomes valid.<br>• **Not after**—End time when the digital certificate becomes invalid. |
| **Public key algorithm** | Encryption algorithm used with the private key, such as **rsaEncryption**(**1024 bits**). |
| **Public key verification status** | Public key verification status: **Failed** or **Passed**. The **detail** output also provides the verification hash. |
| **Signature algorithm** | Encryption algorithm that the CA used to sign the digital certificate, such as **sha1WithRSAEncryption**. |
| **Fingerprint** | Secure Hash Algorithm (**SHA1**) and Message Digest 5 (**MD5**) hashes used to identify the digital certificate. |
| **Distribution CRL** | Distinguished name information and URL for the certificate revocation list (**CRL**) server. |
| **Use for key** | Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Data encipherment**. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security pki local-certificate certificate-id hello

```
user@host> show security pki local-certificate certificate-id hello
Certificate identifier: hello
  Issued to: cn1, Issued by: DC = local, DC = demo, CN = spglab-EVERETT-WIN-CA
  Validity:
    Not before: 08- 8-2012 17:02
    Not after: 08- 8-2014 17:02
  Public key algorithm: rsaEncryption(1024 bits)
```

## Sample Output

show security pki local-certificate

```
user@host> show security pki local-certificate certificate-id hello detail
Certificate identifier: hello
  Certificate version: 3
```


Copyright © 2013, Juniper Networks, Inc.

certificate-id hello detail

```
  Serial number: 61ba9da000000000d72e
  Issuer:
    Common name: spglab-EVERETT-WIN-CA,
    Domain component: local, Domain component: demo
  Subject:
    Organization: o1, Organization: o2,
    Organizational unit: ou1, Organizational unit: ou2, Country: US, State: CA,
    Locality: Sunnyvale, Common name: cn1, Common name: cn2,
    Domain component: dc1, Domain component: dc2
  Subject string:
    C=US, DC=dc1, DC=dc2, ST=CA, L=Sunnyvale, O=o1, O=o2, OU=ou1, OU=ou2, CN=cn1,
CN=cn2
  Alternate subject: "ernie@juniper.net", ernie.juniper.net, 10.1.2.3
  Validity:
    Not before: 08- 8-2012 17:02
    Not after: 08- 8-2014 17:02
  Public key algorithm: rsaEncryption(1024 bits)
    30:81:89:02:81:81:00:b4:14:01:d5:4f:79:87:d5:bb:e6:5e:c1:14
    97:da:b4:40:ad:1a:77:3e:ec:2e:68:8e:e4:93:a3:fe:7c:0b:58:af
    e1:20:27:82:ca:8d:6f:f0:97:d1:ad:fe:df:6c:cb:3c:b0:4f:cc:dd
    ac:d8:69:3f:3c:59:b5:2a:c6:83:e8:b3:94:5e:0a:2d:cd:e2:b0:15
    3e:97:a7:8a:4e:fb:59:f7:20:4c:ba:a8:80:3e:ba:be:69:ef:2b:32
    e4:1a:1c:24:53:1b:d5:c3:aa:d4:25:73:96:76:ea:49:d4:da:7e:3e
    0c:c6:6b:22:43:cb:04:84:0d:25:33:07:6b:49:41:02:03:01:00:01
  Signature algorithm: sha1WithRSAEncryption
  Distribution CRL:
    ldap:///CN=spglab-EVERETT-WIN-CA,CN=everett-win,CN=CDP,CN=Public%20Key
%20Services,CN=Services,CN=Configuration,DC=demo,DC=local?certificateRevocationList?base?
objectClass=cRLDistributionPoint
    http://everett-win.spglab.juniper.net/CertEnroll/spglab-EVERETT-WIN-CA.crl
  Use for key: Key encipherment, Digital signature, 1.3.6.1.5.5.8.2.2,
  1.3.6.1.5.5.8.2.2
  Fingerprint:
    76:a8:5f:65:b4:bf:bd:10:d8:56:82:65:ff:0d:04:3a:a5:e9:41:dd (sha1)
    8f:99:a4:15:98:10:4b:b6:1a:3d:81:13:93:2a:ac:e7 (md5)
  Auto-re-enrollment:
    Status: Disabled
    Next trigger time: Timer not started
```

## Sample Output

show security pki local-certificate system-generated

```
user@host> show security pki local-certificate system-generated
Certificate identifier: system-generated
  Issued to: JN10B9390AGB, Issued by: CN = JN10B9390AGB, CN = system generated,
CN = self-signed
  Validity:
    Not before: 10-30-2009 23:02
    Not after: 10-29-2014 23:02
  Public key algorithm: rsaEncryption(1024 bits)
```

## Sample Output

show security pki local-certificate

```
user@host> show security pki local-certificate system-generated detail
Certificate identifier: system-generated
  Certificate version: 3
```

### system-generated detail

```
  Serial number: e90d42ebd14ef954b3e48c2eed5b30fb
  Issuer:
    Common name: JN10B9390AGB, Common name: system generated, Common name:
self-signed
  Subject:
    Common name: JN10B9390AGB, Common name: system generated, Common name:
self-signed
  Subject string:
    CN=JN10B9390AGB, CN=system generated, CN=self-signed
  Validity:
    Not before: 10-30-2009 23:02
    Not after: 10-29-2014 23:02
  Public key algorithm: rsaEncryption(1024 bits)
    30:81:89:02:81:81:00:cb:c8:3f:e6:d3:e5:ca:9d:dc:2d:e9:ca:c7
    5f:b1:f5:3a:f0:1c:a7:55:43:0f:ef:fd:1c:fe:29:09:d5:37:d0:fa
    d6:ee:bc:b8:3f:58:d4:31:fb:96:4f:4f:cc:a9:1a:8f:2e:1b:50:6f
    2b:88:34:74:b2:6d:ad:94:b5:dd:3d:80:87:56:d0:42:50:4d:ac:d7
    8c:21:06:2d:07:1e:f4:d0:c7:85:2e:25:60:ad:1b:b5:b2:d2:1d:c8
    79:67:8c:56:06:04:75:6e:be:4e:99:b8:07:e6:9a:11:fe:b5:ec:c0
    1e:68:da:47:99:1b:b2:c8:07:ab:cd:6e:fe:c1:fd:02:03:01:00:01
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    be:1f:21:13:71:cd:9d:de:7a:41:d7:4c:52:8d:3e:d6:ba:db:75:96 (sha1)
    ba:fc:90:4b:5f:a8:66:a3:b9:64:89:9f:e2:45:b5:84 (md5)
  Auto-re-enrollment:
    Status: Disabled
    Next trigger time: Timer not started
```


Copyright © 2013, Juniper Networks, Inc.

## show security policies

**Syntax**

show security policies
<detail>
<none>
policy-name *policy-name*
<global>

**Release Information**

Command modified in Junos OS Release 9.2. Support for IPv6 addresses added in Junos OS Release 10.2. Support for IPv6 addresses in active/active chassis cluster configurations in addition to the existing support of active/passive chassis cluster configurations added in Junos OS Release 10.4. Support for wildcard addresses added in Junos OS Release 11.1. Support for global policy added in Junos OS Release 11.4. Support for services offloading added in Junos OS Release 11.4. Support for source-identities added in Junos OS Release 12.1. The **Description** output field added in Junos OS Release 12.1.

**Description**

Display a summary of all security policies configured on the device. If a particular policy is specified, display information particular to that policy.

**Options**

- **none**—Display basic information about all configured policies.
- **detail**—(Optional) Display a detailed view of all of the policies configured on the device.
- **policy-name *policy-name***—(Optional) Display information about the specified policy.
- **global**—Display information about global policies.

**Required Privilege Level**

view

**Related Documentation**

- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- clear security policies statistics on page 1467
- UTM for Security Devices
- Security Policies for Security Devices
- Logical Systems for Security Devices

**List of Sample Output**

show security policies on page 2142
show security policies policy-name p1 detail on page 2142
show security policies (services-offload) on page 2143
show security policies detail on page 2143

**Output Fields**

Table 194 on page 2140 lists the output fields for the **show security policies** command. Output fields are listed in the approximate order in which they appear.

Copyright © 2013, Juniper Networks, Inc.

### Table 194: show security policies Output Fields

| Field Name | Field Description |
|---|---|
| **From zone** | Name of the source zone. |
| **To zone** | Name of the destination zone. |
| **Policy** | Name of the applicable policy. |
| **Description** | Description of the applicable policy. |
| **State** | Status of the policy:<br>• **enabled**: The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it.<br>• **disabled**: The policy cannot be used in the policy lookup process, and therefore it is not available for access control. |
| **Index** | An internal number associated with the policy. |
| **Sequence number** | Number of the policy within a given context. For example, three policies that are applicable in a from-zoneA-to-zoneB context might be ordered with sequence numbers 1, 2, and 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, and 4. |
| **Source addresses** | For standard display mode, the names of the source addresses for a policy. Address sets are resolved to their individual names.<br>For detail display mode, the names and corresponding IP addresses of the source addresses for a policy. Address sets are resolved to their individual address name-IP address pairs. |
| **Destination addresses** | Name of the destination address (or address set) as it was entered in the destination zone's address book. A packet's destination address must match this value for the policy to apply to it. |
| **Source identities** | One or more user roles specified for a policy. |
| **Applications** | Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time.<br>• **IP protocol**: The IP protocol used by the application—for example, TCP, UDP, ICMP.<br>• **ALG**: If an ALG is associated with the session, the name of the ALG. Otherwise, 0.<br>• **Inactivity timeout**: Elapsed time without activity after which the application is terminated.<br>• **Source port range**: The low-high source port range for the session application. |
| **Destination Address Translation** | Status of the destination address translation traffic:<br>• drop translated—Drop the packets with translated destination addresses.<br>• drop untranslated—Drop the packets without translated destination addresses. |


Copyright © 2013, Juniper Networks, Inc.

Table 194: show security policies Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Application Firewall** | An application firewall includes the following:<br>• **Rule-set**—Name of the rule set.<br>• **Rule**—Name of the rule.<br>  • **Dynamic applications**—Name of the applications.<br>  • **Dynamic application groups**—Name of the application groups.<br>  • **Action**—The action taken with respect to a packet that matches the application firewall rule set. Actions include the following:<br>  • **permit**<br>  • **deny**<br>• **Default rule**—The default rule applied when the identified application is not specified in any rules of the rule set. |
| **Action or Action-type** | • The action taken in regard to a packet that matches the policy's tuples. Actions include the following:<br>  • **permit**<br>  • **firewall-authentication**<br>  • **tunnel ipsec-vpn** *vpn-name*<br>  • **pair-policy** *pair-policy-name*<br>  • **source-nat pool** *pool-name*<br>  • **pool-set** *pool-set-name*<br>  • **interface**<br>  • **destination-nat** *name*<br>  • **deny**<br>  • **reject**<br>  • **services-offload** |
| **Session log** | Session log entry that indicates whether the **at-create** and **at-close** flags were set at configuration time to log session information. |
| **Scheduler name** | Name of a preconfigured scheduler whose schedule determines when the policy is active (or inactive) to check an incoming packet to determine how to treat the packet. |
| **Policy statistics** | Policy statistics include the following:<br>• **Input bytes**—The number of bytes presented for processing by the device.<br>• **Output bytes**—The number of bytes actually processed by the device.<br>• **Input packets**—The number of packets presented for processing by the device.<br>• **Active sessions**—The number of sessions currently present because of access control lookups that used this policy.<br>• **Session deletions**—The number of sessions deleted since system startup.<br>• **Policy lookups**—Number of times the policy was accessed to check for a match.<br>NOTE: Configure the Policy P1 with the **count** option to display policy statistics. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security policies

```
user@host> show security policies
From zone: trust, To zone: untrust
  Policy: p1, State: enabled, Index: 4, Sequence number: 1
    Source addresses:
    sa-1-ipv4: 2.2.2.0/24
    sa-2-ipv6: 2001:0db8::/32
    sa-3-ipv6: 2001:0db6/24
    sa-4-wc: 192.168.0.11/255.255.0.255
    Destination addresses:
    da-1-ipv4: 2.2.2.0/24
    da-2-ipv6: 2400:0af8::/32
    da-3-ipv6: 2400:0d78:0/24
    da-4-wc: 192.168.22.11/255.255.0.255
    Source identities: role1, role2, role4
    Applications: any
    Action: permit, application services, log, scheduled
    Application firewall : my_ruleset1
  Policy: p2, State: enabled, Index: 5, Sequence number: 2
    Source addresses:
    sa-1-ipv4: 2.2.2.0/24
    sa-2-ipv6: 2001:0db8::/32
    sa-3-ipv6: 2001:0db6/24
    Destination addresses:
    da-1-ipv4: 2.2.2.0/24
    da-2-ipv6: 2400:0af8::/32
    da-3-ipv6: 2400:0d78:0/24
    Source identities: role1, role4
    Applications: any
    Action: deny, scheduled
```

### show security policies policy-name p1 detail

```
user@host> show security policies policy-name p1 detail
Policy: p1, action-type: permit, State: enabled, Index: 4
  Description: The policy p1 is for the sales team
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    sa-1-ipv4: 2.2.2.0/24
    sa-2-ipv6: 2001:0db8::/32
    sa-3-ipv6: 2001:0db6/24
    sa-4-wc: 192.168.0.11/255.255.0.255
  Destination addresses:
    da-1-ipv4: 2.2.2.0/24
    da-2-ipv6: 2400:0af8::/32
    da-3-ipv6: 2400:0d78:0/24
    da-4-wc: 192.168.22.11/255.255.0.255
 Source identities:
  role1
  role2
  role4
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Destination Address Translation: drop translated
  Application firewall :
  Rule-set: my_ruleset1
    Rule: rule1
```


Copyright © 2013, Juniper Networks, Inc.

```
      Dynamic Applications: junos:FACEBOOK, junos:YSMG
      Dynamic Application groups: junos:web, junos:chat
      Action: deny
    Default rule: permit
  Session log: at-create, at-close
  Scheduler name: sch20
  Policy statistics:
    Input  bytes     :               50000                 100 bps
    Output bytes     :               40000                 100 bps
    Input  packets   :                 200                 200 pps
    Output packets   :                 100                 100 pps
    Session rate     :                   2                   1 sps
    Active sessions  :                  11
    Session deletions:                  20
    Policy lookups   :                  12
```

### show security policies (services-offload)

```
user@host> show security policies
Default policy: deny-all
From zone: trust, To zone: untrust
  Policy: p1, State: enabled, Index: 4, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Source identities: role1, role2, role4
    Applications: any
    Action: permit, services-offload, count
From zone: untrust, To zone: trust
  Policy: p2, State: enabled, Index: 5, Scope Policy: 0, Sequence number: 1
    Source addresses: any
    Destination addresses: any
    Source identities: role1, role2, role4
    Applications: any
    Action: permit, services-offload
```

### show security policies detail

```
user@host> show security policies detail
Default policy: deny-all
Policy: p1, action-type: permit, services-offload:enabled , State: enabled, Index:
 4, Scope Policy: 0
  Policy Type: Configured
  Description: The policy p1 is for the sales team
  Sequence number: 1
  From zone: trust, To zone: untrust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
 Source identities:
  role1
  role2
  role4
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
  Policy statistics:
    Input  bytes     :                 500                   0 bps
    Output bytes     :                 408                   0 bps
    Input  packets   :                   8                   0 pps
```

Copyright © 2013, Juniper Networks, Inc.

```
    Output packets   :                    6                    0 pps
    Session rate     :                    3                    0 sps
    Active sessions  :                    1
    Session deletions:                    2
    Policy lookups   :                    3
Policy: p2, action-type: permit, services-offload:enabled , State: enabled, Index:
 5, Scope Policy: 0
  Policy Type: Configured
  Description: The policy p2 is for the sales team
  Sequence number: 1
  From zone: untrust, To zone: trust
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
 Source identities:
  role1
  role2
  role4
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Per policy TCP Options: SYN check: No, SEQ check: No
```


Copyright © 2013, Juniper Networks, Inc.

## show security policies hit-count

**Syntax**

show security policies hit-count
<ascending | descending>
<from-zone *zone-name*>
<greater-than *count*>
<less-than *count*>
<to-zone *zone-name*>

**Release Information**

Command introduced in Junos OS Release 12.1.

**Description**

Display the utility rate of security policies according to the number of hits they receive. The number of hits can be listed without an order or sorted in either ascending or descending order, and they can be restricted to the number of hits that fall above or below a specific count or within a range. Data is shown for all zones associated with the policies or named zones.

Use this command without options to display the number of hits in random order for all security policies and for all zones.

**Options**

- **ascending** | **descending**—(Optional) Display the number of hits for security policies in ascending or descending order.
- **from-zone** ***zone-name***—(Optional) Display the number of hits for security policies associated with the named source zone.
- **greater-than** ***count***—(Optional) Display security policies for which the number of hits is greater than the specified number.

  **Range**: 0 through 4,294,967,295
- **less-than** ***count***—(Optional) Display security policies for which the number of hits is less than the specified number.

  **Range**: 0 through 4,294,967,295
- **to-zone** ***zone-name***—(Optional) Display the number of hits for security policies associated with the named destination zone.

**Required Privilege Level**

view

**Related Documentation**

- clear security policies hit-count on page 1466
- Security Policies for Security Devices

**List of Sample Output**

show security policies hit-count on page 2146
show security policies hit-count ascending on page 2146
show security policies hit-count descending greater-than 70 less-than 100 on page 2146
show security policies hit-count from-zone untrust to-zone trust on page 2146

**Output Fields**

Table 195 on page 2146 lists the output fields for the **show security policies hit-count** command. Output fields are listed in the approximate order in which they appear.

Copyright © 2013, Juniper Networks, Inc.

Table 195: show security policies hit-count Output Fields

| Field Name | Field Description |
|---|---|
| **from-zone** | Name of the source zone. |
| **to-zone** | Name of the destination zone. |
| **policy** | Name of the security policy. |
| **hit-count** | Number of hits for each security policy. |
| **Number of policy** | Number of security policies for which hit counts are displayed. |

## Sample Output

### show security policies hit-count

```
user@host> show security policies hit-count
from-zone   to-zone  policy  hit-count
untrust     vrtrust  u2t1      40
untrust     trust    u2t2      20
untrust     trust    u2t3      80

Number of policy: 3
```

## Sample Output

### show security policies hit-count ascending

```
user@host> show security policies hit-count ascending
from-zone   to-zone  policy  hit-count
untrust     trust    u2t2      20
untrust     vrtrust  u2t1      40
untrust     trust    u2t3      80

Number of policy: 3
```

## Sample Output

### show security policies hit-count descending greater-than 70 less-than 100

```
user@host> show security policies hit-count descending greater-than 70 less-than 100
from-zone   to-zone  policy  hit-count
untrust     trust    u2t2      100
untrust     vrtrust  u2t1      90
untrust     vrtrust  u2t3      80

Number of policy: 3
```

## Sample Output

### show security policies hit-count from-zone untrust to-zone trust

```
user@host> show security policies hit-count from-zone untrust to-zone trust
from-zone   to-zone  policy  hit-count
untrust     trust    u2t2      20
untrust     trust    u2t3      80

Number of policy: 2
```


Copyright © 2013, Juniper Networks, Inc.

## show security resource-manager group active

**Syntax** show security resource-manager group active
*<group-number >*
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Display security information about active groups created through the resource manager.

**Options**

- none—Display resource manager group service information for all active groups.
- ***group-number*** —(Optional) Display resource manager group service information for a specific group identification number.
- **node**—(Optional) For chassis cluster configurations, display active resource manager group service information on a specific node.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level** view

**List of Sample Output**
show security resource-manager group active on page 2148
show security resource-manager group active 2048 on page 2148
show security resource-manager group active node primary on page 2148
show security resource-manager group active node all on page 2148
show security resource-manager group active 1024 node all on page 2148

**Output Fields** Table 196 on page 2147 lists the output fields for the **show security resource-manager group** command. Output fields are listed in the approximate order in which they appear.

### Table 196: show security resource-manager group Output Fields

| Field Name | Field Description |
|---|---|
| **Total groups** | Total number of groups in the system. |
| **active groups** | Number of active groups. |
| **Group ID** | Identification number whose group information is displayed. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security resource-manager group active

```
user@host> show security resource-manager group active
Total groups 32, active groups 0
```

## Sample Output

show security resource-manager group active 2048

```
user@host> show security resource-manager group active 2048
Total groups 2048, active groups 1
Group ID 2048: state - Active
          : Virtual System      - root
          : Application         - SIP ALG
          : Group Timeout       - 65535
          : Number of resources - 3
               Resource ID - 8190
               Resource ID - 8188
               Resource ID - 8187
```

## Sample Output

show security resource-manager group active node primary

```
user@host> show security resource-manager group active node primary
node0:
--------------------------------------------------------------------------------
Group ID 1024: Application - SIP ALG
Total groups 1024, active groups 1
```

## Sample Output

show security resource-manager group active node all

```
user@host> show security resource-manager group active node all
node0:
--------------------------------------------------------------------------------
Group ID 1024: Application - SIP ALG
Total groups 1024, active groups 1
node1:
--------------------------------------------------------------------------------
Group ID 1024: Application - SIP ALG
Total groups 1024, active groups 1
```

## Sample Output

show security resource-manager

```
user@host> show security resource-manager group active 1024 node all
node0:
--------------------------------------------------------------------------------
```


Copyright © 2013, Juniper Networks, Inc.

### group active 1024 node all

```
Group ID 1024: state - Active
          : Application         - SIP ALG
          : Group Timeout       - 65535
          : Number of resources - 3
               Resource ID - 8192
               Resource ID - 8188
               Resource ID - 8187
node1:
--------------------------------------------------------------------------------
Group ID 1024: state - Active
          : Application         - SIP ALG
          : Group Timeout       - 65535
          : Number of resources - 3
               Resource ID - 8187
               Resource ID - 8186
               Resource ID - 8190
```

Copyright © 2013, Juniper Networks, Inc.

## show security resource-manager resource active

**Syntax**
show security resource-manager resource **active**
*<resource-id* >
<node ( *node-id* | all | local | primary)>

**Release Information**
Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description**
Display security information about active resources created through the resource manager.

**Options**
- none—Display information for all active resources.
- ***resource-id*** —(Optional) Display information for a resource with a specific identification number.
- **node**—(Optional) For chassis cluster configurations, display active resource manager information on a specific node.
  - ***node-id*** —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level**
view

**List of Sample Output**
show security resource-manager resource active on page 2151
show security resource-manager resource active 5 on page 2151
show security resource-manager resource active node local on page 2151
show security resource-manager resource active node primary on page 2151

**Output Fields**
Table 197 on page 2150 lists the output fields for the **show security resource-manager resource** command. Output fields are listed in the approximate order in which they appear.

### Table 197: show security resource-manager resource Output Fields

| Field Name | Field Description |
|---|---|
| **Total resources** | Total number of resources in the system. |
| **active resources** | Number of active resources. |
| **Resource ID** | Identification number whose resource information is displayed. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security resource-manager resource active

```
user@host> show security resource-manager resource active
    Resource ID 7: Group ID - 2, Application - JSF_sip

    Resource ID 6: Group ID - 2, Application - JSF_sip

    Resource ID 5: Group ID - 2, Application - JSF_sip

    Resource ID 4: Group ID - 2, Application - JSF_sip

    Resource ID 3: Group ID - 2, Application - JSF_sip

    Resource ID 1: Group ID - 2, Application - JSF_sip

    Resource ID 2: Group ID - 2, Application - JSF_sip
Total Resources 4326, active resources 7
```

## Sample Output

show security resource-manager resource active 5

```
user@host> show security resource-manager resource active 5
Resource ID 5: state - Active
    Application         - asl_client
    Parent group        - 2
    Policy              - 5
    From zone           - untrust
    To zone             - trust
    Resource timeout    - 0
    Number of sessions  - 0
    Number of Holes     - 1
        Source IP range        - {0.0.0.0, 0.0.0.0}
        Source port range      - {0, 0}
        Destination IP range   - {33.1.0.200, 33.1.0.200}
        Destination port range - {5060, 5060}
        Translated             - {0.0.0.0/0 -> 33.1.0.200/5060}
        Protocol               - 17
        Reference count        - 1
```

## Sample Output

show security resource-manager resource active node local

```
user@host> show security resource-manager resource active node local
node0:
--------------------------------------------------------------------------
    Resource ID 8192: Group ID - 1024, Application - SIP ALG
    Resource ID 8188: Group ID - 1024, Application - SIP ALG
    Resource ID 8187: Group ID - 1024, Application - SIP ALG
Total Resources 8192, active resources 3
```

## Sample Output

show security resource-manager

```
user@host> show security resource-manager resource active node primary
node0:
--------------------------------------------------------------------------
```

Copyright © 2013, Juniper Networks, Inc.

resource active node primary

```
    Resource ID 8192: Group ID - 1024, Application - SIP ALG
    Resource ID 8188: Group ID - 1024, Application - SIP ALG
    Resource ID 8187: Group ID - 1024, Application - SIP ALG
Total Resources 8192, active resources 3
```


Copyright © 2013, Juniper Networks, Inc.

## show security resource-manager settings

**Syntax** show security resource-manager settings
<node ( *node-id* | all | local | primary)>

**Release Information** Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description** Display resource manager settings.

**Options** **node**—(Optional) For chassis cluster configurations, display resource manager settings on a specific node.

- ***node-id*** —Identification number of the node. It can be 0 or 1.
- **all**—Display information about all nodes.
- **local**—Display information about the local node.
- **primary**—Display information about the primary node.

**Required Privilege Level** view

**List of Sample Output**
show security resource-manager settings on page 2154
show security resource-manager settings node primary on page 2154
show security resource-manager settings node all on page 2154

**Output Fields** Table 198 on page 2153 lists the output fields for the **show security resource-manager settings** command. Output fields are listed in the approximate order in which they appear.

### Table 198: show security resource-manager settings Output Fields

| Field Name | Field Description |
|---|---|
| **Client Heartbeat** | Time after which idle an resource manager client is timed out. |
| **Count** | Number of active clients. |
| **Pinhole age** | Duration for which the temporary opening in the security firewall (pinhole) is open for specified traffic. If the specified traffic does not exist during this time period, the pinhole is timed out. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security resource-manager settings

```
user@host> show security resource-manager settings
Client Heartbeat: timeout 600 seconds, count 5
Pinhole age: 32 seconds
```

## Sample Output

show security resource-manager settings node primary

```
user@host> show security resource-manager settings node primary
node0:
--------------------------------------------------------------------------
Client heartbeat: timeout 600 seconds, count 5
Pinhole age: 120 seconds
```

## Sample Output

show security resource-manager settings node all

```
user@host> show security resource-manager settings node all
node0:
--------------------------------------------------------------------------
Client heartbeat: timeout 600 seconds, count 5
Pinhole age: 120 seconds
node1:
--------------------------------------------------------------------------
Client heartbeat: timeout 600 seconds, count 5
Pinhole age: 120 seconds
```


Copyright © 2013, Juniper Networks, Inc.

## show security resource-manager summary

**Syntax** show security resource-manager summary

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Display summary information about active resources, clients, groups, and sessions created through the resource manager.

**Required Privilege Level** view

**List of Sample Output** show security resource-manager summary on page 2155

**Output Fields** Table 199 on page 2155 lists the output fields for the **show security resource-manager summary** command. Output fields are listed in the approximate order in which they appear.

### Table 199: show security resource-manager summary Output Fields

| Field Name | Field Description |
|---|---|
| **Active resource-manager clients** | Number of active resource manager clients. |
| **Active resource-manager groups** | Number of active resource manager groups. |
| **Active resource-manager resources** | Number of active resource manager resources. |
| **Active resource-manager sessions** | Number of active resource manager sessions. |

### Sample Output

show security resource-manager summary

```
user@host> show security resource-manager summary

Active resource-manager clients   : 15
Active resource-manager groups    : 1
Active resource-manager resources : 1
Active resource-manager sessions  : 0
```

Copyright © 2013, Juniper Networks, Inc.

## show security screen ids-option

**Syntax**

show security screen ids-option
screen-name
<node ( *node-id* | all | local | primary)>

**Release Information**

Command introduced in Release 8.5 of Junos OS; **node** options added in Release 9.0 of Junos OS.

**Description**

Display configuration information about the specified security screen.

**Options**

- *screen-name* —Name of the screen.
- **node**—(Optional) For chassis cluster configurations, display the configuration status of the security screen on a specific node.
  - *node-id* —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

**Required Privilege Level**

view

**Related Documentation**

- ids-option on page 661

**List of Sample Output**

show security screen ids-option jscreen on page 2158
show security screen ids-option jscreen1 node all on page 2158

**Output Fields**

Table 200 on page 2156 lists the output fields for the **show security screen ids-option** command. Output fields are listed in the approximate order in which they appear.

### Table 200: show security screen ids-option Output Fields

| Field Name | Field Description |
|---|---|
| **TCP address sweep threshold** | Number of microseconds for which the device accepts 10 TCP packets from the same remote source to different destination addresses. |
| **TCP port scan threshold** | Number of microseconds during which the device accepts packets from the same remote source with up to 10 different port numbers. |
| **ICMP address sweep threshold** | Maximum number of microseconds during which up to 10 ICMP echo requests from the same host are allowed into the device. |
| **UDP flood threshold** | Number of UDP packets per second allowed to ping the same destination address before the device rejects further UDP packets. |
| **TCP winnuke** | Enable or disable the detection of TCP WinNuke attacks. |


Copyright © 2013, Juniper Networks, Inc.

Table 200: show security screen ids-option Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **TCP SYN flood attack threshold** | Number of SYN packets per second required to trigger the SYN proxy response. |
| **TCP SYN flood alarm threshold** | Number of half-complete proxy connections per second at which the device makes entries in the event alarm log. |
| **TCP SYN flood source threshold** | Number of SYN segments to be received per second before the device begins dropping connection requests. |
| **TCP SYN flood destination threshold** | Number of SYN segments received per second before the device begins dropping connection requests. |
| **TCP SYN flood timeout** | Maximum length of time before a half-completed connection is dropped from the queue. |
| **TCP SYN flood queue size** | Number of proxy connection requests that can be held in the proxy connection queue before the device begins rejecting new connection requests. |
| **ICMP large packet** | Enable or disable the detection of any ICMP frame with an IP length greater than 1024 bytes. |
| **UDP address sweep threshold** | Number of microseconds for which the device accepts 10 UDP packets from the same remote source to different destination addresses. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show security screen ids-option jscreen

```
user@host> show security screen ids-option jscreen
Screen object status:
Name                                        Value
  TCP port scan threshold                   5000
  ICMP address sweep threshold              5000
```

## Sample Output

### show security screen ids-option jscreen1 node all

```
user@host>  show security screen ids-option jscreen1 node all
node0:
--------------------------------------------------------------------------
Screen object status:
Name                                        Value
  UDP flood threshold                       1000
  TCP winnuke                               enabled
  TCP SYN flood attack threshold            200
  TCP SYN flood alarm threshold             512
  TCP SYN flood source threshold            4000
  TCP SYN flood destination threshold       4000
  TCP SYN flood timeout                     20
  TCP SYN flood queue size                  1024
  ICMP large packet                         enabled
node1:
--------------------------------------------------------------------------
Screen object status:
Name                                        Value
  UDP flood threshold                       1000
  TCP winnuke                               enabled
  TCP SYN flood attack threshold            200
  TCP SYN flood alarm threshold             512
  TCP SYN flood source threshold            4000
  TCP SYN flood destination threshold       4000
  TCP SYN flood timeout                     20
  TCP SYN flood queue size                  1024
  ICMP large packet                         enabled
```


Copyright © 2013, Juniper Networks, Inc.

## show security screen statistics

**Syntax**

show security screen statistics (zone *zone-name* | interface *interface-name*)
<logical-system (*logical-system-name* | all)>
<node (*node-id* | all | local | primary)>
<root-logical-system>

**Release Information**

Command introduced in Release 8.5 of Junos OS. **node** options added in Release 9.0 of Junos OS. **logical-system all** option added in Release 11.2R6 of Junos OS.

**Description**

Display intrusion detection service (IDS) security screen statistics.

**Options**

- **zone** ***zone-name*** —Display screen statistics for this security zone.
- **interface** *interface-name*—Display screen statistics for this interface.
- **logical-system**—(Optional) Display screen statistics for configured logical systems.
  - ***logical-system-name***—Display screen statistics for the named logical system.
  - **all**—Display screen statistics for all logical systems, including the master (root) logical system.
- **node**—(Optional) For chassis cluster configurations, display screen statistics on a specific node.
  - ***node-id*** —Identification number of a node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.
- **root-logical-system**—(Optional) Display screen statistics for the master logical system only.

**Required Privilege Level**

view

**Related Documentation**

- clear security screen statistics on page 1468
- clear security screen statistics interface on page 1469
- clear security screen statistics zone on page 1470
- Logical Systems for Security Devices

**List of Sample Output**

show security screen statistics zone scrzone on page 2162
show security screen statistics interface ge-0/0/3 on page 2162
show security screen statistics interface ge-0/0/1 node primary on page 2163
show security screen statistics zone trust logical-system all on page 2163

**Output Fields**

Table 201 on page 2160 lists the output fields for the **show security screen statistics** command. Output fields are listed in the approximate order in which they appear.

Copyright © 2013, Juniper Networks, Inc.

### Table 201: show security screen statistics Output Fields

| Field Name | Field Description |
|---|---|
| **ICMP flood** | Internet Control Message Protocol (ICMP) flood counter. An ICMP flood typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed. |
| **UDP flood** | User Datagram Protocol (UDP) flood counter. UDP flooding occurs when an attacker sends IP packets containing UDP datagrams with the purpose of slowing down the resources, such that valid connections can no longer be handled. |
| **TCP winnuke** | Number of Transport Control Protocol (TCP) WinNuke attacks. WinNuke is a denial-of-service (DoS) attack targeting any computer on the Internet running Windows. |
| **TCP port scan** | Number of TCP port scans. The purpose of this attack is to scan the available services in the hopes that at least one port will respond, thus identifying a service to target. |
| **ICMP address sweep** | Number of ICMP address sweeps. An IP address sweep can occur with the intent of triggering responses from active hosts. |
| **IP tear drop** | Number of tear drop attacks. Tear drop attacks exploit the reassembly of fragmented IP packets. |
| **TCP SYN flood** | Number of TCP SYN attacks. |
| **IP spoofing** | Number of IP spoofs. IP spoofing occurs when an invalid source address is inserted in the packet header to make the packet appear to come from a trusted source. |
| **ICMP ping of death** | ICMP ping of death counter. Ping of death occurs when IP packets are sent that exceed the maximum legal length (65,535 bytes). |
| **IP source route option** | Number of IP source route attacks. |
| **TCP address sweep** | Number of TCP address sweeps. |
| **TCP land attack** | Number of land attacks. Land attacks occur when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address. |
| **TCP SYN fragment** | Number of TCP SYN fragments. |
| **TCP no flag** | Number of TCP headers without flags set. A normal TCP segment header has at least one control flag set. |
| **IP unknown protocol** | Number of IPs. |
| **IP bad options** | Number of invalid options. |
| **IP record route option** | Number of packets with the IP record route option enabled. This option records the IP addresses of the network devices along the path that the IP packet travels. |


Copyright © 2013, Juniper Networks, Inc.

Table 201: show security screen statistics Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **IP timestamp option** | Number of IP timestamp option attacks. This option records the time (in Universal Time) when each network device receives the packet during its trip from the point of origin to its destination. |
| **IP security option** | Number of IP security option attacks. |
| **IP loose source route option** | Number of IP loose source route option attacks. This option specifies a partial route list for a packet to take on its journey from source to destination. |
| **IP strict source route option** | Number of IP strict source route option attacks. This option specifies the complete route list for a packet to take on its journey from source to destination. |
| **IP stream option** | Number of stream option attacks. This option provides a way for the 16-bit SATNET stream identifier to be carried through networks that do not support streams. |
| **ICMP fragment** | Number of ICMP fragments. Because ICMP packets contain very short messages, there is no legitimate reason for ICMP packets to be fragmented. If an ICMP packet is so large that it must be fragmented, something is amiss. |
| **ICMP large packet** | Number of large ICMP packets. |
| **TCP SYN FIN** | Number of TCP SYN FIN packets. |
| **TCP FIN no ACK** | Number of TCP FIN flags without the acknowledge (ACK) flag. |
| **Source session limit** | Number of concurrent sessions that can be initiated from a source IP address. |
| **TCP SYN-ACK-ACK proxy** | Number of TCP flags enabled with SYN-ACK-ACK. To prevent flooding with SYN-ACK-ACK sessions, you can enable the SYN-ACK-ACK proxy protection screen option. After the number of connections from the same IP address reaches the SYN-ACK-ACK proxy threshold, J Series and SRX Series devices running Junos OS reject further connection requests from that IP address. |
| **IP block fragment** | Number of IP block fragments. |
| **Destination session limit** | Number of concurrent sessions that can be directed to a single destination IP address. |
| **UDP address sweep** | Number of UDP address sweeps. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security screen statistics zone scrzone

```
user@host> show security screen statistics zone scrzone
Screen statistics:
IDS attack type                          Statistics
  ICMP flood                             0
  UDP flood                              0
  TCP winnuke                            0
  TCP port scan                          91
  ICMP address sweep                     0
  TCP sweep                              0
  UDP sweep                              0
  IP tear drop                           0
  TCP SYN flood                          0
  IP spoofing                            0
  ICMP ping of death                     0
  IP source route option                 0
  TCP land attack                        0
  TCP SYN fragment                       0
  TCP no flag                            0
  IP unknown protocol                    0
  IP bad options                         0
  IP record route option                 0
  IP timestamp option                    0
  IP security option                     0
  IP loose source route option           0
  IP strict source route option          0
  IP stream option                       0
  ICMP fragment                          0
  ICMP large packet                      0
  TCP SYN FIN                            0
  TCP FIN no ACK                         0
  Source session limit                   0
  TCP SYN-ACK-ACK proxy                  0
  IP block fragment                      0
  Destination session limit              0
```

## Sample Output

show security screen statistics interface ge-0/0/3

```
user@host> show security screen statistics interface ge-0/0/3
Screen statistics:
IDS attack type                          Statistics
  ICMP flood                             0
  UDP flood                              0
  TCP winnuke                            0
  TCP port scan                          91
  ICMP address sweep                     0
  TCP sweep                              0
  UDP sweep                              0
  IP tear drop                           0
  TCP SYN flood                          0
  IP spoofing                            0
  ICMP ping of death                     0
  IP source route option                 0
  TCP land attack                        0
  TCP SYN fragment                       0
  TCP no flag                            0
  IP unknown protocol                    0
  IP bad options                         0
```


Copyright © 2013, Juniper Networks, Inc.

```
  IP record route option                  0
  IP timestamp option                     0
  IP security option                      0
  IP loose source route option            0
  IP strict source route option           0
  IP stream option                        0
  ICMP fragment                           0
  ICMP large packet                       0
  TCP SYN FIN                             0
  TCP FIN no ACK                          0
  Source session limit                    0
  TCP SYN-ACK-ACK proxy                   0
  IP block fragment                       0
  Destination session limit               0
```

## Sample Output

### show security screen statistics interface ge-0/0/1 node primary

```
user@host> show security screen statistics interface ge-0/0/1 node primary
node0:
--------------------------------------------------------------------------
Screen statistics:
IDS attack type                         Statistics
  ICMP flood                            1
  UDP flood                             1
  TCP winnuke                           1
  TCP port scan                         1
  ICMP address sweep                    1
  TCP sweep                             1
  UDP sweep                             1
  IP tear drop                          1
  TCP SYN flood                         1
  IP spoofing                           1
  ICMP ping of death                    1
  IP source route option                1
  TCP land attack                       1
  TCP SYN fragment                      1
  TCP no flag                           1
  IP unknown protocol                   1
  IP bad options                        1
  IP record route option                1
  IP timestamp option                   1
  IP security option                    1
  IP loose source route option          1
  IP strict source route option         1
  IP stream option                      1
  ICMP fragment                         1
  ICMP large packet                     1
  TCP SYN FIN                           1
  TCP FIN no ACK                        1
  Source session limit                  1
  TCP SYN-ACK-ACK proxy                 1
  IP block fragment                     1
  Destination session limit             1
```

## Sample Output

### show security screen statistics zone trust logical-system all

```
user@host> show security screen statistics zone trust logical-system all
Logical system: root-logical-system
Screen statistics:
```

```
IDS attack type                          Statistics
  ICMP flood                             0
  UDP flood                              0
  TCP winnuke                            0
  TCP port scan                          0
  ICMP address sweep                     0
  TCP sweep                              0
  UDP sweep                              0
  IP tear drop                           0
  TCP SYN flood                          0
  IP spoofing                            0
  ICMP ping of death                     0
  IP source route option                 0
  TCP land attack                        0
  TCP SYN fragment                       0
  TCP no flag                            0
  IP unknown protocol                    0
  IP bad options                         0
  IP record route option                 0
  IP timestamp option                    0
  IP security option                     0
  IP loose source route option           0
  IP strict source route option          0
  IP stream option                       0
  ICMP fragment                          0
  ICMP large packet                      0
  TCP SYN FIN                            0
  TCP FIN no ACK                         0
  Source session limit                   0
  TCP SYN-ACK-ACK proxy                  0
  IP block fragment                      0
  Destination session limit              0

Logical system: ls1
Screen statistics:

IDS attack type                          Statistics
  ICMP flood                             0
  UDP flood                              0
  TCP winnuke                            0
  TCP port scan                          0
  ICMP address sweep                     0
  TCP sweep                              0
  UDP sweep                              0
  IP tear drop                           0
  TCP SYN flood                          0
  IP spoofing                            0
  ICMP ping of death                     0
  IP source route option                 0
  TCP land attack                        0
  TCP SYN fragment                       0
  TCP no flag                            0
  IP unknown protocol                    0
  IP bad options                         0
  IP record route option                 0
  IP timestamp option                    0
  IP security option                     0
  IP loose source route option           0
  IP strict source route option          0
  IP stream option                       0
  ICMP fragment                          0
```


Copyright © 2013, Juniper Networks, Inc.

```
  ICMP large packet                       0
  TCP SYN FIN                             0
  TCP FIN no ACK                          0
  Source session limit                    0
  TCP SYN-ACK-ACK proxy                   0
  IP block fragment                       0
  Destination session limit               0

Logical system: ls2
Screen statistics:

IDS attack type                           Statistics
  ICMP flood                              0
  UDP flood                               0
  TCP winnuke                             0
  TCP port scan                           0
  ICMP address sweep                      0
  TCP sweep                               0
  UDP sweep                               0
  IP tear drop                            0
  TCP SYN flood                           0
  IP spoofing                             0
  ICMP ping of death                      0
  IP source route option                  0
  TCP land attack                         0
  TCP SYN fragment                        0
  TCP no flag                             0
  IP unknown protocol                     0
  IP bad options                          0
  IP record route option                  0
  IP timestamp option                     0
  IP security option                      0
  IP loose source route option            0
  IP strict source route option           0
  IP stream option                        0
  ICMP fragment                           0
  ICMP large packet                       0
  TCP SYN FIN                             0
  TCP FIN no ACK                          0
  Source session limit                    0
  TCP SYN-ACK-ACK proxy                   0
  IP block fragment                       0
  Destination session limit               0
```

Copyright © 2013, Juniper Networks, Inc.

## show security shadow-policies logical-system

**Syntax** show security shadow-policies logical-system *lsys-name* [from-zone *from-zone-name* to-zone *to-zone-name* policy *policy-name* reverse | global policy *policy-name* reverse ]

**Release Information** Command introduced in Junos OS Release 12.1X44-D10.

**Description** Display the shadowing and shadowed policies in a policy list.

**Required Privilege Level** view

**Related Documentation**
- show security policies on page 2139

**List of Sample Output**
show security shadow-policies from-zone zone-a to-zone zone-b on page 2166
show security shadow-policies from-zone zone-a to-zone zone-b policy P1 on page 2166
show security shadow-policies from-zone zone-a to-zone zone-b policy P4 reverse on page 2166

**Output Fields** Table 202 on page 2166 lists the output fields for the **show security shadow-policies logical-system** command. Output fields are listed in the approximate order in which they appear.

Table 202: show security shadow-policies logical-system Output Fields

| Field Name | Field Description |
|---|---|
| **Policies** | The policies shadowing one or more policies in the policy list. |
| **Shadowed policies** | The policies shadowed by one or more policies in the policy list. |

### Sample Output

show security shadow-policies from-zone zone-a to-zone zone-b

```
root@host> show security shadow-policies from-zone zone-a to-zone zone-b
    Policies              Shadowed policies
    P1                    P3
    P1                    P4
    P2                    P5
```

show security shadow-policies from-zone zone-a to-zone zone-b policy P1

```
root@host> show security shadow-policies from-zone zone-a to-zone zone-b policy P1
   Policies              Shadowed policies
    P1                    P3
    P1                    P4
```

show security shadow-policies from-zone zone-a

```
root@host> show security shadow-policies from-zone zone-a to-zone zone-b policy P4 reverse
   Policies              Shadowed policies
    P1                    P4
```


Copyright © 2013, Juniper Networks, Inc.

to-zone zone-b policy
P4 reverse

Copyright © 2013, Juniper Networks, Inc.

## show security softwires

**Syntax** show security softwires <softwire-name *softwire-name*>
<logical-system (all | *logical-system-name*)>

**Release Information** Command introduced in Release 10.4 of Junos OS. The **logical-system** option introduced in Release 12.1 of Junos OS.

**Description** Display a summary of information of all the softwire concentrators and details on concentrators with specified name.

**Options** **softwire-name *softwire-name***—Display the details of the specified softwire concentrator.

**logical-system (all | *logical-system-name*)**—Display softwire information for all logical systems or for a specified logical system. This option is only available to the master administrator.

**Required Privilege Level** view

**Related Documentation**
- Logical Systems for Security Devices

### Sample Output

```
user@host> show security softwires
Software Name            SC Address         Status   Number of SI connected
  SC-CSSI-1                 3001::1          Connected      2
  SC-CSSI-str00             3100::1          Active         0
  SC-CSSI-str01             3101::1          Inactive       0
  SC-CSSI-str02             3001::1          Connected      2520
```

```
user@host> show security softwires softwire-name SC-CSSI-1
Name of softwire: SC-CSSI-1
   SC status: Connected
   SC address: 3001::1
   Zone: trust
   VR ID: 0
 SI Address               SI Status                  SPU
 3001::2                  Active                     spu-1
 3001::2                  Active                     spu-21
 SI number: 2
```

```
user@host> show security softwires logical-system ls-product-design
Software Name            SC Address         Status   Number of SI connected
  sc_1                      3000::1         Connected      1
```


Copyright © 2013, Juniper Networks, Inc.

## show security user-identification local-authentication-table

**Syntax** show security user-identification local-authentication-table [ ( all [brief | extensive])
|ip-address *ip-address* | role *role-name* | start *value* | count *value* | user *user-name*]

**Release Information** Command introduced in release 12.1 of Junos OS.

**Description** This command displays the content of the local authentication table by IP address.

all—(Optional) All entries displayed from the beginning of the table or from the specified starting entry.

brief—(Default) Uses a tabular format and truncates longer entries:
username—displays up to 13 characters, roles—displays up to 32 characters.

extensive—(Optional) Displays the full names and all items.

count *value*—(Optional) The total number of entries to display.

ip-address *ip-address*—(Optional) The IP address of the entry to display.

role *role-name*—(Optional) The role name of the entries to display.

start *value*—(Optional) The first entry to display.

user *user-name*—(Optional) The user name of the entry to display.

**Required Privilege Level** view

**Related Documentation**
- request security user-identification local-authorization-table add on page 1519
- Understanding the User Identification Table

**List of Sample Output**
show security user-identification local-authentication-table all on page 2170
show security user-identification local-authentication-table ip-address on page 2170
show security user-identification local-authentication-table start on page 2170
show security user-identification local-authentication-table role on page 2170

**Output Fields** Table 203 on page 2169 lists the output fields for the **show security user-identification local-authentication-table** command. Output fields are listed in the approximate order in which they appear.

### Table 203: show security user-identification local-authentication-table Output Fields

| Field Name | Field Description |
|---|---|
| **Total entries** | The number of entries in the table. |
| **IP address** | IP address of the associated user.<br>NOTE: Only one user can be associated with an IP address. |
| **Username** | User associated with the specified IP address. |

Copyright © 2013, Juniper Networks, Inc.

Table 203: show security user-identification local-authentication-table Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Roles** | A comma-separated list of all roles associated with this IP address and user. |

## Sample Output

**show security user-identification local-authentication-table all**

```
user@host> show security user-identification local-authentication-table all
Total entries: 3
Source IP       Username     Roles
1.1.1.1         user1        role1
2.2.2.2         user1        role2
3.3.3.3         user3        role1, role2
```

**show security user-identification local-authentication-table ip-address**

```
user@host> show security user-identification local-authentication-table ip-address 2.2.2.2
Ip-address: 2.2.2.2
    Username: user2
    Roles: role2, role3, role1
```

**show security user-identification local-authentication-table start**

```
user@host> show security user-identification local-authentication-table start 2 count 2
Total entries: 2
    Ip-address: 2.2.2.2
    Username: user2
    Roles: role2, role3, role1

    Ip-address: 3.3.3.3
    Username: user3
    Roles: role2, role3
```

**show security user-identification local-authentication-table role**

```
user@host> show security user-identification local-authentication-table role qa3456
Total entries: 3
    Ip-address: 2.2.2.2
    Username: dev-grp-3
    Roles: qa432, qa3456, qa84, qa794

    Ip-address: 3.3.3.3
    Username: dev-qa
    Roles: qa3456, qa3985, qa23

    Ip-address: 2.2.2.2
    Username: brandall
    Roles: qa3456
```


Copyright © 2013, Juniper Networks, Inc.

## show security user-identification role-provision all

**Syntax** show security user-identification role-provision all

**Release Information** Command introduced in Release 12.1 of Junos OS.

**Description** Display all the available user roles for policy provisioning. The output combines user roles from all available UITs.

**Required Privilege Level** view

**Related Documentation**
- Security Policies for Security Devices
- show security user-identification user-provision all on page 2173
- show security user-identification source-identity-provision all on page 2172

**List of Sample Output** show security user-identification role-provision all on page 2171

**Output Fields** Table 204 on page 2171 lists the output fields for the **show security user-identification role-provision all** command. Output fields are listed in the approximate order in which they appear.

Table 204: show security user-identification role-provision all Output Fields

| Field Name | Field Description |
|---|---|
| Roles | A comma-separated list of all user roles available for provisioning in user role policies. This list combines user roles from both the local authentication table and any UAC authentication tables that have been configured. |

### Sample Output

show security user-identification role-provision all

```
user@host> show security user-identification role-provision all
Roles: role1, role2, role3, role4, role_0_1, role_1_1
```

Copyright © 2013, Juniper Networks, Inc.

## show security user-identification source-identity-provision all

**Syntax** show security user-identification source-identity-provision all

**Release Information** Command introduced in Release 12.1X44-D10 of Junos OS.

**Description** Display the available source identities for policy provisioning. The output combines users and user roles from all available UITs.

**Required Privilege Level** view

**Related Documentation**

- Security Policies for Security Devices
- show security user-identification role-provision all on page 2171
- show security user-identification user-provision all on page 2173

**List of Sample Output** show security user-identification source-identity-provision all on page 2172

**Output Fields** Table 205 on page 2172 lists the output fields for the **show security user-identification source-identity-provision all** command. Output fields are listed in the approximate order in which they appear.

Table 205: show security user-identification source-identity-provision all Output Fields

| Field Name | Field Description |
|---|---|
| Source identities | A comma-separated list of all users and user roles available for policy provisioning. This list combines users and user roles from both the local authentication table and any UAC authentication tables that have been configured. |

### Sample Output

show security user-identification source-identity-provision all

```
user@host> show security user-identification source-identity-provision all
Source identities: ariana, ben, guest5, role1, role2, role3, role4, role_0_1,
role_1_1,u1, user2
```


Copyright © 2013, Juniper Networks, Inc.

## show security user-identification user-provision all

**Syntax** show security user-identification user-provision all

**Release Information** Command introduced in Release 12.1X44-D10 of Junos OS.

**Description** Display the available user names for policy provisioning. The output combines users from all available UITs.

**Required Privilege Level** view

**Related Documentation**
- Security Policies for Security Devices
- show security user-identification role-provision all on page 2171
- show security user-identification source-identity-provision all on page 2172

**List of Sample Output** show security user-identification user-provision all on page 2173

**Output Fields** Table 206 on page 2173 lists the output fields for the **show security user-identification user-provision all** command. Output fields are listed in the approximate order in which they appear.

Table 206: show security user-identification user-provision all Output Fields

| Field Name | Field Description |
|---|---|
| Users | A comma-separated list of all users available for policy provisioning. This list combines users from both the local authentication table and any UAC authentication tables that have been configured. |

### Sample Output

show security user-identification user-provision all

```
user@host> show security user-identification user-provision all
Users: ariana, ben, guest5, u1 user2, ...
```

Copyright © 2013, Juniper Networks, Inc.

## show security utm anti-spam statistics

**Syntax** show security utm anti-spam statistics

**Release Information** Command introduced in Release 9.5 of Junos OS.
Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Display antispam statistics for connections including total e-mail scanned, tagged, and dropped connections.

Statistics from both the nodes (with full chassis cluster support for UTM) is displayed.

**Required Privilege Level** view

**Related Documentation**

- clear security utm anti-spam statistics on page 1472
- show security utm anti-spam status on page 2175
- UTM for Security Devices

**Output Fields** show security utm anti-spam statistics

Output fields are listed in the approximate order in which they appear.

## show security utm anti-spam statistics

```
user@host> show security utm anti-spam statistics
Total connections:     0
Denied connections:    0
Total greetings:       0
Denied greetings:      0
Total e-mail scanned:  0
White list hit:        0
Black list hit:        0
Spam total:            0
Spam tagged:           0
Spam dropped:          0
DNS errors:            0
Timeout errors:        0
Return errors:         0
Invalid parameter errors: 0
```


Copyright © 2013, Juniper Networks, Inc.

## show security utm anti-spam status

**Syntax** show security utm anti-spam status

**Release Information** Command introduced in Release 9.5 of Junos OS.
Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Display antispam status for connections including whitelist and blacklist server information. Status of both the nodes (with full chassis cluster support for UTM) is displayed.

**Required Privilege Level** view

**Related Documentation**

- clear security utm anti-spam statistics on page 1472
- show security utm anti-spam statistics on page 2174
- UTM for Security Devices

**Output Fields** show security utm anti-spam status

Output fields are listed in the approximate order in which they appear.

## show security utm anti-spam status

```
user@host> show security utm anti-spam status
SBL Whitelist Server:
SBL Blacklist Server:
    msgsecurity.juniper.net

DNS Server:
    Primary  :     1.2.3.4, Src Interface: ge-0/0/0
    Secondary:     0.0.0.0, Src Interface: ge-0/0/1
    Ternary  :     0.0.0.0, Src Interface: fe-0/0/2
```

Copyright © 2013, Juniper Networks, Inc.

## show security utm anti-virus statistics

**Syntax** show security utm anti-virus statistics

**Release Information** Command introduced in Release 9.5 of Junos OS. Support for Sophos Antivirus added in Release 11.1 of Junos OS.
Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Display antivirus statistics for connections including clean and infected files and scan engine status. Statistics from both the nodes (with full chassis cluster support for UTM) is displayed.

**Required Privilege Level** view

**Related Documentation**

- clear security utm antivirus statistics on page 1473
- show security utm anti-virus status on page 2178
- request security utm anti-virus juniper-express-engine on page 1522
- request security utm anti-virus kaspersky-lab-engine on page 1523
- UTM for Security Devices
- Unified Threat Management

**Output Fields** show security utm anti-virus statistics

Output fields are listed in the approximate order in which they appear.


Copyright © 2013, Juniper Networks, Inc.

## show security utm anti-virus statistics

```
user@host>show security utm anti-virus statistics
Intelligent-prescreening passed:      0
 MIME-whitelist passed:                0
 URL-whitelist passed:                 0
 Forwarded to scan engine:             0

Scan Mode:
     scan-all:                         0
     Scan-extension:                   0

 Scan Code:
     clear:                            0
     Infected:                         0
     Password files                    0
     Decompress layers:                0
     Corrupt files:                    0
     Out of resources:                 0
     Internal errors:                  0

 Fall back:           log-and-permit     block
     Engine not ready:            0              0
     Password file:               0              0
     Decompress layer:            0              0
     Corrupt files:               0              0
     Out of resources:            0              0
     Timeout:                     0              0
     Maximum content size:        0              0
     Too many requests:           0              0
     Others:                      0              0
```

Copyright © 2013, Juniper Networks, Inc.

## show security utm anti-virus status

**Syntax** show security utm anti-virus status

**Release Information** Command introduced in Release 9.5 of Junos OS.
Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Display antivirus status for connections including clean and infected files and scan engine status. Status of both the nodes (with full chassis cluster support for UTM) is displayed.

**Required Privilege Level** view

**Related Documentation**

- clear security utm antivirus statistics on page 1473
- show security utm anti-virus statistics on page 2176
- request security utm anti-virus juniper-express-engine on page 1522
- request security utm anti-virus kaspersky-lab-engine on page 1523
- UTM for Security Devices
- Unified Threat Management

**Output Fields** show security utm anti-virus status

Output fields are listed in the approximate order in which they appear.


Copyright © 2013, Juniper Networks, Inc.

## show security utm anti-virus status

```
user@host> show security utm anti-virus status
Anti-virus key expire date: 2010-07-30
    Update server: http://update.juniper-updates.net/EAV/SRX210/
           Interval: 1440 minutes
           Pattern update status: next update in 922 minutes
           Last result: download catalog file failed
    Anti-virus signature version: 000000_00
    Anti-virus signature compiler version: N/A
    Scan engine type: juniper-express-engine
    Scan engine information: Engine not ready
    Pattern type: N/A
    Total number of signatures: 11020
    New signatures (13):
    ------------------------
    00021301 Backdoor.Win32.Frauder.ky
    00021296 Rootkit.Win32.Pakes.e
    00021323 Trojan-Downloader.Win32.Exchanger.agf
    00021303 Trojan-Downloader.Win32.Injecter.arc
    00021325 Trojan-PSW.Win32.LdPinch.abgp
    00021299 Trojan-Ransom.Win32.Hexzone.pr
    00021298 Trojan-Spy.Win32.Zbot.fgt
    00021300 Trojan-Spy.Win32.Zbot.fgv
    00021324 Trojan-Spy.Win32.Zbot.fgw
    00021322 Trojan-Spy.Win32.Zbot.fhc
    00021321 Trojan-Spy.Win32.Zbot.fhd
    00021297 Trojan.Win32.FraudPack.aju
    00021302 Trojan.Win32.Inject.isz
    Modified signatures (0):
    ------------------------
    Removed signatures (1):
    ------------------------
    00020871 Trojan-GameThief.Win32.OnLineGames.bjpk
```

Copyright © 2013, Juniper Networks, Inc.

## show security utm content-filtering statistics

**Syntax** show security utm content-filtering statistics

**Release Information** Command introduced in Release 9.5 of Junos OS.
Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Display content-filtering statistics for connections including lists of blocked files and the reasons for blocking. Statistics from both the nodes (with full chassis cluster support for UTM) is displayed.

**Required Privilege Level** view

**Related Documentation**
- clear security utm content-filtering statistics on page 1474

**Output Fields** show security utm content-filtering statistics

Output fields are listed in the approximate order in which they appear.

## show security utm content-filtering statistics

```
user@host> show security utm content-filtering statistics
Content-filtering-statistic:         Blocked
     Base on command list:                   0
     Base on mime list:                      0
     Base on extension list:                 0
     ActiveX plugin:                         0
     Java applet:                            0
     EXE files:                              0
     ZIP files:                              0
     HTTP cookie:                            0
```


Copyright © 2013, Juniper Networks, Inc.

## show security utm session

**Syntax** show security utm session

**Release Information** Command introduced in Release 9.5 of Junos OS.
Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Display general UTM session information including all allocated sessions and active sessions. Also, displays information from both nodes in a chassis cluster.

**Required Privilege Level** view

**Related Documentation**

- clear security utm session on page 1475
- show security utm status on page 2182
- UTM for Security Devices
- Unified Threat Management

**Output Fields** show security utm session

Output fields are listed in the approximate order in which they appear.

### show security utm session

```
user@host> show security utm session
Maximum sessions:           4000
 Total allocated sessions:         0
 Total freed sessions:             0
 Active sessions:                  0
```

Copyright © 2013, Juniper Networks, Inc.

## show security utm status

**Syntax** show security utm status

**Release Information** Command introduced in Release 9.5 of Junos OS.
Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Displays whether the UTM service is running or not and status of both the nodes (with full chassis cluster support for UTM).

**Required Privilege Level** view

**Related Documentation**

- clear security utm session on page 1475
- show security utm session on page 2181
- UTM for Security Devices
- Unified Threat Management

**Output Fields** show security utm status

Output fields are listed in the approximate order in which they appear.

## show security utm status

```
user@host> show security utm status
UTM service status: Running
```


Copyright © 2013, Juniper Networks, Inc.

## show security utm web-filtering statistics

**Syntax** show security utm web-filtering statistics

**Release Information** Command introduced in Release 9.5 of Junos OS.
Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Display web-filtering statistics for connections including whitelist and blacklist hits and custom category hits. Statistics from both the nodes (with full chassis cluster support for UTM) is displayed.

**Required Privilege Level** view

**Related Documentation**

- clear security utm web-filtering statistics on page 1476
- show security utm web-filtering status on page 2185
- Unified Threat Management
- UTM for Security Devices

**Output Fields** show security utm web-filtering statistics

Output fields are listed in the approximate order in which they appear.

Copyright © 2013, Juniper Networks, Inc.

## show security utm web-filtering statistics

```
user@host> show security utm web-filtering statistics
 UTM web-filtering statistics:
    Total requests:                     65
    white list hit:                     0
    Black list hit:                     0
    Queries to server:                  62
    Server reply permit:                0
    Server reply block:                 0
    Server reply quarantine:            52
    Server reply quarantine block:      0
    Server reply quarantine permit:     4
    Custom category permit:             0
    Custom category block:              0
    Custom category quarantine:         0
    Custom category qurantine block:    0
    Custom category quarantine permit:  0
    Site reputation permit:             6
    Site reputation block:              0
    Site reputation quarantine:         0
    Site reputation quarantine block:   0
    Site reputation quarantine permit:  0
    Cache hit permit:                   0
    Cache hit block:                    0
    Cache hit quarantine:               2
    Cache hit quarantine block:         0
    Cache hit quarantine permit:        1
    Safe-search redirect:               0
    Web-filtering sessions in total:    16000
    Web-filtering sessions in use:      0


Fall back:           log-and-permit      block
          Default                 0              0
          Timeout                 0              0

Connectivity              0              0

Too-many-requests         0              0
```


Copyright © 2013, Juniper Networks, Inc.

## show security utm web-filtering status

**Syntax** show security utm web-filtering status

**Release Information** Command introduced in Release 9.5 of Junos OS.
Support for UTM in chassis cluster added in Release 11.4 of Junos OS.

**Description** Display whether the SurfControl CPA server is running or not. Status of both the nodes (with full chassis cluster support for UTM) is displayed.

**Required Privilege Level** view

**Related Documentation**

- clear security utm web-filtering statistics on page 1476
- show security utm web-filtering statistics on page 2183
- Unified Threat Management
- UTM for Security Devices

**Output Fields** show security utm web-filtering status

Output fields are listed in the approximate order in which they appear.

## show security utm web-filtering status

```
user@host> show security utm web-filtering status
UTM web-filtering status:
    Server status: SC-CPA server down
```

Copyright © 2013, Juniper Networks, Inc.

## show security zones

**Syntax**
**show security zones**
**<detail | terse>**
**< *zone-name* >**

**Release Information**
Command introduced in Junos OS Release 8.5. The **Description** output field added in Junos OS Release 12.1.

**Description**
Display information about security zones.

**Options**
- none—Display information about all zones.
- **detail | terse**—(Optional) Display the specified level of output.
- ***zone-name*** —(Optional) Display information about the specified zone.

**Required Privilege Level**
view

**Related Documentation**
- Ethernet Port Switching for Security Devices
- Layer 2 Bridging and Transparent Mode for Security Devices
- security-zone on page 923
- Security Zones and Interfaces for Security Devices
- Logical Systems for Security Devices

**List of Sample Output**
show security zones on page 2188
show security zones abc on page 2188
show security zones abc detail on page 2188
show security zones terse on page 2188

**Output Fields**
Table 207 on page 2186 lists the output fields for the **show security zones** command. Output fields are listed in the approximate order in which they appear.

### Table 207: show security zones Output Fields

| Field Name | Field Description |
|---|---|
| **Security zone** | Name of the security zone. |
| **Description** | Description of the security zone. |
| **Policy configurable** | Whether the policy can be configured or not. |
| **Interfaces bound** | Number of interfaces in the zone. |
| **Interfaces** | List of the interfaces in the zone. |
| **Zone** | Name of the zone. |


Copyright © 2013, Juniper Networks, Inc.

Table 207: show security zones Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Type** | Type of the zone. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security zones

```
user@host> show security zones
Functional zone: management
   Description: This is the management zone.
   Policy configurable: No
   Interfaces bound: 1
   Interfaces:
     ge-0/0/0.0
Security zone: Host
   Description: This is the host zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     fxp0.0
Security zone: abc
   Description: This is the abc zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     ge-0/0/1.0
Security zone: def
   Description: This is the def zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     ge-0/0/2.0
```

## Sample Output

show security zones abc

```
user@host> show security zones abc
Security zone: abc
   Description: This is the abc zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     ge-0/0/1.0
```

## Sample Output

show security zones abc detail

```
user@host> show security zones abc detail
Security zone: abc
   Description: This is the abc zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     ge-0/0/1.0
```

## Sample Output

show security zones

```
user@host> show security zones terse
```


Copyright © 2013, Juniper Networks, Inc.

terse

```
Zone                 Type
my-internal          Security
my-external          Security
dmz                  Security
```

## show security zones type

**Syntax**
**show security zones type**
**(functional | security)**
<detail | terse>

**Release Information**
Command introduced in Junos OS Release 8.5. The **Description** output field added in Junos OS Release 12.1.

**Description**
Display information about security zones of the specified type.

**Options**
- **functional**—Display functional zones.
- **security**—Display security zones.
- **detail | terse**—(Optional) Display the specified level of output.

**Required Privilege Level**
view

**Related Documentation**
- security-zone on page 923
- Security Zones and Interfaces for Security Devices

**List of Sample Output**
show security zones type functional on page 2191
show security zones type security on page 2191
show security zones type security terse on page 2191
show security zones type security detail on page 2191

**Output Fields**
Table 208 on page 2190 lists the output fields for the **show security zones type** command. Output fields are listed in the approximate order in which they appear.

### Table 208: show security zones type Output Fields

| Field Name | Field Description |
|---|---|
| **Security zone** | Zone name. |
| **Description** | Description of the security zone. |
| **Policy configurable** | Whether the policy can be configured or not. |
| **Interfaces bound** | Number of interfaces in the zone. |
| **Interfaces** | List of the interfaces in the zone. |
| **Zone** | Name of the zone. |
| **Type** | Type of the zone. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show security zones type functional

```
user@host> show security zones type functional
Functional zone: management
  Description: management zone
  Policy configurable: No
  Interfaces bound: 0
  Interfaces:
```

## Sample Output

show security zones type security

```
user@host> show security zones type security
Security zone: trust
  Description: trust zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
  ge-0/0/0.0
Security zone: untrust
  Description: untrust zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
  ge-0/0/1.0
Security zone: junos-host
  Description: junos-host zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
```

## Sample Output

show security zones type security terse

```
user@host> show security zones type security terse
Zone                    Type
trust                   Security
untrust                 Security
junos-host              Security
```

## Sample Output

show security zones type security detail

```
user@host> show security zones type security detail
Security zone: trust
  Description: trust zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
  ge-0/0/0.0
Security zone: untrust
  Description: untrust zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
```

Copyright © 2013, Juniper Networks, Inc.

```
  Interfaces bound: 1
  Interfaces:
  ge-0/0/1.0
Security zone: junos-host
  Description: junos-host zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
```


Copyright © 2013, Juniper Networks, Inc.

## show services accounting

**Syntax**

show services accounting
aggregation
errors
flow
flow-detail
memory
packet-size-distribution
status
usage

**Release Information**

Command introduced in Release 10.4 of Junos OS.

**Description**

Display sampled accounting service.

**Options**

- aggregation—Display aggregation information.
- errors—Display error statistics.
- flow—Display flow information.
- flow-detail—Display flow detail.
- memory—Display memory information.
- packet-size-distribution—Display packet size distribution.
- status–Display service accounting parameters.
- usage–Display CPU usage.

**Required Privilege Level**

view

Copyright © 2013, Juniper Networks, Inc.

## show services accounting aggregation (View)

**Syntax** show services accounting aggregation

**Release Information** Command introduced in Release 10.4 of Junos OS.

**Description** Display aggregation information for the accounting service.

**Options**

- as—Display aggregation type AS.
- destination-prefix—Display aggregation type destination-prefix.
- protocol-port—Display aggregation type protocol-port.
- source-destination-prefix—Display aggregation type source-destination-prefix.
- source-prefix—Display aggregation type source-prefix.
- template—Display aggregation type template.

**Required Privilege Level** view


Copyright © 2013, Juniper Networks, Inc.

## show services accounting aggregation template (View)

**Syntax** show services accounting aggregation template

**Release Information** Command introduced in Release 10.4 of Junos OS.

**Description** Display aggregation type template.

**Options**
- detail—Display detailed output.
- extensive—Display extensive output.
- template-name—Display name of the template.
- terse—Display terse output (default).

**Required Privilege Level** view

Copyright © 2013, Juniper Networks, Inc.

## show services accounting flow-detail (View)

**Syntax** show services accounting flow-detail

**Release Information** Command introduced in Release 10.4 of Junos OS.

**Description** Display flow detail

**Options**

- destination-as—Filter term destination AS.
- destination-port—Filter term destination port.
- destination-prefix—Filter term destination prefix.
- detail—Display detailed output.
- extensive—Display extensive output.
- input-snmp-interface-index—Filter term input SNMP interface index.
- limit—Display maximum number of flows to display.
- name-Display name of the service, wildcard, or 'all'.
- order—Display order for displaying flows.
- output-snmp-interface-index—Filter term output SNMP interface index.
- proto—Filter term protocol.
- source-as—Filter term source AS.

**Required Privilege Level** view


Copyright © 2013, Juniper Networks, Inc.

## show services application-identification application

**Syntax**
show services application-identification application
(detail *application-name* | summary)

**Release Information**
Command introduced in Junos OS Release 11.4. Output updated in Junos OS Release 12.1X44-D10.

**Description**
Display detailed information about a specified application, all applications, or a summary of the existing applications. Both custom and predefined applications can be displayed.

**Options**
**detail *application-name***—Specify the application name for detailed information.

**summary**—Summary information about the applications on the system.

**Required Privilege Level**
view

**Related Documentation**
- Application Identification for Security Devices
- Application Firewall
- request services application-identification application on page 1525

**List of Sample Output**
show services application-identification application summary on page 2200
show services application-identification application detail on page 2200

**Output Fields**
Table 209 on page 2197 lists the output fields for the **show services application-identification application** command. Output fields are listed in the approximate order in which they appear.

Table 210 on page 2198 lists shows the output details for the **show services application-identification application detail** command.

### Table 209: show services application-identification application summary Output Fields

| Field Name | Field Description |
|---|---|
| **Application(s)** | The number of applications present. |
| **Nested Application(s)** | The number of nested applications present. |
| **Application** | Name of the predefined or custom application or nested application. |
| **Application Group** | Name of the application group associated with the application or nested application. |
| **Disabled** | The status of the application or nested application and whether the mapping method is currently used to identify this application. |

Copyright © 2013, Juniper Networks, Inc.

Table 209: show services application-identification application summary Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **ID** | The unique ID number of an application or nested application. ID numbers 1 through 32,767 are automatically generated for predefined applications and nested applications; these IDs do not change. ID numbers for custom applications and nested applications use ID numbers 32,768 to 65,534. |
| **Order** | A unique number used to specify priority when multiple applications match the traffic. The lowest order number takes the highest priority. |

Table 210: show services application-identification application detail Output Fields

| Field Name | Field Description |
|---|---|
| **Application Name** | Name of the predefined or custom application or nested application. |
| **Application Type** | The basic application type, such as HTTP. |
| **Description** | A description of the predefined or custom application or nested application. |
| **Application ID** | The unique ID number of an application or nested application. ID numbers 1 through 32,767 are automatically generated for predefined applications and nested applications; these IDs do not change. ID numbers for custom applications and nested applications use ID numbers 32,768 to 65,534. |
| **Disabled** | The status of the application or nested application and whether it is currently used to identify traffic. |
| **Risk** | Category specifying the level of risk of the application or nested application. |
| **Technology** | Category specifying the technology of the application or nested application. |
| **Characteristic** | Category specifying one or more characteristics of the application or nested application. |
| **Application Groups** | Name of application groups associated with this application or nested application. |
| **ICMP Mapping** | ICMP mapping criteria associated with the application. |
| **Type** | The ICMP type associated with the application or nested application. |
| **Code** | The ICMP code association with the application or nested application. |
| **IP protocol mapping:** | IP-protocol mapping criteria for application identification. |
| **IP Protocol** | The IP protocol number associated with the application or nested application. |
| **Signature:** | Signature mapping criteria for application identification. |
| **Port range** | Default ranges: TCP/0 through 65,535; UDP/0 through 65,535 (optional). |


Copyright © 2013, Juniper Networks, Inc.

Table 210: show services application-identification application detail Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Client-to-server: DFA Pattern** | Pattern-matching scheme used for client-to-server traffic. Maximum length is 1023 (optional). |
| **Client-to-server: Regex Pattern** | A compatible regular expression used to match client-to-server traffic. |
| **Server to-client: DFA Pattern** | Pattern-matching scheme used for server-to-client traffic. Maximum length is 1023 (optional). |
| **Server-to-client: Regex Pattern** | A compatible regular expression used to match server-to-client traffic. |
| **Minimum data client-to-server** | The minimum number of bytes or packets to apply to the DFA pattern for client-to-server traffic. |
| **Minimum data server-to-client** | The minimum number of bytes or packets to apply to the DFA pattern for server-to-client traffic. |
| **Address Mapping:** | Address mapping criteria for application identification. |
| **IP address** | IP addresses or wildcard addresses associated with the application or nested application. |
| **port** | Ports associated with the application or nested application. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show services application-identification application summary

```
user@host> show services application-identification application summary
Application(s): 150
Nested Application(s): 600

Application              Disabled      ID        Order
...                      ...           ...       ...
junos:FTP                No            63        59
junos:HTTP               Yes           64        122
...                      ...           ...       ...
my:APPLICATION-A         No            700       730
my:APPLICATION-B         No            701       731
...                      ...           ...       ...
```

### show services application-identification application detail

```
user@host> show services application-identification application detail junos:FTP
Application Name: junos:FTP
Description: This signature detects the File Transfer Protocol (FTP), which
provides
           facilities for transferring files to and from remote computer systems.

             It usually runs on TCP port 21.
Application ID: 63
Disabled: No
Number of Parent Group(s): 1
Application Groups:
    junos:file-server
Application Tags:
    characteristic        : Supports File Transfer
    characteristic        : Known Vulnerabilities
    characteristic        : Capable of Tunneling
    risk                  : 3
    category              : FILE-SERVER
Port Mapping:
    Default ports: TCP/21
Signature:
     Port range: TCP/0-24,26-65535
     Client-to-server
         DFA Pattern: \[(USER|STAT|PORT|CHMOD\](\s|\x0d 0a\x|\x0a\x).*
         Regex Pattern: None
     Server-to-client
         DFA Pattern: (220|230|331|530)[\s\-].*
         Regex Pattern: None
     Minimum data client-to-server: 8
     Minimum data server-to-client: 8
     Order: 71

user@host> show services application-identification application detail junos:IGMP
Application Name: junos:IGMP
Description: This signature detects ...
Application ID: 112
Disabled: No
Risk: N/A
Technology: N/A
Characteristic: N/A
Application Groups:
```


Copyright © 2013, Juniper Networks, Inc.

```
IP protocol mapping:
  IP protocol: 50

user@host> show services application-identification application detail junos:SKYPE
Application Name: junos:skype
Description: This signature detects Skype ...
Application ID: 111
Disabled: No
Risk: N/A
Technology: N/A
Characteristic: N/A
Number of Parent Group(s): 1
Application Groups:
    junos:peer-to-peer:voip
Signature:
    Port range: TCP/0-65535
    Client-to-server
        DFA Pattern: .*\x16 03 01 00\x[\x00]?[\xb0-\xff].*
        PCRE Pattern: None
    Server-to-client
        DFA Pattern: .*\x17 03 01 00\x[\x00]?[\xd9\xf0\xf4].*
        PCRE Pattern: None
    Minimum data client-to-server: 100
    Minimum data server-to-client: 100
    Order: 169
Address-Mappings:
    IP address:
        2.3.4.5-2.3.4.99,2.3.4.99,2.3.4.113
    port:
        tcp/5000-6000,udp/7000-8000,udp/9001,udp/9002


user@host> show services application-identification application detail junos:PING
Application Name: junos:PING
Application type: PING
Description: This signature detects the ICMP ping protocol.
Application ID: 1002
Disabled: No
Number of Parent Group(s): 0
Application Tags:
    characteristic        : Loss of Productivity
    characteristic        : Prone to Misuse
    risk                  : 3
    subcategory           : Subcategory
    category              : Example-Category
ICMP Mapping:
    Type: 8
    Code: 0
```

Copyright © 2013, Juniper Networks, Inc.

## show services application-identification application-system-cache (View)

**Syntax** show services application-identification application-system-cache

**Release Information** Command introduced in Release 10.2 of Junos OS.
Command updated in Release 10.4 of Junos OS.
Command updated in Release 12.1 of Junos OS.

**Description** Display application ID from default port/protocol binding or from the application system cache.

**Required Privilege Level** view

**Related Documentation**
- Application Identification for Security Devices
- clear services application-identification application-system-cache (Junos OS) on page 1480

**List of Sample Output** show services application-identification application-system-cache on page 2203

**Output Fields** Table 211 on page 2202 lists the output fields for the **show services application-identification application-system-cache** command. Output fields are listed in the approximate order in which they appear.

Table 211: show services application-identification application-system-cache Output Fields

| Field Name | Field Description |
|---|---|
| **application-cache** | On or Off status of the application cache. |
| **nested-application-cache** | On or Off status of the nested application cache. |
| **cache-unknown-result** | On or Off status for caching unknown results. |
| **cache-entry-timeout** | The number of seconds the mapping information is saved. |
| **pic** | The PIC location of the cache. |
| **Vsys-ID** | Application identification number. |
| **IP address** | IP address. |
| **Port** | Port number that is used with the current session. |
| **Protocol** | Name of the session protocol. |
| **Application** | Name of the service and application that was identified. |
| **Encrypted** | Yes or No identifying the traffic as encrypted or not. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show services application-identification application-system-cache

```
user@host> show services application-identification application-system-cache
Application System Cache Configurations:
application-cache: on
nested-application-cache: on
cache-unknown-result: on
cache-entry-timeout: 3600 seconds
pic: 1/0
Logical system name: root-logical-system
IP address: 5.0.0.1                                  Port: 443    Protocol: TCP
Application: SSL                                     Encrypted: Yes

pic: 1/1
Logical system name: root-logical-system
IP address: 5.0.0.1                                  Port: 80     Protocol: TCP
Application: HTTP                                    Encrypted: No

IP address: 5.0.0.1                                 Port: 4433     Protocol: TCP
Application: HTTP                                    Encrypted: Yes
```

Copyright © 2013, Juniper Networks, Inc.

## show services application-identification counter (AppSecure)

**Syntax** show services application-identification counter

**Release Information** Command introduced in Junos OS Release 10.2. Output updated in Junos OS Release 12.1X44-D10.

**Description** Display the status of all Junos OS application identification counter values per SPU.

**Required Privilege Level** view

**Related Documentation**
- Application Identification for Security Devices
- clear services application-identification counter (Values) on page 1481

**List of Sample Output** show services application-identification counter on page 2205

**Output Fields** Table 212 on page 2204 lists the output fields for the **show services application-identification counter** command. Output fields are listed in an approximate order in which they appear.

### Table 212: show services application-identification counter Output Fields

| Field Name | Field Description |
|---|---|
| **AI cache hits** | Number of sessions found application in AI cache. |
| **AI cache hits by nested application** | Number of sessions found nested application in AI cache. |
| **AI cache misses** | Number of sessions those did not find application from AI cache. |
| **AI matches** | Number of times an application is successfully identified. |
| **AI uni-matches** | |
| **AI no-matches** | Number of times no application match is found. |
| **AI partial matches** | Number of times an application matched only one side signature. |
| **AI no-partial matches** | Number of times no partial match occurs. |
| **AI address based matches** | Number of matches using address-based application identification. |
| **AI ICMP based matches** | Number of matches using ICMP-based application identification. |
| **AI IP protocol based matches** | Number of matches using IP protocol-based application identification. |
| **Sessions that triggered Appid create session API** | Number of sessions that carried out the internal session create process. |


Copyright © 2013, Juniper Networks, Inc.

Table 212: show services application-identification counter Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Sessions that do not incur signature match or decoding** | Number of sessions that do not receive heavy weighted application identification process. |
| **Sessions that incur signature match or decoding** | Number of sessions that receive heavy weighted application identification process. |
| **Client-to-server packets processed** | Number of client-to-server packets processed. |
| **Server-to-client packets processed** | Number of server-to-client packets processed. |
| **Client-to-server layer-7 bytes processed** | Number of client-to-sever Layer 7 payload bytes processed. |
| **Server-to-client layer-7 bytes processed** | Number of server-to-client Layer 7 payload bytes processed. |
| **Terminal first data packets on both direction** | Number of times the first data packet in each direction triggers final application match. |
| **Unspecified encrypted sessions** | Number of encrypted sessions identified by heuristics. |
| **Encrypted P2P sessions** | Number of encrypted P2P sessions identified by heuristics. |

## Sample Output

### show services application-identification counter

```
user@host> show services application-identification counter
pic: 1/0
  Counter type                                                    Value
 AI cache hits                                                        0
 AI cache hits by nested application                                  0
 AI cache misses                                                      0
 AI matches                                                           0
 AI uni-matches                                                       0
 AI no-matches                                                        0
 AI partial matches                                                   0
 AI no-partial matches                                                0
 AI address based matches                                             0
 AI ICMP based matches                                                0
 AI IP protocol based matches                                         0
 Sessions that triggered Appid create session API                     0
 Sessions that do not incur signature match or decoding               0
 Sessions that incur signature match or decoding                      0
 Client-to-server packets processed                                   0
 Server-to-client packets processed                                   0
 Client-to-server layer-7 bytes processed                             0
 Server-to-client layer-7 bytes processed                             0
 Terminal first data packets on both direction                        0
 Unspecified encrypted sessions                                       0
 Encrypted P2P sessions                                               0
```

Copyright © 2013, Juniper Networks, Inc.

## show services application-identification counter ssl-encrypted-sessions

**Syntax** show services application-identification counter ssl-encrypted-sessions

**Release Information** Command introduced in Release 12.1 of Junos OS.

**Description** Display application identification counters for SSL-encrypted traffic.

**Required Privilege Level** view

**Related Documentation**
- Application Identification for Security Devices

**List of Sample Output** show services application-identification counter ssl-encrypted-sessions on page 2207

**Output Fields** Table 213 on page 2206 lists the output fields for the **show services application-identification counter ssl-encrypted-sessions** command. Output fields are listed in the approximate order in which they appear.

### Table 213: show services application-identification counter ssl-encrypted-sessions Output Fields

| Field Name | Field Description |
|---|---|
| **AI cache hits** | Number of sessions in which an application was found in AI cache. |
| **AI cache hits by nested application** | Number of sessions in which a nested application was found in AI cache. |
| **AI cache misses** | Number of sessions in which an application was not found in AI cache. |
| **AI matches** | Number of times an application was successfully identified. |
| **AI uni-matches** | Number of times a unidirectional match was successfully made. |
| **AI no-matches** | Number of times no application match was found. |
| **AI partial matches** | Number of times an application matched only one side signature. |
| **AI no-partial matches** | Number of times no partial match was found. |
| **Sessions that triggered Appid create session API** | Number of sessions that carried out the internal session create process. |
| **Sessions that do not incur signature match or decoding** | Number of sessions that did not receive heavy weighted application identification process. |
| **Sessions that incur signature match or decoding** | Number of sessions that received heavy weighted application identification process. |
| **Client-to-server packets processed** | Number of client-to-server packets processed. |


Copyright © 2013, Juniper Networks, Inc.

Table 213: show services application-identification counter ssl-encrypted-sessions Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Server-to-client packets processed** | Number of server-to-client packets processed. |
| **Client-to-server layer-7 bytes processed** | Number of client-to-sever Layer 7 payload bytes processed. |
| **Server-to-client layer-7 bytes processed** | Number of server-to-client Layer 7 payload bytes processed. |
| **Terminal first data packets on both direction** | Number of times the first data packet in each direction triggered a final application match. |

## Sample Output

show services application-identification counter ssl-encrypted-sessions

```
user@host> show services application-identification counter ssl-encrypted-sessions
pic: 1/0
Counter type                                                    Value
AI cache hits                                                       0
AI cache hits by nested application                                 0
AI cache misses                                                     0
AI matches                                                          0
AI uni-matches                                                      0
AI no-matches                                                       0
AI partial matches                                                  0
AI no-partial matches                                               0
Sessions that triggered Appid create session API                    0
Sessions that do not incur signature match or decoding              0
Sessions that incur signature match or decoding                     0
Client-to-server packets processed                                  0
Server-to-client packets processed                                  0
Client-to-server layer-7 bytes processed                            0
Server-to-client layer-7 bytes processed                            0
Terminal first data packets on both direction                       0
pic: 1/1
Counter type                                                    Value
AI cache hits                                                       0
AI cache hits by nested application                                 0
AI cache misses                                                     0
AI matches                                                          0
AI uni-matches                                                      0
AI no-matches                                                       0
AI partial matches                                                  0
AI no-partial matches                                               0
Sessions that triggered Appid create session API                    0
Sessions that do not incur signature match or decoding              0
Sessions that incur signature match or decoding                     0
Client-to-server packets processed                                  0
Server-to-client packets processed                                  0
Client-to-server layer-7 bytes processed                            0
Server-to-client layer-7 bytes processed                            0
Terminal first data packets on both direction                       0
```

Copyright © 2013, Juniper Networks, Inc.

## show services application-identification group

**Syntax** show services application-identification group [detail *application-group name*| summary]

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Display detailed or summary information about a specified application signature group or all application signature groups. Both custom and predefined application signature groups can be displayed.

**Required Privilege Level** view

**Related Documentation**

- Application Identification for Security Devices
- Application Firewall
- request services application-identification group on page 1529

**List of Sample Output**

show services application-identification group summary on page 2209
show services application-identification group detail on page 2209

**Output Fields** Table 214 on page 2208 lists the output fields for the **show services application-identification group** command. Output fields are listed in the approximate order in which they appear.

Table 214: show services application-identification group Output Fields

| Field Name | Field Description |
|---|---|
| **Description** | Description of the specified application in the detailed display. |
| **Group ID** or **ID** | The unique ID number of an application signature or application signature group. ID numbers 1 through 32,767 are automatically generated for predefined application signatures and application signature groups; these IDs do not change. ID numbers for custom application signatures and application signature groups use ID numbers 32,768 to 65,534. |
| **Disabled** | The status of the application signature group and whether the signature method is currently used to identify this application. The default is No. |
| **Application Group(s)** | The application signature groups present. |
| **Applications** | The application signatures associated with this application signature group. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show services application-identification group summary

```
user@host> show services application-identification group summary
Application Group(s): 24
Application Groups                                  Disabled  ID
  my:enterprise                                      No        32770
  junos:enterprise:voip                              No        25
  junos:peer-to-peer:voip                            No        24
  junos:peer-to-peer:chat                            No        23
  junos:peer-to-peer:file-sharing                    No        22
...
```

### show services application-identification group detail

```
user@host> show services application-identification group detail junos:social-networking
Description: Detection for social networking sites such as Myspace, Facebook and
 similar.
Group ID: 8
Disabled: no
Application-groups:
    junos:social-networking:facebook;
    junos:social-networking:myspace;

Applications:
    junos:4CHAN;
    junos:ADULTFRIENDFINDER;
    junos:BADOO;
    junos:BEBO;
    junos:BLOGGER-POST;
    junos:BLOGSPOT-POST;
```

Copyright © 2013, Juniper Networks, Inc.

## show services application-identification statistics applications

**Syntax** show services application-identification statistics applications <interval *interval-number*>

**Release Information** Command introduced in Release 11.4 of Junos OS.
Command updated in Release 12.1 of Junos OS.

**Description** Display application usage statistics.

**Options**

- none—Display cumulative session and byte statistics per application. Statistics are displayed in alphabetical order.
- **interval** ***interval-number***—(Optional) Display interval statistics per application. Interval statistics are displayed in Top-N format, such that the first application displayed has the largest byte count. If this parameter is not specified, then the default is 1, which is the current interval. The previous interval is 2, and the least current (oldest) is 8.

**Required Privilege Level** view

**Related Documentation**

- Application Identification for Security Devices
- statistics (Services) on page 1181
- clear services application-identification application-statistics on page 1477

**List of Sample Output**
show services application-identification statistics applications on page 2211
show services application-identification statistics applications interval 3 on page 2211

**Output Fields** Table 215 on page 2210 lists the output fields for the **show services application-identification statistics applications** command. Output fields are listed in the approximate order in which they appear.

Table 215: show services application-identification statistics applications Output Fields

| Field Name | Field Description |
|---|---|
| **Application** | Name of the application. |
| **Sessions** | Number of sessions for the application. |
| **Bytes** | Size of the application in bytes. |
| **Encrypted** | Yes or No identifying the traffic as encrypted or not. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show services application-identification statistics applications

```
user@host> show services application-identification statistics applications
Last Reset: 2012-02-14 21:23:45 UTC

Application    Sessions              Bytes    Encrypted
HTTP                  1               2291          Yes
HTTP                  1                942           No
SSL                   1               2291          Yes
unknown               1                100           No
unknown               1                100          Yes
```

### show services application-identification statistics applications interval 3

```
user@host> show services application-identification statistics applications interval 3
Interval start: 2012-01-14 19:22:45 UTC
Elapsed time: 4 minutes 29 seconds

Application    Sessions              Bytes    Encrypted
FTP                2800         1099289882          Yes
HTTP               3000          127498499          Yes
FACEBOOK            500             910091          Yes
UNSPECIFIED        1500              78390          Yes
DNS                 120               4509          Yes
```

Copyright © 2013, Juniper Networks, Inc.

## show services application-identification statistics application-groups

**Syntax** show services application-identification statistics application-groups <interval *interval-number*>

**Release Information** Command introduced in Release 11.4 of Junos OS.

**Description** Display application group usage statistics.

**Options**
- none—Display cumulative session and byte statistics per application group. Statistics are displayed in alphabetical order.
- **interval** ***interval-number***— (Optional) Display interval statistics per application group. Interval statistics are displayed in Top-N format, such that the first application group displayed has the largest byte count. If this parameter is not specified, then the default is 1, which is the current interval. The previous interval is 2, and the least current (oldest) is 8.

**Required Privilege Level** view

**Related Documentation**
- Application Identification for Security Devices
- statistics (Services) on page 1181
- clear services application-identification application-statistics on page 1477

**List of Sample Output** show services application-identification statistics application-groups on page 2212
show services application-identification statistics application-groups interval 8 on page 2213

**Output Fields** Table 216 on page 2212 lists the output fields for the **show services application-identification statistics application-groups** command. Output fields are listed in the approximate order in which they appear.

Table 216: show services application-identification statistics application-groups Output Fields

| Field Name | Field Description |
|---|---|
| **Application Group** | Displays the name of the application group. |
| **Sessions** | Displays the number of sessions for the application group. |
| **Kilo Bytes** | Displays the size of the application group in kilobytes. |

### Sample Output

show services application-identification

```
user@host> show services application-identification statistics application-groups
Last Reset: 2010-06-14 21:23:45 UTC
```


Copyright © 2013, Juniper Networks, Inc.

statistics application-groups

```
Application Group     Sessions          Kilo Bytes

EMAIL                 4000                  10
IM                    1000                 789
P2P                   5000                   0
```

show services application-identification statistics application-groups interval 8

```
user@host> show services application-identification statistics application-groups interval 8
Interval start: 2010-06-14 21:23:45 UTC
Elapsed time: 5 minutes 0 seconds

Application Group     Sessions          Kilo Bytes

IM                    1000                 789
UNASSIGNED            2000                 109
EMAIL                 4000                  10
```

Copyright © 2013, Juniper Networks, Inc.

## show services application-identification version

**Syntax** show services application-identification version

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display the Junos OS application package version.

**Required Privilege Level** view

**Related Documentation**
- Application Identification for Security Devices
- request services application-identification download on page 1527

**List of Sample Output** show services application-identification version on page 2214

### Sample Output

show services application-identification version

The following output shows that the application package version is 1608.

```
user@host> show services application-identification version
Application package version: 1608
```


Copyright © 2013, Juniper Networks, Inc.

## show services ip-monitoring status

**Syntax** show services ip-monitoring status

**Release Information** Command modified in Release 11.4 R2 of Junos OS.

**Description** Display a brief summary of IP monitoring status along with the current state for a given policy.

**Required Privilege Level** view

**Related Documentation**
- IP Monitoring
- show services rpm probe-results (View) on page 2219

**List of Sample Output**
show services ip-monitoring status on page 2217
show services ip-monitoring status on page 2217
show services ip-monitoring status on page 2217

**Output Fields** Table 217 on page 2215 lists the output fields for the **show services ip-monitoring status** command. Output fields are listed in the approximate order in which they appear.

Table 217: show services ip-monitoring status Output Fields

| Field Name | Field Description |
|---|---|
| **Policy** | Name of the policy configured. |
| **Probe Name** | Name of the probe configured. |
| **Address** | Displays the configured target address. |
| **Status** | Displays the status of the probe on the target address. If the status is PASS, then the target address is reached. |
| **Route-Action** | Displays route injection information configured for the policy and its failover status. |
| **Route-Instance** | Displays the routing instance of the route to be injected during failover. |
| **Route** | Routing address of the route to be injected during failover. |
| **Next-Hop** | Specifies the next-hop address of the route to be injected during failover. |
| **State** | Display the state of the route injection action. If the state is APPLIED, then the ip-monitoring policy is in failover state. |
| **Interface Action** | Displays the interface action type as enable or disable. |
| **Policy Action** | Displays the policy action type as enable or disable. |

Copyright © 2013, Juniper Networks, Inc.

Table 217: show services ip-monitoring status Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Admin State** | Displays the current admin state of the interface. |
| **Action Status** | Displays the current action status of the interface. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show services ip-monitoring status

```
user@host> show services ip-monitoring status

Policy - policy1 (Non-preemptive. Status: FAIL)
  RPM Probes:
    Probe name             Test Name       Address          Status
    ---------------------- --------------- ---------------- ---------
    probe_a                a1              15.1.1.10        FAIL
    probe_a                a2              200.1.1.1        FAIL
  Route-Action:
    route-instance    route              next-hop         State
    ----------------- ------------------ ---------------- -------------
    inet.0            200.1.1.0          150.1.1.1        APPLIED
  Interface-Action:
    interface         policy action   admin state action status
    ----------------- --------------- ----------- -----------------
    fe-0/0/5.2        Enable          UP          FAILOVER
    fe-0/0/5.4        Disable         DOWN        FAILOVER
    t1-1/0/0          Enable          UP          FAILOVER
    dl0               Enable          UP          FAILOVER
    ge-0/0/1          Enable          UP          FAILOVER
```

## Sample Output

show services ip-monitoring status

In this example, the policy is in the failback state, and the no-preempt option is not configured.

```
user@host> show services ip-monitoring status

Policy - policy1 (Status: PASS)
  RPM Probes:
    Probe name             Test Name       Address          Status
    ---------------------- --------------- ---------------- ---------
    probe1                 a1              99.1.1.2         PASS
  Route-Action:
    route-instance    route              next-hop         state
    ----------------- ------------------ ---------------- -------------
    inet.0            99.1.1.0           12.12.12.2       NOT-APPLIED
  Interface-Action:
    interface         policy action   admin state action status
    ----------------- --------------- ----------- -----------------
    at-2/0/0          Enable          DOWN        MARKED-DOWN
    ge-0/0/2.2        Enable          DOWN        MARKED-DOWN
    ge-0/0/2.3        Enable          DOWN        MARKED-DOWN
```

## Sample Output

show services ip-monitoring status

In this example, the policy is in the failover state, and the primary is restored. The no-preempt option is configured.

```
user@host> show services ip-monitoring status

Policy - policy1 (Non-preemptive. Status: FAILOVER-NO-PREEMPT)
  RPM Probes:
```

Copyright © 2013, Juniper Networks, Inc.

```
   Probe name              Test Name       Address           Status
  ---------------------- --------------- ---------------- ---------
   probe1                  a1              99.1.1.2         PASS
Route-Action:
  route-instance    route              next-hop         state
  ----------------- ----------------- ---------------- -------------
  inet.0            99.1.1.0          12.12.12.2       APPLIED
Interface-Action:
  interface         policy action   admin state action status
  ----------------- --------------- ----------- -----------------
  at-2/0/0          Enable          UP          FAILOVER
  ge-0/0/2.2        Enable          UP          FAILOVER
  ge-0/0/2.3        Enable          UP          FAILOVER
```


Copyright © 2013, Juniper Networks, Inc.

## show services rpm probe-results (View)

**Syntax**
show services rpm probe-results
<owner *owner*>
<test *name*>

**Release Information**
Command introduced in Release 11.2 of Junos OS.

**Description**
Display the results of the most recent real-time performance monitoring (RPM) probes.

**Options**
**none**—Display all results of the most recent RPM probes.

**owner *owner***—(Optional) Display information for the specified probe owner.

**test *name***—(Optional) Display information for the specified test.

**Required Privilege Level**
view

**Related Documentation**
- IP Monitoring
- show services ip-monitoring status on page 2215
- Device and Routing Operations Monitoring
- Troubleshooting for Security Devices

**List of Sample Output**
show services rpm probe-results on page 2222

**Output Fields**
Table 218 on page 2219 lists the output fields for the **show services rpm probe-results** command. Output fields are listed in the approximate order in which they appear.

### Table 218: show services rpm probe-results Output Fields

| Field Name | Field Description |
|---|---|
| **Owner** | Owner name. When you configure the probe owner statement at the **[edit services rpm]** hierarchy level, this field displays the configured owner name. When you configure BGP neighbor discovery through RPM, the output for this field is **Rpm-Bgp-Owner.** |
| **Test** | Name of a test representing a collection of probes. When you configure the test test-name statement at the **[edit services rpm probe owner]** hierarchy level, the field displays the configured test name. When you configure BGP neighbor discovery through RPM, the output for this field is **Rpm-BGP-Test-*n***, where *n* is a cumulative number. |
| **Target address** | Destination address used for the probes. |
| **Source address** | Source address used for the probes. |
| **Probe type** | Protocol configured on the receiving probe server: **http-get, http-metadata-get, icmp-ping, icmp-ping-timestamp, tcp-ping, udp-ping,** or **udp-ping-timestamp**. |
| **Test size** | Number of probes within a test. |

Copyright © 2013, Juniper Networks, Inc.

Table 218: show services rpm probe-results Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Routing Instance Name** | (BGP neighbor discovery) Name of the configured (if any) routing instance, logical system name, or both, in which the probe is configured:<br>• When a routing instance is defined within a logical system, the logical system name is followed by the routing instance name. A slash **( / )** is used to separate the two entities. For example, if the routing instance called **R1** is configured within the logical system called **LS**, the name in the output field is **LS/R1**.<br>• When a routing instance is configured but the default logical system is used, the name in the output field is the name of the routing instance.<br>• When a logical system is configured but the default routing instance is used, the name in the output field is the name of the logical system followed by **default**. A slash (**/**) is used to separate the two entities. For example, **LS/default**. |
| **Probe results** | Raw measurement of a particular probe sample done by a remote host. This data is provided separately from the calculated results. The following information is contained in the raw measurement:<br>• **Response received**—Timestamp when the probe result was determined.<br>• **Client and server hardware timestamps**—If timestamps are configured, an entry appears at this point.<br>• **Rtt**—Average ping round-trip time (RTT), in microseconds.<br>• **Egress jitter**—Egress jitter, in microseconds.<br>• **Ingress jitter**—Ingress jitter, in microseconds.<br>• **Round trip jitter**—Round-trip jitter, in microseconds.<br>• **Egress interarrival jitter**—Egress interarrival jitter, in microseconds.<br>• **Ingress interarrival jitter**—Ingress interarrival jitter, in microseconds.<br>• **Round trip interarrival jitter**—Round-trip interarrival jitter, in microseconds. |
| **Results over current test** | Probes are grouped into tests, and the statistics are calculated for each test. If a test contains 10 probes, the average, minimum, and maximum results are calculated from the results of those 10 probes. If the command is issued while the test is in progress, the statistics use information from the completed probes.<br>• **Probes sent**—Number of probes sent within the current test.<br>• **Probes received**—Number of probe responses received within the current test.<br>• **Loss percentage**—Percentage of lost probes for the current test.<br>• **Measurement**—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type **icmp-ping-timestamp**, the egress delay and ingress delay.<br>For each measurement type, the following individual calculated results are provided:<br>◦ **Samples**—Number of probes.<br>◦ **Minimum**—Minimum RTT, ingress delay, or egress delay measured over the course of the current test.<br>◦ **Maximum**—Maximum RTT, ingress delay, or egress delay measured over the course of the current test.<br>◦ **Average**—Average RTT, ingress delay, or egress delay measured over the course of the current test.<br>◦ **Peak to peak**—Peak-to-peak difference, in microseconds.<br>◦ **Stddev**—Standard deviation, in microseconds.<br>◦ **Sum**—Statistical sum. |


Copyright © 2013, Juniper Networks, Inc.

Table 218: show services rpm probe-results Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Results over last test** | Results for the most recently completed test. If the command is issued while the first test is in progress, this information is not displayed<br>• **Probes sent**—Number of probes sent for the most recently completed test.<br>• **Probes received**—Number of probe responses received for the most recently completed test.<br>• **Loss percentage**—Percentage of lost probes for the most recently completed test.<br>• **Test completed**—Time the most recent test was completed.<br>• **Measurement**—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type **icmp-ping-timestamp**, the egress delay and ingress delay.<br>For each measurement type, the following individual calculated results are provided:<br>◦ **Samples**—Number of probes.<br>◦ **Minimum**—Minimum RTT, ingress delay, or egress delay measured for the most recently completed test.<br>◦ **Maximum**—Maximum RTT, ingress delay, or egress delay measured for the most recently completed test.<br>◦ **Average**—Average RTT, ingress delay, or egress delay measured for the most recently completed test.<br>◦ **Peak to peak**—Peak-to-peak difference, in microseconds.<br>◦ **Stddev**—Standard deviation, in microseconds.<br>◦ **Sum**—Statistical sum. |
| **Results over all tests** | Displays statistics made for all the probes, independently of the grouping into tests, as well as statistics for the current test.<br>• **Probes sent**—Number of probes sent in all tests.<br>• **Probes received**—Number of probe responses received in all tests.<br>• **Loss percentage**—Percentage of lost probes in all tests.<br>• **Measurement**—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe types **icmp-ping-timestamp** and **udp-ping-timestamp**, the egress delay and ingress delay.<br>For each measurement type, the following individual calculated results are provided:<br>◦ **Samples**—Number of probes.<br>◦ **Minimum**—Minimum RTT, ingress delay, or egress delay measured over the course of the current test.<br>◦ **Maximum**—Maximum RTT, ingress delay, or egress delay measured over the course of the current test.<br>◦ **Average**—Average RTT, ingress delay, or egress delay measured over the course of the current test.<br>◦ **Peak to peak**—Peak-to-peak difference, in microseconds.<br>◦ **Stddev**—Standard deviation, in microseconds.<br>◦ **Sum**—Statistical sum. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show services rpm probe-results

```
user@host> show services rpm probe-results

    Owner: probe_a, Test: a1
    Target address: 200.1.1.2, Probe type: icmp-ping
    Destination interface name: ge-0/0/6.0
    Test size: 10 probes
    Probe results:
      Response received, Sat Jul 30 11:52:21 2011, No hardware timestamps
      Rtt: 1897 usec
    Results over current test:
      Probes sent: 8, Probes received: 8, Loss percentage: 0
      Measurement: Round trip time
        Samples: 8, Minimum: 1897 usec, Maximum: 7205 usec, Average: 2848 usec,
        Peak to peak: 5308 usec, Stddev: 1715 usec, Sum: 22783 usec
    Results over last test:
      Probes sent: 10, Probes received: 10, Loss percentage: 0
      Test completed on Sat Jul 30 11:52:01 2011
      Measurement: Round trip time
        Samples: 10, Minimum: 1907 usec, Maximum: 8201 usec, Average: 3111 usec,

        Peak to peak: 6294 usec, Stddev: 2306 usec, Sum: 31106 usec
    Results over all tests:
      Probes sent: 598, Probes received: 327, Loss percentage: 45
      Measurement: Round trip time
        Samples: 327, Minimum: 1878 usec, Maximum: 133729 usec,
        Average: 3304 usec, Peak to peak: 131851 usec, Stddev: 7561 usec,
        Sum: 1080434 usec
```


Copyright © 2013, Juniper Networks, Inc.

## show services ssl proxy statistics

**Syntax** **show services ssl proxy statistics**

**Release Information** Command introduced in Release 12.1 of Junos OS.

**Description** Display information about the SSL proxy statistics.

**Options** **none**—Display summary information about SSL proxy.

**Required Privilege Level** view

**Related Documentation**
- clear services ssl proxy statistics on page 1483

**List of Sample Output** show services ssl proxy statistics on page 2223

**Output Fields** Table 219 on page 2223 describes the output fields for the **show services ssl proxy statistics** command. Output fields are listed in the approximate order in which they appear.

Table 219: show services ssl proxy statistics Output Fields

| Field Name | Field Description |
|---|---|
| **proxy sessions matched** | The number of proxy sessions that are matched. |
| **sessions whitelisted** | The number of sessions that are whitelisted. Whitelists comprise addresses or domain names that you want to exempt from the SSL proxy processing. |
| **proxy sessions created** | The number of proxy sessions that are newly created. |
| **proxy sessions destroyed** | The number of proxy sessions that are destroyed. |
| **proxy sessions ignored** | The number of proxy sessions that are ignored. |

### Sample Output

**show services ssl proxy statistics**

```
user@host> show services ssl proxy statistics
PIC:spu-10 fpc[5] pic[0] ------
        proxy sessions matched                  3
        sessions whitelisted                    0
        proxy sessions created                  2
        proxy sessions destroyed                2
```

## show services unified-access-control authentication-table

**Syntax** show services unified-access-control authentication-table

**Release Information** Command introduced in Junos OS Release 9.4. Options updated in Junos OS Release 12.1.

**Description** Display a summary of the authentication table entries configured from the IC Series UAC Appliance. Authentication tables store mappings between traffic sessions and Unified Access Control (UAC) roles. The IC Series appliance uses the roles specified in the mappings to help determine which UAC policies to apply to a session.

Use this command when you have configured the SRX Series device to act as a Junos OS Enforcer in a UAC deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series appliance.

You can also use this command to display the content of the authentication table in a user role firewall implementation. The table, pushed from a supporting UAC device, provides the user roles associated with incoming traffic.

**Options**

- **detail**—Display a detailed view of all authentication table entries.
- **extended**—Display a view of all authentication table entries with the user roles listed.
- **identifier** *id*—Display all authentication table entries with the specified identifier number.
- **ip** *source-ip-address*—Display any authentication table entry for the specified IP address.
- **role** *role-name*—Display all authentication table entries for the specified role name.
- **user** *username*—Display all authentication table entries for the specified user.

**Required Privilege Level** view

**Related Documentation**

- Unified Access Control Solution for Security Devices

**List of Sample Output**

show services unified-access-control authentication-table on page 2225
show services unified-access-control authentication-table detail on page 2225
show services unified-access-control authentication-table extended on page 2225
show services unified-access-control authentication-table identifier id on page 2225
show services unified-access-control authentication-table ip on page 2225
show services unified-access-control authentication-table role on page 2225
show services unified-access-control authentication-table user username on page 2225


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show services unified-access-control authentication-table

```
user@host>show services unified-access-control authentication-table
Id    Source IP       Username     Age      Role identifier
1     172.24.72.79    atsang       0        0000000001.000005.0
Total: 1
```

show services unified-access-control authentication-table detail

```
user@host>show services unified-access-control authentication-table detail
Identifier: 1
  Source IP: 172.24.72.79
  Username: atsang
  Age: 0
  Role identifier       Role name
    0000000001.000005.0 Users
    1113249951.100616.0 PersonalFirewall
    1183670148.427197.0 UAC
Total: 1
```

show services unified-access-control authentication-table extended

```
user@host>show services unified-access-control authentication-table extended
Id    Source IP       Username     Age   Role name
3     10.214.161.195  prasanta     60    Users, PersonalFirewall
6     10.214.161.183  june         60    role-1
Total: 2
```

show services unified-access-control authentication-table identifier id

```
user@host>show services unified-access-control authentication-table identifier 1
Identifier: 1
  Source IP: 172.24.72.79
  Username: atsang
  Age: 0
  Role identifier       Role name
    0000000001.000005.0 Users
    1113249951.100616.0 PersonalFirewall
    1183670148.427197.0 UAC
Total: 1
```

show services unified-access-control authentication-table ip

```
user@host>show services unified-access-control authentication-table ip 10.214.161.183
Id    Source IP       Username     Age      Role identifier
8     10.214.161.183  june          0        1420298444.225667.0
Total: 1
```

show services unified-access-control authentication-table role

```
user@host>show services unified-access-control authentication-table role role-1
Id    Source IP       Username     Age      Role identifier
6     10.214.161.183  june         60       1420298444.225667.0
Total: 1
```

show services unified-access-control authentication-table user username

```
user@host>show services unified-access-control authentication-table user prasanta
Id    Source IP       Username     Age      Role identifier
7     10.214.161.195  prasanta     0        0000000001.000005.0
Total: 1
```

Copyright © 2013, Juniper Networks, Inc.

## show services unified-access-control counters

**Syntax** show services unified-access-control counters

**Release Information** Command introduced in Release 12.1X44-D10 of Junos OS.

**Description** Display the number of sessions allowed, denied, and terminated by the Unified Access Control (UAC) service when invoked by a firewall policy with the uac-policy action. Counts are reported for each action taken by UAC. Sessions that were allowed, denied, or terminated by other firewall policy actions are not included in these statistics.

On high-end SRX Series devices, UAC counts are grouped and displayed for each PIC on the device. On branch SRX Series devices, UAC counts are accumulated by device only. There is no PIC specification on these devices.

**Required Privilege Level** view

**List of Sample Output** show services unified-access-control counters on page 2227

**Output Fields** Table 220 on page 2226 lists the output fields for the **show services unified-access-control counters** command. Output fields are listed in the approximate order in which they appear.

Table 220: show services unified-access-control counters Output Fields

| Field Name | Field Description |
|---|---|
| **PIC** | If applicable, the number of each PIC implementing UAC. UAC statistics are grouped by PIC. |
| **Sessions allowed** | The sessions permitted by UAC when invoked by a user role firewall policy. |
| **Policy action** | Number of sessions permitted by UAC based on the UAC policy action. |
| **Timeout action** | Number of sessions permitted by the timeout action while the SRX was disconnected from the UAC device. |
| **Sessions denied** | The sessions denied by UAC when invoked by a user role firewall policy. |
| **Unauthenticated** | Number of sessions denied by UAC because the user was not authenticated. |
| **Policy action** | Number of sessions denied by UAC based on the UAC policy action. |
| **Policy not matched** | Number of sessions denied because no UAC policy match was found. |
| **Timeout action** | Number of sessions denied by the timeout action while the SRX was disconnected from the access control device. |
| **Sessions terminated** | The sessions originally permitted that were later terminated. |
| **Reevaluation** | Number of sessions terminated due to a change in the UAC user roles associated with the session. |


Copyright © 2013, Juniper Networks, Inc.

Table 220: show services unified-access-control counters Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Signout** | Number of sessions terminated due to the user signing out. |

## Sample Output

### show services unified-access-control counters

```
user@host> show services unified-access-control counters
PIC: fpc2.pic0
  Sessions allowed
    Policy action: 0
    Timeout action: 0
  Sessions denied
    Unauthenticated: 0
    Policy action: 0
    Policy not matched: 0
    Timeout action: 0
  Sessions terminated
    Reevaluation: 0
    Signout: 0
```

Statistics on branch devices are accumulated by device only. There is no PIC specification on these devices.

```
user@host> show services unified-access-control counters
Sessions allowed
    Policy action: 0
    Timeout action: 0
  Sessions denied
    Unauthenticated: 0
    Policy action: 0
    Policy not matched: 0
    Timeout action: 0
  Sessions terminated
    Reevaluation: 0
    Signout: 0
```

Copyright © 2013, Juniper Networks, Inc.

## show services unified-access-control policies

**Syntax** show services unified-access-control policies

**Release Information** Command introduced in Junos OS Release.

**Description** Display a summary of resource access policies configured from the IC Series UAC Appliance.

Use this command when you have configured the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series appliance.

**Options**

- **detail**—Display a detailed view of all policies.
- **identifier *id***—Display information about a specific policy by identification number.

**Required Privilege Level** view

**Related Documentation**

- Unified Access Control Solution for Security Devices

**List of Sample Output**

show services unified-access-control policies on page 2229
show services unified-access-control policies detail on page 2229
show services unified-access-control policies identifier 1 on page 2229


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

show services unified-access-control policies

```
user@host> services unified-access-control policies
Id    Resource                Action Apply        Role identifier
1     10.100.15.0/24:*        allow  selected     1113249951.100616.0
2     10.100.17.0/24:*        deny   all
```

## Sample Output

show services unified-access-control policies detail

```
user@host> services unified-access-control policies detail
Identifier: 1
  Resource: 10.100.15.0/24:*
  Resource: 10.100.16.23-10.100.16.60:*
  Action: allow
  Apply: selected
  Role identifier       Role name
    1113249951.100616.0 Personal Firewall
    1112927873.881659.0 Antivirus
    1183670148.427197.0 UAC
Identifier: 2
  Resource: 10.100.17.0/24:*
  Resource: 10.100.16.23-10.100.16.60:*
  Resource: 10.100.18.0/24:*
  Action: deny
  Apply: all
```

## Sample Output

show services unified-access-control policies identifier 1

```
user@host> show services unified-access-control policies identifier 1
Identifier: 1
  Resource: 10.100.15.0/24:*
  Resource: 10.100.16.23-10.100.16.60:*
  Action: allow
  Apply: selected
  Role identifier       Role name
    1113249951.100616.0 Personal Firewall
    1112927873.881659.0 Antivirus
    1183670148.427197.0 UAC
```

Copyright © 2013, Juniper Networks, Inc.

## show services unified-access-control roles

**Syntax** show services unified-access-control roles

**Release Information** Command introduced in Junos OS Release 12.1.

**Description** When implementing user role firewall, display a summary of the roles that have been pushed to the SRX Series device from the access control service.

**Required Privilege Level** view

**Related Documentation**
- Understanding the User Identification Table
- Understanding User Role Firewalls
- Unified Access Control Solution for Security Devices

**List of Sample Output** show services unified-access-control roles on page 2230

**Output Fields** Table 221 on page 2230 lists the output fields for the **show services unified-access-control roles** command. Output fields are listed in the approximate order in which they appear.

Table 221: show services unified-access-control roles Output Fields

| Field Name | Field Description |
|---|---|
| **Name** | Name of the user role. |
| **Identifier** | Unique identifier associated with the specified user role. |
| **Total** | Total number of user roles specified in the table. |

### Sample Output

show services unified-access-control roles

```
user@host> show services unified-access-control roles
Name                                                Identifier
Users                                               0000000001.000005.0
admin-1                                             1420298444.225667.0
Total: 2
```


Copyright © 2013, Juniper Networks, Inc.

## show services unified-access-control status

**Syntax** show services unified-access-control status

**Release Information** Command introduced in Junos OS Release 9.4.

**Description** Display the status of the connection between the SRX Series device and the IC Series UAC Appliance as well as statistics to help debug connections to the IC Series appliance.

Use this command when you have configured the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series appliance.

**Required Privilege Level** view

**Related Documentation**
- Unified Access Control Solution for Security Devices

**List of Sample Output** show services unified-access-control status on page 2231

### Sample Output

show services unified-access-control status

```
user@host> show services unified-access-control status
Host           Address         Port   Interface     State
dev106vm26     10.64.11.106    11123  ge-0/0/0.0    connected
dev107vm26     10.64.11.106    11123  ge-0/0/0.0    closed
```

Copyright © 2013, Juniper Networks, Inc.

## show snmp health-monitor

**Syntax** show snmp health-monitor
<alarms <detail>> | <logs>

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10 for SRX Series devices.

**Description** Display information about SNMP health monitor alarms and logs.

**Options** **none**—Display information about all health monitor alarms and logs.

**alarms <detail>**—(Optional) Display detailed information about health monitor alarms.

**logs**—(Optional) Display information about health monitor logs.

**Required Privilege Level** view

**Related Documentation**
- Device and Routing Operations Monitoring

**List of Sample Output**
show snmp health-monitor on page 2235
show snmp health-monitor alarms detail on page 2235
show snmp health-monitor alarms brief on page 2237

**Output Fields** Table 222 on page 2232 describes the output fields for the **show snmp health-monitor** command. Output fields are listed in the approximate order in which they appear.

Table 222: show snmp health-monitor Output Fields

| Field Name | Field Description |
|---|---|
| **Alarm Index** | Alarm identifier. |
| **Variable description** | Description of the health monitor object instance being monitored. |
| **Variable name** | Name of the health monitor object instance being monitored. |
| **Value** | Current value of the monitored variable in the most recent sample interval. |


Copyright © 2013, Juniper Networks, Inc.

Table 222: show snmp health-monitor Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **State** | State of the alarm or event entry:<br>• Alarms:<br>  • **moderate-threshold**—Percentage of moderate threshold level resource utilization.<br>  • **high-threshold** —Percentage of high-threshold level resource utilization.<br>  • **critical-threshold** —Percentage of citical threshold level resource utilization.<br>  • **active**—Entry is fully configured and activated.<br>  • **falling threshold crossed**—Value of the variable has crossed the lower threshold limit.<br>  • **rising threshold crossed**—Value of the variable has crossed the upper threshold limit.<br>  • **under creation**—Entry is being configured and is not yet activated.<br>  • **startup**—Alarm is waiting for the first sample of the monitored variable.<br>  • **object not available**—Monitored variable of that type is not available to the health monitor agent.<br>  • **instance not available**—Monitored variable's instance is not available to the health monitor agent.<br>  • **object type invalid**—Monitored variable is not a numeric value.<br>  • **object processing errored**—An error occurred when the monitored variable was processed.<br>  • **unknown**—State is not one of the above. |
| **Variable OID** | Object ID to which the variable name is resolved. The format is **x.x.x.x**. |
| **Sample type** | Method of sampling the monitored variable and calculating the value to compare against the upper and lower thresholds. It can have the value of **absolute value** or **delta value**. |
| **Startup alarm** | Alarm that might be sent when this entry is first activated, depending on the following criteria:<br>• Alarm is sent when one of the following situations exists:<br>  • Value of the alarm is above or equal to the rising threshold and the startup type is either **rising alarm** or **rising or falling alarm.**<br>  • Value of the alarm is below or equal to the falling threshold and the startup type is either **falling alarm** or **rising or falling alarm**.<br>• Alarm is *not* sent when one of the following situations exists:<br>  • Value of the alarm is above or equal to the rising threshold and the startup type is **falling alarm**.<br>  • Value of the alarm is below or equal to the falling threshold and the startup type is **rising alarm**.<br>  • Value of the alarm is between the thresholds. |
| **Owner** | Name of the entry configured by the user. If the entry was created through the CLI, the owner has **monitor** prepended to it. |
| **Creator** | Mechanism by which the entry was configured (**Health Monitor**). |

Copyright © 2013, Juniper Networks, Inc.

Table 222: show snmp health-monitor Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Sample interval** | Time period between samples (in seconds). |
| **Rising threshold** | Upper limit threshold value as a percentage of the maximum possible value. |
| **Falling threshold** | Lower limit threshold value as a percentage of the maximum possible value. |
| **Rising event index** | Event triggered when the rising threshold is crossed. |
| **Falling event index** | Event triggered when the falling threshold is crossed. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show snmp health-monitor

```
user@host> show snmp health-monitor

Alarm
Index  Variable description                              Value State

 32770 Health Monitor: md3:/jail/mfs utilization
       jnxHrStoragePercentUsed.16                          0 active

 32773 Health Monitor: md2:/mfs/var/run/utm utilization
       jnxHrStoragePercentUsed.15                          0 active

 32776 Health Monitor: md1:/mfs utilization
       jnxHrStoragePercentUsed.11                         11 active

 32779 Health Monitor: /var file system utilization
       jnxHrStoragePercentUsed.10                         44 critical threshold

 32782 Health Monitor: root file system utilization
       jnxHrStoragePercentUsed.1                          52 critical threshold

 32785 Health Monitor: /config file system utilization
       jnxHrStoragePercentUsed.2                           0 active

 32788 Health Monitor: RE 0 CPU utilization
       jnxOperatingCPU.9.1.0.0                            20 active

 32791 Health Monitor: RE 0 memory utilization
       jnxOperatingBuffer.9.1.0.0                         52 active

 32792 Health Monitor: Max Kernel Memory Used (%)
       jnxBoxKernelMemoryUsedPercent.0                     3 active

 32793 Health Monitor: jroute daemon memory usage
       Routing protocols process                       51452 active
       Management process                              38284 active
       Periodic packet management process               9828 active
       Bidirectional Forwarding Detection process      13088 active
       Service Deployment Client                       10012 active
       Event processing process                        12692 active
       Layer 2 address flooding and learning process       20212 active
       MPLS Periodic Traceroute process                10488 active
       Multicast Snooping process                       9608 active
       Feature license management process              12372 active
```

### show snmp health-monitor alarms detail

```
user@host> show snmp health-monitor alarms detail

  Alarm Index 32770:
  Variable name                     jnxHrStoragePercentUsed.16
  Variable OID                      1.3.6.1.4.1.2636.3.31.1.1.1.1.16
  Sample type                       absolute value
  Startup alarm                     rising alarm
  Owner                             Health Monitor: md3:/jail/mfs utilization

  Creator                           Health Monitor
  State                             active
  Sample interval                 15 seconds
```

Copyright © 2013, Juniper Networks, Inc.

```
  Moderate threshold               20
  High threshold                   30
  Critical threshold               40
  Rising event index            32768
  Falling event index           32768
    Instance Value: 0
    Instance State: active

Alarm Index 32773:
  Variable name                       jnxHrStoragePercentUsed.15
  Variable OID                        1.3.6.1.4.1.2636.3.31.1.1.1.1.15
  Sample type                         absolute value
  Startup alarm                       rising alarm
  Owner                               Health Monitor: md2:/mfs/var/run/utm
                                      utilization
  Creator                             Health Monitor
  State                               active
  Sample interval                  15 seconds
  Moderate threshold               20
  High threshold                   30
  Critical threshold               40
  Rising event index            32768
  Falling event index           32768
    Instance Value: 0
    Instance State: active

Alarm Index 32793:
  Variable name                       sysApplElmtRunMemory.5
  Variable OID                        1.3.6.1.2.1.54.1.2.3.1.10.5
  Sample type                         absolute value
  Startup alarm                       rising alarm
  Owner                               Health Monitor: jroute daemon memory
                                      usage
  Creator                             Health Monitor
  State                               active
  Sample interval                  20 seconds
  Rising threshold              104857
  Falling threshold              91750
  Rising event index             32768
  Falling event index            32768
    Instance Name: sysApplElmtRunMemory.5.5.1258
    Instance Description: Routing protocols process
    Instance Value: 51452
    Instance State: active

    Instance Name: sysApplElmtRunMemory.5.6.1255
    Instance Description: Management process
    Instance Value: 38284
    Instance State: active

    Instance Name: sysApplElmtRunMemory.5.6.3816
    Instance Description: Management process
    Instance Value: 38352
    Instance State: active

    Instance Name: sysApplElmtRunMemory.5.8.3815
    Instance Description: Command-line interface
    Instance Value: 49108
    Instance State: active
```


Copyright © 2013, Juniper Networks, Inc.

## show snmp health-monitor alarms brief

```
user@host> show snmp health-monitor alarms brief
 32791 Health Monitor: RE 0 memory utilization
       jnxOperatingBuffer.9.1.0.0                          52 active

 32792 Health Monitor: Max Kernel Memory Used (%)
       jnxBoxKernelMemoryUsedPercent.0                      3 active

 32793 Health Monitor: jroute daemon memory usage
       Routing protocols process                        51452 active
       Management process                               38284 active
       Management process                               38356 active
       Command-line interface                           49108 active
       Periodic packet management process                9828 active
       Bidirectional Forwarding Detection process       13088 active
       Service Deployment Client                        10012 active
       Event processing process                         12692 active
       Layer 2 address flooding and learning process        20212 active
       MPLS Periodic Traceroute process                 10488 active
       Multicast Snooping process                        9608 active
       Feature license management process               12372 active

 32794 Health Monitor: jkernel daemon memory usage
       Init daemon                                       1684 active
       Chassis control process                         115888 rising threshold
       Firewall process                                 22584 active
       Interface control process                        34000 active
       Simple Network Management Protocol process       21772 active
       Management Information Base II process           27848 active
       Alarm control process                            12568 active
       Packet Forwarding Engine statistics management process       24388 active
       Craft interface I/O control process              13248 active
       Remote operations process                        13712 active
       Class-of-service process                         18908 active
       Internal routing service process                  7924 active
       Inet process                                      6052 active
       USB supervise process                             2388 active
       PPP process                                       8772 active
       Juniper Stateful Redundancy Protocol Daemon       13668 active
       Network security daemon                          24248 active
       Simple Mail Transfer Protocol Client process         8088 active
       PFE relay process                                 8044 active
       Subscriber management process                    17852 active
       Subscriber management helper process             21076 active
       Web management gatekeeper process                12820 active
       Application-identification process               18328 active
       IDP policy daemon                                30188 active
       Shared memory routing socket message database process       15672 active
       System Health Management Daemon                  15004 active
       Network security trace daemon                    10400 active
       Wireless WAN process                             15016 active
       Wireless LAN service process                     13936 active

 32797 Health Monitor: RE Temperature
       jnxFruTemp.9.1.0.0                                  51 active

 32800 Health Monitor: RE Process count usage
       hrSystemProcesses.0                                123 moderate threshold

 32803 Health Monitor: RE Open file Descriptor count
       jnxHrSystemOpenFiles.0                             738 active
```

Copyright © 2013, Juniper Networks, Inc.

```
32804 Health Monitor: FWDD Micro-Kernel threads total CPU Utilization
      jnxFwddMicroKernelCPUUsage.0                      11 active

32805 Health Monitor: FWDD Real-Time threads total CPU Utilization
      jnxFwddRtThreadsCPUUsage.0                         0 active

32806 Health Monitor: FWDD DMA Memory utilization
      jnxFwddDmaMemUsage.0                               1 active

32807 Health Monitor: FWDD Heap utilization
      jnxFwddHeapUsage.0                                39 active
```


Copyright © 2013, Juniper Networks, Inc.

## show snmp health-monitor routing engine history

**Syntax** show snmp health-monitor routing-engine history resource <*cpu* | *memory* | *open-files-count* | *process-count* | *storage* | *temperature*>;

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10 for branch SRX Series devices.

**Description** Displays the health-monitoring information collected for a Routing Engine.

**Options** **brief**—Displays brief health monitor history.

**extensive**—Displays extensive health monitor history.

**Required Privilege Level** view

**Related Documentation**
- show snmp health-monitor on page 2232
- Device and Routing Operations Monitoring

**List of Sample Output**
show snmp health-monitor routing engine history on page 2241
show snmp health-monitor routing engine history extensive on page 2241

**Output Fields** Table 223 on page 2239 describes the output fields for the **show snmp health-monitor routing engine** command. Output fields are listed in the approximate order in which they appear.

Table 223: show snmp health-monitor routing engine Output Fields

| Field Name | Field Description |
|---|---|
| **Resource** | Name of the health monitor object instance being monitored. |
| **Alarm Index** | Alarm identifier. |
| **Description** | Description of the health monitor object instance being monitored. |
| **Current Value** | Current value of the monitored variable in the most recent sample interval. |

Copyright © 2013, Juniper Networks, Inc.

Table 223: show snmp health-monitor routing engine Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Alarm State** | Indicates the current state of the resource.<br>• Alarms:<br>  • **active**—Entry is fully configured and activated.<br>  • **moderate-threshold**—Percentage of moderate threshold level resource utilization.<br>  • **high-threshold** —Percentage of high-threshold level resource utilization.<br>  • **critical-threshold** —Percentage of critical threshold level resource utilization.<br>  • **under creation**—Entry is being configured and is not yet activated.<br>  • **startup**—Alarm is waiting for the first sample of the monitored variable.<br>  • **object not available**—Monitored variable of that type is not available to the health monitor agent.<br>  • **instance not available**—Monitored variable's instance is not available to the health monitor agent.<br>  • **object type invalid**—Monitored variable is not a numeric value.<br>  • **object processing errored**—An error occurred when the monitored variable was processed.<br>  • **unknown**—State is not one of the above. |
| **Configuration** | Effective configuration of a resource. |
| **Top daemon** | List of processes with high resource utilization. |
| **Growing daemons** | List of processes with high incremental resource utilization from the previous sample. |
| **Top files** | List of large files in a partition. |
| **Growing files** | List of files in a partition that have gotten larger since the previous sample. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show snmp health-monitor routing engine history

```
user@host> show snmp health-monitor routing engine history brief
Period for which history is available: 6d 00:14 (hh:mm:ss)
Time at which monitoring started: 2012-05-29 16:45:27 UTC
Configuration:  Interval  Moderate threshold  High threshold Critical threshold
                15          70                 80             90

Resource: jnxHrStoragePercentUsed.16, Alarm index: 32770
    Description: MD3:/jail/mfs monitoring
    Current Value: 0
    Alarm State: active
Configuration:  Interval  Moderate threshold  High threshold Critical threshold
                15          20                 30             40

Resource: jnxHrStoragePercentUsed.15, Alarm index: 32773
    Description: MD2:/mfs/var/run/utm monitoring
    Current Value: 0
    Alarm State: active
Configuration:  Interval  Moderate threshold  High threshold Critical threshold
                15          20                 30             40
```

### show snmp health-monitor routing

```
user@host> show snmp health-monitor routing engine history extensive
Period for which history is available: 6d 23:11 (hh:mm:ss)
Time at which monitoring started: 2012-05-29 16:45:27 UTC
```

Copyright © 2013, Juniper Networks, Inc.

engine history extensive

```
    Time: 2012-05-24 11:13:18 UTC
    Description: Health Monitor: jnxHrStoragePercentUsed.10 Recent Records: 58
58 58 58 58 58 58 58 58 58

    Time: 2012-05-24 11:13:20 UTC
    Description: Health Monitor: jnxHrStoragePercentUsed.10 Recent Records: 58
58 58 58 58 58 58 58 58 58

    Time: 2012-05-24 11:13:22 UTC
    Description: Health Monitor: jnxHrStoragePercentUsed.10 Recent Records: 58
58 58 58 58 58 58 58 58 58

    Time: 2012-05-24 11:13:24 UTC
    Description: Health Monitor: jnxHrStoragePercentUsed.1 Recent Records: 52 52
 52 52 52 52 52 52 52 52 52

    Time: 2012-05-24 11:13:26 UTC
    Description: Health Monitor: jnxHrStoragePercentUsed.1 Recent Records: 52 52
 52 52 52 52 52 52 52 52 52

    Time: 2012-05-24 11:13:28 UTC
    Description: Health Monitor: jnxHrStoragePercentUsed.1 Recent Records: 52 52
 52 52 52 52 52 52 52 52 52

   Time: 2012-04-20 16:05:43 UTC
    Description: Health Monitor: crossed Moderate rising threshold :
hrSystemProcesses.0

        Top Daemons                 Usage
        init                        61
        swapper                     59
        mgd                         2
        sh                          1
        login                       1

        Growing Daemons             Usage
        init                        4
        httpd-gk                    1
        sh                          1

        Usage unit: absolute

    Time: 2012-05-16 13:55:07 UTC
    Description: Health Monitor: crossed Moderate rising threshold :
hrSystemProcesses.0

        Top Daemons                 Usage
        init                        60
        swapper                     59
        mgd                         3
        sh                          2
        csh                         1

        Growing Daemons             Usage
        mgd                         2
        chassisd                    1
        sh                          1
        mgd                         1
        sh                          1
```


Copyright © 2013, Juniper Networks, Inc.

```
        Usage unit: absolute

    Time: 2012-05-16 14:04:39 UTC
    Description: Health Monitor: crossed Moderate rising threshold :
hrSystemProcesses.0

        Top Daemons                 Usage
        swapper                     59
        init                        58
        chassisd                    1
        csh                         1
        csh                         1

        Growing Daemons             Usage
        su                          1
        csh                         1
        inetd                       1
        login                       1
        telnetd                     1

        Usage unit: absolute
```

Copyright © 2013, Juniper Networks, Inc.

## show snmp mib (View)

**Syntax** show snmp mib (get | get-next | walk) (ascii | decimal) *object-id*

**Release Information** Command introduced in Release 9.4 of Junos OS for SRX Series Services Gateways.

**Description** Display local SNMP MIB object values.

**Options**

**get**—Retrieve and display one or more SNMP object values.

**get-next**—Retrieve and display the next SNMP object values.

**walk**—Retrieve and display the SNMP object values that are associated with the requested object identifier (OID). When you use this option, the Junos OS displays the objects below the subtree that you specify.

**ascii**—Display the SNMP object's string indices as an ASCII-key representation.

**decimal**—Display the SNMP object values in the decimal (default) format. The **decimal** option is the default option for this command. Therefore, issuing the **show snmp mib (get | get-next | walk) decimal object-id** and the **show snmp mib (get | get-next | walk) object-id** commands display the same output.

***object-id***—The object can be represented by a sequence of dotted integers (such as **1.3.6.1.2.1.2**) or by its subtree name (such as **interfaces**). When entering multiple objects, enclose the objects in quotation marks.

**Required Privilege Level** snmp—To view this statement in the configuration.

**List of Sample Output**

show snmp mib walk (standalone) on page 2245
show snmp mib walk (HA) on page 2245

**Output Fields** Table 224 on page 2244 describes the output fields for the **show snmp mib** command. Output fields are listed in the approximate order in which they appear.

### Table 224: show snmp mib Output Fields

| Field Name | Field Description |
|---|---|
| ***name*** | Object name and numeric instance value. |
| ***object value*** | Object value. The Junos OS translates OIDs into the corresponding object names. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show snmp mib walk (standalone)

```
user@host> show snmp mib walk jnxJsSPUMonitoringObjectsTable
jnxJsSPUMonitoringFPCIndex.5 = 5
jnxJsSPUMonitoringSPUIndex.5 = 0
jnxJsSPUMonitoringCPUUsage.5 = 0
jnxJsSPUMonitoringMemoryUsage.5 = 61
jnxJsSPUMonitoringCurrentFlowSession.5 = 0
jnxJsSPUMonitoringMaxFlowSession.5 = 524288
jnxJsSPUMonitoringCurrentCPSession.5 = 0
jnxJsSPUMonitoringMaxCPSession.5 = 2359296
jnxJsSPUMonitoringNodeIndex.5 = 0
jnxJsSPUMonitoringNodeDescr.5 = single
```

### show snmp mib walk (HA)

```
user@switch> show snmp mib walk jnxJsSPUMonitoringObjectsTable
jnxJsSPUMonitoringFPCIndex.20 = 5
jnxJsSPUMonitoringFPCIndex.21 = 5
jnxJsSPUMonitoringFPCIndex.44 = 5
jnxJsSPUMonitoringFPCIndex.45 = 5
jnxJsSPUMonitoringSPUIndex.20 = 0
jnxJsSPUMonitoringSPUIndex.21 = 1
jnxJsSPUMonitoringSPUIndex.44 = 0
jnxJsSPUMonitoringSPUIndex.45 = 1
jnxJsSPUMonitoringCPUUsage.20 = 0
jnxJsSPUMonitoringCPUUsage.21 = 0
jnxJsSPUMonitoringCPUUsage.44 = 0
jnxJsSPUMonitoringCPUUsage.45 = 0
jnxJsSPUMonitoringMemoryUsage.20 = 64
jnxJsSPUMonitoringMemoryUsage.21 = 60
jnxJsSPUMonitoringMemoryUsage.44 = 64
jnxJsSPUMonitoringMemoryUsage.45 = 60
jnxJsSPUMonitoringCurrentFlowSession.20 = 0
jnxJsSPUMonitoringCurrentFlowSession.21 = 1
jnxJsSPUMonitoringCurrentFlowSession.44 = 0
jnxJsSPUMonitoringCurrentFlowSession.45 = 1
jnxJsSPUMonitoringMaxFlowSession.20 = 421888
jnxJsSPUMonitoringMaxFlowSession.21 = 843776
jnxJsSPUMonitoringMaxFlowSession.44 = 421888
jnxJsSPUMonitoringMaxFlowSession.45 = 843776
jnxJsSPUMonitoringCurrentCPSession.20 = 1
jnxJsSPUMonitoringCurrentCPSession.21 = 0
jnxJsSPUMonitoringCurrentCPSession.44 = 1
jnxJsSPUMonitoringCurrentCPSession.45 = 0
jnxJsSPUMonitoringMaxCPSession.20 = 2359296
jnxJsSPUMonitoringMaxCPSession.21 = 0
jnxJsSPUMonitoringMaxCPSession.44 = 2359296
jnxJsSPUMonitoringMaxCPSession.45 = 0
jnxJsSPUMonitoringNodeIndex.20 = 0
jnxJsSPUMonitoringNodeIndex.21 = 0
jnxJsSPUMonitoringNodeIndex.44 = 1
jnxJsSPUMonitoringNodeIndex.45 = 1
jnxJsSPUMonitoringNodeDescr.20 = node0
jnxJsSPUMonitoringNodeDescr.21 = node0
jnxJsSPUMonitoringNodeDescr.44 = node1
jnxJsSPUMonitoringNodeDescr.45 = node1
```

Copyright © 2013, Juniper Networks, Inc.

## show system alarms

**Syntax** show system alarms

**Release Information** Command introduced in Junos OS Release 11.1 for SRX Series devices.

**Description** Display active system alarms.

**Options** This command has no options.

**Additional Information** System alarms are preset. They include a **configuration** alarm that appears when no rescue configuration alarm is set and a **license** alarm that appears when a software feature is configured but no valid license is configured for the feature. For more information about system alarms, see the Junos OS System Basics Configuration Guide.

**Required Privilege Level** admin

**Related Documentation**
- Device and Routing Operations Monitoring

**List of Sample Output** show system alarms on page 2246

### Sample Output

show system alarms

```
user@host> show system alarms
5 alarms currently active
Alarm time               Class  Description
2012-05-29 16:47:18 UTC  Major  /var partition usage crossed critical threshold
2012-05-29 16:47:18 UTC  Minor  /var partition usage crossed high threshold
2012-05-29 16:47:18 UTC  Major  /root partition usage crossed critical threshold
2012-05-29 16:47:18 UTC  Minor  /root partition usage crossed high threshold
2012-05-29 16:47:18 UTC  Minor  Rescue configuration is not set
```


Copyright © 2013, Juniper Networks, Inc.

## show system autorecovery state

**Syntax** show system autorecovery state

**Release Information** Command introduced in Release 11.2 of Junos OS.

**Description** Performs checks and shows status of all autorecovered items.

**Required Privilege Level** view

**Related Documentation**
- request system autorecovery state on page 1534
- Device Configuration

**List of Sample Output** show system autorecovery state on page 2247

**Output Fields** Table 225 on page 2247 lists the output fields for the **show system autorecovery state** command. Output fields are listed in the approximate order in which they appear.

### Table 225: show system autorecovery state Output Fields

| Field Name | Field Description |
|---|---|
| File | The name of the file on which autorecovery checks are performed. |
| Slice | The disk partition on which autorecovery checks are performed. |
| Recovery Information | Indicates whether autorecovery information for the file or slice has been saved. |
| Integrity Check | Displays the status of the file's integrity check (passed or failed). |
| Action / Status | Displays the status of the item, or the action required to be taken for that item. |

## Sample Output

### show system autorecovery state

```
user@host> show system autorecovery state

Configuration:
File            Recovery Information    Integrity Check    Action / Status
rescue.conf.gz  Saved                   Passed             None
Licenses:
File            Recovery Information    Integrity Check    Action / Status
JUNOS282736.lic Saved                   Passed             None
JUNOS282737.lic Not Saved               Not checked        Requires save
BSD Labels:
Slice           Recovery Information    Integrity Check    Action / Status
s1              Saved                   Passed             None
s2              Saved                   Passed             None
s3              Saved                   Passed             None
s4              Saved                   Passed             None
```

Copyright © 2013, Juniper Networks, Inc.

## show system download

**Syntax** show system download <*download-id*>

**Release Information** Command introduced in Release 11.2 of Junos OS.

**Description** Display a brief summary of all the download instances along with their current state and extent of progress. If a **download-id** is provided, the command displays a detailed report of the particular download instance.

**Options**
- **download-id**—(Optional) The ID number of the download instance.

**Required Privilege Level** view

**Related Documentation**
- request system download start on page 1541
- Device Configuration

**List of Sample Output**
show system download on page 2249
show system download 1 on page 2249

**Output Fields** Table 226 on page 2248 lists the output fields for the **show system download** command. Output fields are listed in the approximate order in which they appear.

### Table 226: show system download Output Fields

| Field Name | Field Description |
|---|---|
| **ID** | Displays the download identification number. |
| **Status** | Displays the state of a particular download. |
| **Start Time** | Displays the start time of a particular download. |
| **Progress** | Displays the percentage of a download that has been completed. |
| **URL** | Displays the location of the downloaded file. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show system download

```
user@host> show system download
Download Status Information:
ID  Status      Start Time       Progress  URL
1   Active      May 4 06:28:36   5%        ftp://ftp-server//tftpboot/1m_file
2   Active      May 4 06:29:07   3%        ftp://ftp-server//tftpboot/5m_file
3   Error       May 4 06:29:22   Unknown   ftp://ftp-server//tftpboot/badfile
4   Completed   May 4 06:29:40   100%      ftp://ftp-server//tftpboot/smallfile
```

### show system download 1

```
user@host> show system download 1

Download ID     : 1
Status          : Active
Progress        : 6%
URL             : ftp://ftp-server//tftpboot/1m_file
Local Path      : /var/tmp/1m_file
Maximum Rate    : 1k
Creation Time   : May 4 06:28:36
Scheduled Time  : May 4 06:28:36
Start Time      : May 4 06:28:37
Error Count     : 0
```

Copyright © 2013, Juniper Networks, Inc.

## show system license (View)

**Syntax**
show system license
<installed | keys | status | usage>

**Release Information**
Command introduced in Release 9.5 of Junos OS. Logical system status option added in Release 11.2 of Junos OS.

**Description**
Display licenses and information about how licenses are used.

**Options**
**none**—Display all license information.

**installed**—(Optional) Display installed licenses only.

**keys**—(Optional) Display a list of license keys. Use this information to verify that each expected license key is present.

**status**—(Optional) Display license status for a specified logical system or for all logical systems.

**usage**—(Optional) Display the state of licensed features.

**Required Privilege Level**
view

**Related Documentation**
- Device Configuration

**List of Sample Output**
show system license on page 2252
show system license installed on page 2252
show system license keys on page 2252
show system license usage on page 2252
show system license status logical-system all on page 2253

**Output Fields**
Table 227 on page 2250 lists the output fields for the **show system license** command. Output fields are listed in the approximate order in which they appear.

### Table 227: show system license Output Fields

| Field Name | Field Description |
|---|---|
| **Feature name** | Name assigned to the configured feature. You use this information to verify that all the features for which you installed licenses are present. |
| **Licenses used** | Number of licenses used by the device. You use this information to verify that the number of licenses used matches the number configured. If a licensed feature is configured, the feature is considered used. |


Copyright © 2013, Juniper Networks, Inc.

Table 227: show system license Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Licenses installed** | Information about the installed license key:<br>• **License identifier**—Identifier associated with a license key.<br>• **License version**—Version of a license. The version indicates how the license is validated, the type of signature, and the signer of the license key.<br>• **Valid for device**—Device that can use a license key.<br>• **Features**—Feature associated with a license, such as data link switching (DLSw). |
| **Licenses needed** | Number of licenses required for features being used but not yet properly licensed. |
| **Expiry** | Time remaining in the grace period before a license is required for a feature being used. |
| **Logical system license status** | Displays whether a license is enabled for a logical system. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show system license

```
user@host> show system license

License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  av_key_kaspersky_engine               1            1           0    2012-03-30
 01:00:00 IST
  wf_key_surfcontrol_cpa                0            1           0    2012-03-30
 01:00:00 IST
  dynamic-vpn                           0            1           0    permanent
  ax411-wlan-ap                         0            2           0    permanent

Licenses installed:
  License identifier: JUNOS301998
  License version: 2
  Valid for device: AG4909AA0080
  Features:
    av_key_kaspersky_engine - Kaspersky AV
      date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST

  License identifier: JUNOS302000
  License version: 2
  Valid for device: AG4909AA0080
  Features:
    wf_key_surfcontrol_cpa - Web Filtering
      date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

### show system license installed

```
user@host> show system license installed

License identifier: JUNOS301998
  License version: 2
  Valid for device: AG4909AA0080
  Features:
    av_key_kaspersky_engine - Kaspersky AV
      date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST

  License identifier: JUNOS302000
  License version: 2
  Valid for device: AG4909AA0080
  Features:
    wf_key_surfcontrol_cpa - Web Filtering
      date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

### show system license keys

```
user@host> show system license keys

XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
         xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
         xxxxxx xxxxxx xxx
```

### show system license usage

```
user@host> show system license usage

                                  Licenses     Licenses    Licenses  Expiry
Feature name                             used     installed      needed
  av_key_kaspersky_engine               1            1           0    2012-03-30
 01:00:00 IST
```


Copyright © 2013, Juniper Networks, Inc.

```
  wf_key_surfcontrol_cpa                0          1          0    2012-03-30
01:00:00 IST
  dynamic-vpn                           0          1          0    permanent
  ax411-wlan-ap                         0          2          0    permanent
```

## show system license status logical-system all

```
user@host> show system license status logical-system all
Logical system license status:

logical system name                 license status
root-logical-system                 enabled
LSYS0                               enabled
LSYS1                               enabled
LSYS2                               enabled
```

## show system security-profile

**Syntax** show system security-profile (all-resource | *resource*) <detail | terse> <logical-system (all | *logical-system-name*)> <root-logical-system> <summary>

**Release Information** Command introduced in Release 11.2 of Junos OS. Support for application firewall added in Release 11.3 of Junos OS. Option to display all resources for a logical system added in Release 11.3 of Junos OS. Resource information for ports in source NAT pools with port translation added in Release 11.4 of Junos OS.

**Description** Display information about a resource allocated to the logical system in a security profile. For each resource specified, the number used by the logical system and the configured maximum and reserved values are displayed.

This command can be used by the master administrator to display resource information for the master logical system or user logical system. This command can also be used by the user logical system administrator to display resource information for a user logical system.

**Options** Either specify **all-resource** to display information about all resources allocated for the logical system, or specify one of the following resources:

- address-book—Address books.
- appfw-rule-set—Application firewall rule set entries.
- appfw-rule—Application firewall rule entries.
- auth-entry—Firewall authentication entries.
- cpu—CPU utilization.
- flow-gate—Flow gates, also known as pinholes.
- flow-session—Flow sessions.
- nat-cone-binding—Network Address Translation (NAT) cone bindings.
- nat-destination-pool—NAT destination pools.
- nat-destination-rule—NAT destination rules.
- nat-nopat-address—NAT without port address translations.
- nat-pat-address—NAT with port address translations.
- nat-pat-portnum—NAT source port numbers for port translation
- nat-port-ol-ipnumber—NAT port overloading IP numbers.
- nat-rule-referenced-prefix—NAT rule referenced IP-prefixes.
- nat-source-pool—NAT source pools.
- nat-source-rule—NAT source rules.
- nat-static-rule—NAT static rules.


Copyright © 2013, Juniper Networks, Inc.

- policy—Security policies.
- policy-with-count—Security policies with a count.
- scheduler—Schedulers.
- zone—Security zones.

detail | terse—(Optional) Display the specified level of output.

The following options are available only to the master administrator:

- logical-system—Display resource information for a specified user logical system. Specify **all** to display resource information for all logical systems, including the master logical system.
- root-logical-system—Display resource information for the master (root) logical system.
- summary—Display summary information about the resource for all logical systems.

**Required Privilege Level** view

**Related Documentation**
- security-profile resources on page 1281 configuration statement
- Logical Systems for Security Devices

**List of Sample Output**
show system security-profile all-resource on page 2257
show system security-profile policy on page 2257
show system security-profile cpu on page 2257
show system security-profile cpu logical-system all on page 2257
show system security-profile cpu summary on page 2258
show system security-profile nat-pat-portnum on page 2258
show system security-profile nat-pat-portnum summary on page 2258

**Output Fields** Table 228 on page 2255 lists the output fields for the **show system security-profile** command. Output fields are listed in the approximate order in which they appear.

### Table 228: show system security-profile Output Fields

| Field Name | Field Description |
|---|---|
| **logical system name** | Name of the logical system. |
| **security profile name** | Name of the security profile bound to the logical system. |
| **usage** | Number of resources that are currently being used by the logical system. |
| **reserved** | Number of resources that are guaranteed to be available to the logical system. |
| **maximum** | Number of resources that the logical system can use. The maximum does not guarantee that the amount specified for the resource in the security profile is available. The maximum is not applicable for CPU resources. |

Copyright © 2013, Juniper Networks, Inc.

Table 228: show system security-profile Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **CPU control** | **TRUE** if CPU control is enabled or **FALSE** if CPU control is not enabled. |
| **CPU control target** | Upper limit for CPU utilization on the device. The default value is 80 percent. |
| **CPU name** | Central point (CP) or services processing unit (SPU). CP utilization and average utilization of all SPUs is shown. The **detail** option shows CPU utilization on each SPU. |
| **drop rate** | Packets dropped for CPU control. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show system security-profile all-resource

```
user@host> show system security-profile all-resource

resource                                  usage    reserved     maximum

[logical system name:   root-logical-system]
[security profile name: Default-Profile]
address-book                                  0           0         512
auth-entry                                    0           0  2147483647
cpu on CP                                 0.00%       1.00%      80.00%
cpu on SPU                                0.00%       1.00%      80.00%
flow-gate                                     0           0      524288
flow-session                                  2           0     6291456
nat-cone-binding                              0           0       65536
nat-destination-pool                          0           0        4096
nat-destination-rule                          0           0        8192
nat-nopat-address                             0           0     1048576
nat-pat-address                               0           0        2048
nat-port-ol-ipnumber                          0           0           4
nat-rule-referenced-prefix                    0           0     1048576
nat-source-pool                               0           0        2048
nat-source-rule                               0           0        8192
nat-static-rule                               0           0       20480
policy                                        0           0       40000
policy-with-count                             0           0        1024
scheduler                                     0           0          64
zone                                          0           0         512
```

### show system security-profile policy

```
user@host> show system security-profile policy
logical system name   security profile name       usage    reserved     maximum

ls-product-design     ls-design-profile               0          40          50
```

### show system security-profile cpu

```
user@host> show system security-profile cpu
CPU control: TRUE
CPU control target: 80.00%
logical system name    profile name    CPU name    usage(%)    reserved(%)
drop rate(%)
root-logical-system    Default-Profile CP             0.00%          1.00%
     0.00%
root-logical-system    Default-Profile SPU            0.00%          1.00%
     0.00%
```

### show system security-profile cpu logical-system all

```
user@host> show system security-profile cpu logical-system all
CPU control: TRUE
CPU control target: 80.00%
logical system name    profile name    CPU name    usage(%)    reserved(%)
drop rate(%)
root-logical-system    Default-Profile CP             0.00%          1.00%
     0.00%
root-logical-system    Default-Profile SPU            0.00%          1.00%
     0.00%
ls-product-design      ls-design-profile CP           0.00%          0.00%
     0.00%
ls-product-design      ls-design-profile SPU          0.00%          0.00%
     0.00%
```

Copyright © 2013, Juniper Networks, Inc.

```
ls-marketing-dept      ls-acct-mrkt-profile CP        0.00%          0.00%
     0.00%
ls-marketing-dept      ls-acct-mrkt-profile SPU       0.00%          0.00%
     0.00%
```

Should the above output actually look as follows?

```
logical system name    security profile name    usage    reserved    maximum
root-logical-system    Default-Profile         67108864     0      134217728
lsys1                  profile1                193536     6000     134217728
```

### show system security-profile cpu summary

```
user@host> show system security-profile cpu summary
CPU control: TRUE
CPU control target: 80.00%

CPU type                :     CP
global used amount      :  0.00%
global maximum quota    : 80.00%
global available amount : 80.00%
total logical systems   :      3
total security profiles :      3
heaviest usage / user   :  0.00%      / root-logical-system
lightest usage / user   :  0.00%      / root-logical-system

CPU type                :    SPU
global used amount      :  0.00%
global maximum quota    : 80.00%
global available amount : 80.00%
total logical systems   :      3
total security profiles :      3
heaviest usage / user   :  0.00%      / root-logical-system
lightest usage / user   :  0.00%      / root-logical-system
```

### show system security-profile nat-pat-portnum

```
user@host> show system security-profile cpu nat-pat-portnum
CPU control: TRUE
CPU control target: 80.00%
logical system name    security profile name        usage(%)    reserved(%)
maximum
root-logical-system    Default-Profile CP             67108864          0
    134217728
```

### show system security-profile nat-pat-portnum summary

```
user@host> show system security-profile nat-pat-portnum summary
global used amount    :67302400
global maximum quota    :134217728
global available amount   :66915328
total logical systems    :2
total security profiles   :1
heaviest usage / user    :193536 / lsys1
```


Copyright © 2013, Juniper Networks, Inc.

## show system services dhcp client

**Syntax**
**show system services dhcp client**
**< *interface-name* >**
**<statistics>**

**Release Information** Command introduced in Release 8.5 of Junos OS.

**Description** Display information about DHCP clients.

**Options**
- none—Display DHCP information for all interfaces.
- ***interface-name*** —(Optional) Display DHCP information for the specified interface.
- **statistics**—(Optional) Display DHCP client statistics.

**Required Privilege Level** view and system

**Related Documentation**
- dhcp on page 181
- request system services dhcp on page 1547
- Device Configuration

**List of Sample Output**
show system services dhcp client on page 2261
show system services dhcp client ge-0/0/1.0 on page 2261
show system services dhcp client statistics on page 2261

**Output Fields** Table 229 on page 2259 lists the output fields for the **show system services dhcp client** command. Output fields are listed in the approximate order in which they appear.

### Table 229: show system services dhcp client Output Fields

| Field Name | Field Description |
|---|---|
| **Logical Interface Name** | Name of the logical interface. |
| **Client Status** | State of the client binding. |
| **Vendor Identifier** | Vendor ID. |
| **Server Address** | IP address of the DHCP server. |
| **Address obtained** | IP address obtained from the DHCP server. |
| **Lease Obtained at** | Date and time the lease was obtained. |
| **Lease Expires at** | Date and time the lease expires. |

Copyright © 2013, Juniper Networks, Inc.

Table 229: show system services dhcp client Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **DHCP Options** | • **Name: server-identifier**, **Value:**IP address of the name server.<br>• **Name: device**, **Value:** IP address of the name device.<br>• **Name: domain-name**, **Value:** Name of the domain. |
| **Packets dropped** | **Total** packets dropped. |
| **Messages received** | **Number of the following DHCP messages received:**<br>• **DHCPOFFER**—First packet received on a logical interface when DHCP is enabled.<br>• **DHCPACK**—When received from the server, the client sends an ARP request for that address and adds a (ARP response) timer for 4 seconds and stop the earlier timer added for DHCPACK.<br>• **DHCPNAK**—When a DHCPNAK is received instead of DHCPACK, the logical interface sends a DHCPDISCOVER packet. |
| **Messages sent** | **Number of the following DHCP messages sent:**<br>• **DHCPDECLINE**—Packet sent when ARP response is received and there is a conflict. The logical interface sends a new DHCPDISCOVER packet.<br>• **DHCPDISCOVER**—Packet sent on the interface for which the DHCP client is enabled.<br>• **DHCPREQUEST**—Packet sent to the DHCP server after accepting the DHCPOFFER. After sending the DHCPREQUEST, the device adds a retransmission-interval timer.<br>• **DHCPINFORM**—Packet sent to the DHCP server for local configuration parameters.<br>• **DHCPRELEASE**—Packet sent to the DHCP server to relinquish network address and cancel remaining lease.<br>• **DHCPRENEW**—Packet sent to the DHCP server to renew the address. The next message to be sent will be a DHCPREQUEST message, which will be unicast directly to the server.<br>• **DHCPREBIND**—Packet sent to any server to renew the address. The next message to be sent will be a DHCPREQUEST message, which will be broadcast. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show system services dhcp client

```
user@host> show system services dhcp client
Logical Interface Name       ge-0/0/1.0
      Hardware address        00:0a:12:00:12:12
      Client Status           bound
      Vendor Identifier       ether
      Server Address          10.1.1.1
      Address obtained        10.1.1.89
      update server           enabled
      Lease Obtained at       2006-08-24 18:13:04 PST
      Lease Expires at        2006-08-25 18:13:04 PST
 DHCP Options :
           Name: name-server, Value: [ 10.209.194.131, 2.2.2.2, 3.3.3.3 ]
           Name: server-identifier, Value: 10.1.1.1
           Name: router, Value: [ 10.1.1.80 ]
           Name: domain-name, Value: netscreen-50
```

## Sample Output

### show system services dhcp client ge-0/0/1.0

```
user@host> show system services dhcp client ge-0/0/1.0
Logical Interface name         ge-0/0/1.0
Hardware address        00:12:1e:a9:7b:81
Client status           bound
Address obtained        30.1.1.20
Update server           disabled
Lease obtained at       2007-05-10 18:16:18 UTC
Lease expires at        2007-05-11 18:16:18 UTC
DHCP options:
    Name: server-identifier, Value: 30.1.1.2
Code: 1, Type: ip-address, Value: 255.255.255.0
Name: name-server, Value: [ 77.77.77.77, 55.55.55.55 ]
Name: domain-name, Value: englab.juniper.net
```

## Sample Output

### show system services dhcp client statistics

```
user@host> show system services dhcp client statistics
Packets dropped:
    Total                     0
Messages received:
    DHCPOFFER                 0
    DHCPACK                   8
    DHCPNAK                   0
Messages sent:
    DHCPDECLINE               0
    DHCPDISCOVER              0
    DHCPREQUEST               1
    DHCPINFORM                0
    DHCPRELEASE               0
    DHCPRENEW                 7
    DHCPREBIND                0
```

Copyright © 2013, Juniper Networks, Inc.

## show system login lockout

**Syntax** show system login lockout

**Release Information** Command introduced in Release 11.2 of Junos OS.

**Description** Display the user names locked after unsuccessful login attempts.

**Required Privilege Level** view and system

**Related Documentation**
- lockout-period
- clear system login lockout on page 1484
- Device Configuration

**List of Sample Output** show system login lockout on page 2262

**Output Fields** Table 230 on page 2262 lists the output fields for the **show system login lockout** command. Output fields are listed in the approximate order in which they appear. Field names might be abbreviated (as shown in parentheses) when no level of output is specified or when the **detail** keyword is used.

### Table 230: show system login lockout

| Field Name | Field Description | Level of Output |
|---|---|---|
| **User** | Username | All levels |
| **Lockout start** | Date and time the username was locked | All levels |
| **Lockout end** | Date and time the username was unlocked | All levels |

## Sample Output

### show system login lockout

```
user@host>show system login lockout

User                 Lockout start           Lockout end
root                 2011-05-11 09:11:15 UTC 2011-05-11 09:13:15 UTC
```


Copyright © 2013, Juniper Networks, Inc.

## show system services dhcp relay-statistics

**Syntax** **show system services dhcp relay-statistics**

**Release Information** Command introduced in Release 8.5 of Junos OS.

**Description** Display information about the DHCP relay.

**Required Privilege Level** view and system

**Related Documentation**
- dhcp on page 181
- Device Configuration

**List of Sample Output** show system services dhcp relay-statistics on page 2264

**Output Fields** Table 231 on page 2263 lists the output fields for the **show system services dhcp relay-statistics** command. Output fields are listed in the approximate order in which they appear.

### Table 231: show system services dhcp relay-statistics Output Fields

| Field Name | Field Description |
|---|---|
| **Received packets** | Total DHCP packets received. |
| **Forwarded packets** | Total DHCP packet forwarded. |
| **Dropped packets** | Total DHCP packets dropped for the following reasons:<br>• **Due to a missing interface in the relay database**—Number of packets discarded because they did not belong to a configured interface.<br>• **Due to a missing matching routing instance**—Number of packets discarded because they did not belong to a configured routing instance.<br>• **Due to an error during packet read**—Number of packets discarded because of a system read error.<br>• **Due to an error during packet send**—Number of packets that the DHCP relay application could not send.<br>• **Due to an invalid server address**—Number of packets discarded because an invalid server address was specified.<br>• **Due to a missing valid local address**—Number of packets discarded because there was no valid local address.<br>• **Due to a missing route to the server or client**—Number of packets discarded because there were no addresses available for assignment. |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show system services dhcp relay-statistics

```
user@host> show system services dhcp relay-statistics
  Received packets: 4
  Forwarded packets: 4
  Dropped packets: 4
    Due to missing interface in relay database: 4
    Due to missing matching routing instance: 0
    Due to an error during packet read: 0
    Due to an error during packet send: 0
    Due to invalid server address: 0
    Due to missing valid local address: 0
    Due to missing route to server/client: 0
```


Copyright © 2013, Juniper Networks, Inc.

## show system services dynamic-dns

**Syntax** show system services dynamic-dns

**Release Information** Command introduced in Junos OS Release 12.1X44-D10.

**Description** Display information about dynamic DNS clients.

**Required Privilege Level** view

**Related Documentation**
- dynamic-dns

**List of Sample Output**
show system services dynamic-dns client on page 2266
show system services dynamic-dns client detail on page 2266

**Output Fields** When you enter this command, you are provided feedback on the status of your request. The following table lists the output fields for the **show system services dynamic-dns** command.

### Table 232: show system services dynamic-dns

| Field Name | Field Description |
|---|---|
| **Hostname** | Hostname of the registered client |
| **Server** | DDNS server name |
| **Agent** | Name of the DDNS agent |
| **Last response** | Status of the last response |
| **Last update** | Date and time of the last update |
| **Interface** | name of the interface |

Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show system services dynamic-dns client

```
user@host> show system services dynamic-dns client
Internal hostname      Server                  Last response
jnpr.ddo.jp             ddo.jp                  success
jnr.ddo.jp              ddo.jp                  failure
newsam.getmyip.com      members.dyndns.org      nochg
rkhetan.gotdns.com      members.dyndns.org      nochg
```

### show system services dynamic-dns client detail

```
user@host>show system services dynamic-dns client detail
Hostname     : jnpr.ddo.jp
Server       : ddo.jp
Agent        : branch-0.1
Last response: success
Last update  : 2006-08-29 04:02:52 PDT
Interface    : fe-0/0/0.0

Hostname     : jnr.ddo.jp
Server       : ddo.jp
Agent        : Branch-0.1
Last response: failure
Last update  : 2006-08-29 04:03:03 PDT
Interface    : fe-0/0/0.0

Hostname     : newsam.getmyip.com
Server       : members.dyndns.org
Agent        : Branch-0.1
Last response: nochg
Last update  : 2006-08-29 04:02:50 PDT
Username     : rkhetan
Interface    : fe-0/0/1.0
```


Copyright © 2013, Juniper Networks, Inc.

## show system services dns dns-proxy

**Syntax** show system services dns dns-proxy

**Release Information** Command introduced in Junos OS Release 12.1X44-D10.

**Description** Display domain name system (DNS) proxy information.

**Options**
- **none**—Display DNS proxy statistics information.
- **cache**—(Optional) Display the DNS proxy cache.
- **statistics**—(Optional) Display the DNS proxy statistics.

**Required Privilege Level** view

**Related Documentation**
- clear system services dns dns-proxy on page 1485
- dns-proxy on page 1236

**List of Sample Output**
show system services dns-proxy statistics on page 2269
show system services dns-proxy cache on page 2269
show system services dns-proxy cache <viewname V1> on page 2269

**Output Fields** lists the output fields for the **show system services dns-proxy** command. Output fields are listed in the table below:

### Table 233: show system services dns-proxy

| Field Name | Field Description |
|---|---|
| **DNS proxy statistics** | Display information about the DNS proxy.<br>• **Status**—State of the proxy server as Enabled or disabled.<br>• **Queries received**—Number of DNS queries received by the DNS proxy.<br>• **Responses sent**—Number of DNS responses sent by the DNS proxy.<br>• **Queries forwarded**—Number of DNS queries forwarded by the DNS proxy.<br>• **Negative responses**—Number of negative responses the DNS proxy sent to the DNS client.<br>• **Retry requests**—Number of retries the DNS proxy received from the DNS client.<br>• **Pending requests**—Number of pending queries the DNS proxy has yet to send the DNS client a response for.<br>• **Server failures**—Number of DNS proxy server failures. |
| **Hostname** | Hostname of the host that has been cached. |
| **IP address** | IP address of the host. |

Copyright © 2013, Juniper Networks, Inc.

Table 233: show system services dns-proxy *(continued)*

| Field Name | Field Description |
|---|---|
| **Time-to-live** | Length of time before an entry is purged from the DNS cache. |
| **Type** | Type of DNS Resource Record. For example, A records refer to IPv4 host addresses. |
| **Class** | Class of DNS. A parameter used to define a DNS Resource Record. For example, IN class is used for Internet domain names. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show system services dns-proxy statistics

```
user@host> show system services dns-proxy statistics
DNS proxy statistics        :
    DNS proxy statistics    :
    Status              : enabled
    IPV4 Queries received   : 30
    IPV6 Queries received   : 0
    Responses sent      : 30
    Queries forwarded   : 13
    Negative responses  : 23
    Positive responses  : 23
    Retry requests      : 0
    Pending requests    : 0
    Server failures     : 0
    Interfaces          : fe-0/0/0.0, fe-1/0/1.0
```

### show system services dns-proxy cache

```
user@host>show system services dns-proxy cache
Hostname                Time-to-live      Type        Class   IP address/Hostname
juniper.net               408               A           IN      207.17.137.229
whitestar.juniper.net     408               A           IN      172.17.27.50
scarlet.juniper.net       408               A           IN      172.17.28.11
bng-admin1.juniper.net    408               A           IN      10.209.194.131
wf-nis1.juniper.net       408               A           IN      10.10.4.202
asg-ns1.juniper.net       408               A           IN      10.16.0.11
ruby.juniper.net          408               A           IN      172.17.28.100
a.l.google.com            408               A           IN      216.239.53.9
b.l.google.com            408               A           IN      64.233.179.9
maps.l.google.com         408               A           IN      64.233.189.104
c.l.google.com            408               A           IN      64.233.161.9
d.l.google.com            408               A           IN      64.233.183.9
e.l.google.com            408               A           IN      66.102.11.9
g.l.google.com            408               A           IN      64.233.167.9
magenta.juniper.net.      408               A           IN      172.17.27.123
mail.juniper.net.         408               CNAME       IN
magenta.juniper.net.
```

### show system services dns-proxy cache <viewname V1>

```
user@host>show system services dns-proxy cache <viewname V1>
Hostname                Time-to-live    Type        Class     IP address/Hostname
yahoo.com.                408             A           IN        72.30.38.140
yahoo.com.                408             A           IN        98.139.183.24
yahoo.com.                408             A           IN        209.191.122.70
magenta.juniper.net.      495             A           IN        172.17.27.123
mail.juniper.net.         495             CNAME       IN        magenta.juniper.net.
d.root-servers.net.       424             A           IN        128.8.10.90
e.root-servers.net.       424             A           IN        192.203.230.10
f.root-servers.net.       424             A           IN        192.5.5.241
g.root-servers.net.       424             A           IN        192.112.36.4
h.root-servers.net.       424             A           IN        128.63.2.53
i.root-servers.net.       424             A           IN        192.36.148.17
j.root-servers.net.       424             A           IN        192.58.128.30
m.root-servers.net.       424             A           IN        202.12.27.33
```

Copyright © 2013, Juniper Networks, Inc.

## show system snapshot media

**Syntax** show system snapshot media *media-type*

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display the snapshot information for both root partitions on SRX Series devices

**Options**
- internal— Show snapshot information from internal media.
- usb— Show snapshot information from device connected to USB port.
- external— Show snapshot information from the external compact flash. This option is available on the SRX650 Services Gateway.

**Required Privilege Level** View

**Related Documentation**
- Upgrades and Downgrades

### show system snapshot media internal

**show system snapshot media internal**

```
Information for snapshot on       internal (/dev/da0s1a) (primary)
Creation date: Jan 15 10:43:26 2010
JUNOS version on snapshot:
  junos  : 10.1B3-domestic
Information for snapshot on       internal (/dev/da0s2a) (backup)
Creation date: Jan 15 10:15:32 2010
JUNOS version on snapshot:
  junos  : 10.2-20100112.0-domestic
```

### show system snapshot media usb

**show system snapshot media usb**

```
Information for snapshot on       usb (/dev/da1s1a) (primary)
            Creation date: Jul 24 16:16:01 2009
            JUNOS version on snapshot:
            junos  : 10.0I20090723_1017-domestic
            Information for snapshot on       usb (/dev/da1s2a) (backup)
            Creation date: Jul 24 16:17:13 2009
            JUNOS version on snapshot:
            junos  : 10.0I20090724_0719-domestic
```


Copyright © 2013, Juniper Networks, Inc.

## show system storage partitions (View SRX Series)

**Syntax** show system storage partitions

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Displays the partitioning scheme details on SRX Series devices.

**Required Privilege Level** View

**Related Documentation**
- Upgrades and Downgrades

### show system storage partitions (dual root partitioning)

**show system storage partitions**

```
Boot Media: internal (da0)
Active Partition: da0s2a
Backup Partition: da0s1a
Currently booted from: active (da0s2a)

Partitions Information:
  Partition  Size   Mountpoint
      s1a    293M   altroot
      s2a    293M   /
      s3e    24M    /config
      s3f    342M   /var
      s4a    30M    recovery
```

### show system storage partitions (single root partitioning)

**show system storage partitions**

```
Boot Media: internal (da0)
Partitions Information:
  Partition  Size   Mountpoint
      s1a    898M   /
      s1e    24M    /config
      s1f    61M    /var
```

### show system storage partitions (USB)

**show system storage partitions**

```
Boot Media: usb (da1)
Active Partition: da1s1a
Backup Partition: da1s2a
Currently booted from: active (da1s1a)

Partitions Information:
  Partition  Size   Mountpoint
      s1a    293M   /
      s2a    293M   altroot
      s3e    24M    /config
      s3f    342M   /var
      s4a    30M    recovery
```

Copyright © 2013, Juniper Networks, Inc.

## show wan-acceleration status

**Syntax** **show wan-acceleration status**

**Release Information** Command introduced in Release 8.5 of Junos OS.

**Description** Display the redirection status and related information about the WXC Integrated Services Module (ISM 200) for WAN acceleration.

**Required Privilege Level** view

**Related Documentation**
- request wan-acceleration login on page 1558

**List of Sample Output** show wan-acceleration status on page 2272

**Output Fields** Table 234 on page 2272 lists the output fields for the **show wan-acceleration status** command. Output fields are listed in the approximate order in which they appear.

### Table 234: show wan-acceleration status Output Fields

| Field Name | Field Description |
|---|---|
| **Redirection status** | Indicates whether traffic redirection to the WXC ISM 200 is active. |
| **Interface** | Name of the WXC ISM 200 interface. |
| **Primary address** | Address used to manage the WXC ISM 200, and as the source address of traffic sent across the WAN. |
| **Secondary address** | Source address of traffic destined for an alternate WAN path when the Multi-Path feature is configured (optional). |
| **JUNOS version** | Installed version of Junos OS. |
| **WXOS version** | Installed version of WXOS. |
| **JUNOS/WXOS protocol** | Indicates whether the Junos OS and WXOS versions are compatible. |

## Sample Output

show wan-acceleration status

```
user@host> show wan-acceleration status
Redirection status: active, Interface: wx-2/0/0
Primary address: 10.87.5.2, Secondary address: 0.0.0.0
JUNOS version: 9.0R1 Enhanced Services
WXOS version: 5.4.6.0j
JUNOS/WXOS protocol: Version compatible
```


Copyright © 2013, Juniper Networks, Inc.

## show wlan access-points

**Syntax** show wlan access-points <*ap-name*> <detail> <virtual-access-points> <detail> <client-associations> <neighbors>

**Release Information** Command introduced in Release 10.0 of Junos OS.

**Description** Display information about the wireless LAN access points configured on the services gateway.

**Options**

- none—Display the status of all access points on the services gateway.
- *ap-name*—(Optional) Display information about a specific access point on the services gateway.
- **detail**—(Optional) Display detailed information about a specific access point on the services gateway.
- **virtual-access-points**—(Optional) Display information about the virtual access points configured on a specific access point on the services gateway.
- **detail**—(Optional) Display detailed information about a specific virtual access point on the services gateway.
- **client-associations**—(Optional) Display information about the client associations on a specific access point on the services gateway.
- **neighbors**—(Optional) Display information about the neighbor access points, including the last beacon (receive) time with the most active neighbors displayed first, in descending order.

**Required Privilege Level** view

**Related Documentation**

- clear wlan access-point neighbors on page 1486
- WLAN Configuration and Administration

**List of Sample Output**

show wlan access-points on page 2275
show wlan access-points wl-ap8 on page 2275
show wlan access-points wl-ap8 detail on page 2275
show wlan access-points wl-ap8 virtual-access-points on page 2275
show wlan access-points wl-ap8 virtual-access-points detail on page 2276
show wlan access-points wl-ap8 neighbors on page 2276

**Output Fields** Table 235 on page 2273 lists the output fields for the **show wlan access-points** command. Output fields are listed in the approximate order in which they appear.

### Table 235: show wlan access-points Output Fields

| Field Name | Field Description |
|---|---|
| **Access-Point** | Name of the access point. |

Copyright © 2013, Juniper Networks, Inc.

Table 235: show wlan access-points Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| **Type** | Access point type, for example “Ext” for external access point. |
| **Interface** | Interface on the SRX Series device to which the access point is connected. |
| **Radio-mode/Channel** | Physical Layer (PHY) standard mode of the radio and the channel used for transmitting and receiving. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show wlan access-points

```
user@host> show wlan access-points
Active access points information


Access-Point   Type   Interface    Radio-mode/Channel
wl-ap8         Ext    vlan.0       an/44, bgn/4
wl-ap6         Ext    vlan.0       an/149, bgn/4
```

### show wlan access-points wl-ap8

```
user@host> show wlan access-points wl-ap8
Active access point information

Access Point        : wl-ap8
Type                : External
Access Interface    : vlan.0
IPv4 Address        : 40.0.0.70
Management Status   : Managed
Packet Capture      : Off
Radio1              : Mode: IEEE 802.11a/n, Channel: 44 (5220 MHz)
Radio2              : Mode: IEEE 802.11b/g/n, Channel: 4 (2427 MHz
```

### show wlan access-points wl-ap8 detail

```
user@host> show wlan access-points wl-ap8 detail
Active access point detail information

Access Point          : wl-ap8
Type                  : External
Location              : Default Location
Serial Number         : BE2610AF0019
Firmware Version      : 10.1.3.7
Alternate Version     : 10.1.3.7
Regulatory Domain     : FCC
Country               : UNDEFINED
Access Interface      : vlan.0
Packet Capture        : Off
Ethernet Port:
    MAC Address       : 80:71:1F:3D:C5:00
    IPv4 Address      : 40.0.0.70
Radio1:
    Status            : On
    MAC Address       : 80:71:1F:3D:C5:00
    Mode              : IEEE 802.11a/n
    Channel           : 44 (5220 MHz)
Radio2:
    Status            : On
    MAC Address       : 80:71:1F:3D:C5:10
    Mode              : IEEE 802.11b/g/n
    Channel           : 4 (2427 MHz)
```

### show wlan access-points wl-ap8 virtual-access-points

```
user@host> show wlan access-points wl-ap8 virtual-access-points
Virtual access points information

Access point name         : wl-ap8
Radio1:
  VAP0:
    SSID                  : wl-ap8vap0
    MAC Address           : 80:71:1F:3D:C5:00
```

Copyright © 2013, Juniper Networks, Inc.

```
    VLAN ID               : 1
    Traffic Statistics    :
      Input Bytes         : 0
      Output Bytes        : 722
      Input Packets       : 0
      Output Packets      : 6
Radio2:
  VAP0:
    SSID                  : wl-ap8vap0-rad2
    MAC Address           : 80:71:1F:3D:C5:10
    VLAN ID               : 1
    Traffic Statistics    :
      Input Bytes         : 0
      Output Bytes        : 497
      Input Packets       : 0
      Output Packets      : 5
```

### show wlan access-points wl-ap8 virtual-access-points detail

```
user@host> show wlan access-points wl-ap8 virtual-access-points detail
Virtual access points information

Access point name           : wl-ap8
Radio1:
  VAP0:
    SSID                    : wl-ap8vap0
    MAC Address             : 80:71:1F:3D:C5:00
    VLAN ID                 : 1
    VAP SECURITY            : wpa-personal
    Wpaversion              :
     Wpa2                   : Enable
     Wpa                    : Disable
    Ciper-Suites            :
     Ccmp(AES)              : Enable
     Tkpi                   : Disable
     Broadcast-Refresh-Rate : 0
Radio2:
  VAP0:
    SSID                    : wl-ap8vap0-rad2
    MAC Address             : 80:71:1F:3D:C5:10
    VLAN ID                 : 1
    VAP SECURITY            : wpa-personal
    Wpaversion              :
     Wpa2                   : Enable
     Wpa                    : Disable
    Ciper-Suites            :
     Ccmp(AES)              : Enable
     Tkpi                   : Disable
     Broadcast-Refresh-Rate : 0
```

### show wlan access-points wl-ap8 neighbors

```
user@host> show wlan access-points wl-ap8 neighbors
Access point neighbors information

Access point: wl-ap8
MAC               Sec/WPA  Band/Chan/Sig  Last Beacon      SSID
80:71:1f:3d:f7:90 On/Off   2.4/4/-3       Jul 31 14:24:10  wl-ap6vap0-rad2
80:71:1f:3d:db:00 On/Off   5/44/-36        Jul 31 14:16:41  juniper-default
```


Copyright © 2013, Juniper Networks, Inc.

## show wlan diagnostics

**Syntax** show wlan diagnostics

**Release Information** Command introduced in Release 10.2 of Junos OS.

**Description** Display the Wireless LAN diagnostics information status such as Packet Capture and System log messages.

**Required Privilege Level** maintenance

**Related Documentation**
- WLAN Configuration and Administration

### Example

**user@host# show wlan diagnostics**

```
Active access points diagnostics information

    Access-Point        Pcap-Status   Pcap-Interface   Syslog-Status
    mav0                Off           None             Off
    mav1                Off           None             Off
```

Copyright © 2013, Juniper Networks, Inc.

## show wireless-wan adapter

**Syntax** show wireless-wan adapter

**Release Information** Command introduced in Release 11.4R2 of Junos OS.

**Description** Displays all configured adapters along with their IP addresses.

**Options**
- **adapter-name**—Displays the name of the adapter.
- **detail**—Displays details of the adapter.
- **firmware**—Displays the firmware upgrade status.
- **modem**—Displays information about the specified modem port.

**Required Privilege Level** view

**Related Documentation**
- request wireless-wan adapter firmware upgrade on page 1561
- WLAN Configuration and Administration

**List of Sample Output**
show wireless-wan adapter on page 2281
show wireless-wan adapter CX111-0 on page 2281
show wireless-wan adapter CX111-0 detail on page 2281
show wireless-wan adapter firmware upgrade CX111-0 on page 2281
show wireless-wan adapter detail on page 2281
show wireless-wan adapter CX111-0 modem [usb1|usb2 |usb3|expresscard] on page 2282

**Output Fields** Lists the output fields for the **show wireless-wan adapter** command.

Table 236: show wireless-wan adapter Output Fields

| Field Name | Field Description |
|---|---|
| **Adapter information fields** | |
| Adapter name | Name of the adapter. |
| Adapter firmware version | Displays the firmware version. |
| **Modem information fields** | |
| Number of cellular modems connected | Displays the number of modems connected to the adapter. |
| Cellular modem index | Displays the modem index number. |
| Modem information | Displays the modem description. |
| Modem port | Displays the modem port. |


Copyright © 2013, Juniper Networks, Inc.

Table 236: show wireless-wan adapter Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| Modem signal strength | Displays the cellular modems signal strength, given in dBm's. |
| Modem status | Displays the modem WAN connection details. The available status options are: established, establishing, ready, error, disconnected, disconnecting, suspended, empty, not configured and user stopped. |
| Modem ecio | Displays the cellular modems Ec/ Io ratio given in dBm's |
| Modem serial number | Displays the unique serial number of the device. |
| Modem firmware version | Displays the current firmware version of the modem. |
| Connection status | Displays the current operational state of the interface. The available status options are: Up and Down. |
| IP address | Displays the address information for the modem, received from WAN network. |
| Sent bytes | Displays the total number of octets transmitted out of the interface, including framing characters. |
| Sent packets | Displays the total number of packets that higher-level protocols requested to be transmitted to a subnetwork-unicast address, including the packets that were discarded or not sent. |
| Outbound packet discards | Displays the number of outbound packets that are chosen to be discarded even after no errors being detected to prevent their being transmitted. One possible reason for discarding such a packet might be to free up buffer space. |
| Outbound packet errors | Displays the number of outbound packets that cannot be transmitted because of errors. |
| Received bytes | Displays the total number of octets received on the interface, including framing characters. |
| Received packets | Displays the number of subnetwork-unicast packets delivered to a higher-layer protocol. |
| Inbound packet discards | Display the number of inbound packets that are chosen to be discarded even after no errors being detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet might be to free up buffer space. |
| Inbound packet errors | Displays the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. |
| **Firmware information fields** | |
| Adapter current firmware version | Displays the current firmware version. |
| **Adapter firmware upgrade mode** | Displays the firmware upgrade mode. The available modes are none, auto, and manual. |
| Adapter firmware upgrade URL | Displays the firmware upgrade URL. |

Copyright © 2013, Juniper Networks, Inc.

Table 236: show wireless-wan adapter Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| Adapter firmware upgrade status | Displays the firmware upgrade status. The available status options are idle, upgrading, uptodate, updateAvail, and failure. |


Copyright © 2013, Juniper Networks, Inc.

## Sample Output

### show wireless-wan adapter

```
user@host> show wireless-wan adapter

Adapter information
Adapter-name         IP-address
CX111-0              192.168.0.1
CX111-1              192.168.0.2
CX111-2              192.168.0.3
```

### show wireless-wan adapter CX111-0

```
user@host> show wireless-wan adapter CX111-0

Adapter information
Adapter name : CX111-0
Adapter firmware version             : "1.9.0"
Number of cellular modems connected  : 2
```

### show wireless-wan adapter CX111-0 detail

```
user@host> show wireless-wan adapter CX111-0 detail

Adapter name : CX111-0
Adapter firmware version             : "1.9.0"
Number of cellular modems connected  : 2

 Cellular modem index: 1
 Modem information: "AC503"
 Modem port: "ExpressCard"
 Modem signal strength: 0 dBm

 Cellular modem index: 2
 Modem information: "USB 308"
 Modem port: "USB1"
 Modem signal strength: -94 dBm
```

### show wireless-wan adapter firmware upgrade CX111-0

```
user@host> show wireless-wan adapter firmware upgrade CX111-0

Adapter firmware upgrade details
 Adapter current firmware version: "1.9.0"
 Adapter firmware upgrade mode: auto
 Adapter firmware upgrade URL: Juniper cloud server
 Adapter firmware upgrade status: upgrading
```

### show wireless-wan adapter detail

```
user@host> show wireless-wan adapter detail

Adapter name : CX111-0
Adapter firmware version             : "1.9.0"
Number of cellular modems connected  : 2

 Cellular modem index: 1
 Modem information: "AC503"
 Modem port: "ExpressCard"
 Modem signal strength: 0 dBm

 Cellular modem index: 2
 Modem information: "USB 308"
```

Copyright © 2013, Juniper Networks, Inc.

```
 Modem port: "USB1"
 Modem signal strength: -94 dBm

Adapter name : CX111-1
Adapter firmware version             : "1.9.0"
Number of cellular modems connected  : 1

 Cellular modem index: 1
 Modem information: "AC503"
 Modem port: "ExpressCard"
 Modem signal strength: 0 dBm

Adapter name : CX111-2 is not reachable
Adapter name : CX111-3 is not reachable
```

### show wireless-wan adapter CX111-0 modem [usb1|usb2 |usb3|expresscard]

```
user@host> show wireless-wan adapter CX111-0 modem usb1

Modem information: "AC503"
Modem port: "ExpressCard"
Modem signal strength: -60 dBm
Modem status: established
Modem ecio: 0 dBm
Modem serial number: "356470031505691"
Modem firmware version: "M3_0_10_1AP C:/WS/FW/M3_0_10_1AP/MDM8200/SRC/AMSS
2010/03/29 17:52:11"
Connection status: Up
IP address:  49.203.226.149
Sent bytes: 726
Sent packets: 9
Outbound packet discards: 0
Outbound packet errors: 0
Received bytes: 1063
Received packets: 7
Inbound packet discards: 0
Inbound packet errors: 0
```


Copyright © 2013, Juniper Networks, Inc.

PART 3

# Index


- Index on page 2285


Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.

# Index

## Symbols


#, comments in configuration statements....l
( ), in syntax descriptions....l
(antivirus utm-policy)....641
< >, in syntax descriptions....xlix
[ ], in configuration statements....l
{ }, in configuration statements....l
| (pipe), in syntax descriptions....l


## A


accept-source-mac....172
Access Configuration Statement Hierarchy....3
access-point statement
    WLAN....1304
access-point-name statement....173
access-point-options statement
    WLAN....1308
access-point-queues statement
    WLAN....1309
access-profile statement
    (Dynamic VPNs)....367
    (IPsec VPNs)....367
Accounting-Options Configuration Statement Hierarchy....53
ack-number statement....368
action
    GTP
        GPRS....369
action (web filtering)....372
action statement....371
    (Security Application-Level DDoS)....370
action-profile statement....373
actions
    (Services)....1137
activation-priority statement....173
active-policy statement....374
adaptive-shaper statement....113
adaptive-shapers statement....114
address statement....1138, 1197
    (ARP Proxy Services Gateway)....376
    (Destination NAT )....376
    (IKE Gateway)....377
    (NDP Proxy)....378
    (Source NAT )....378
    address book....375
address-assignment statement....8
address-blacklist....379
address-book statement....380, 872, 1220
address-mapping statement....381
address-persistent statement....382
address-pool statement....10
address-set statement....382
address-whitelist....383
admin-email statement....383
admin-search statement....11
administrator statement....384
administrator-email....385
administrator-email statement
    (Security Fallback Block)....384
after-keygeneration statement....1221
aging statement....385
alarm statement....387
alarm-threshold statement....386
alarm-without-drop statement....386
alarms....1383, 1753
alert statement....388
alg statement....57, 389
alg-ike-esp-nat....394
alg-manager....394
alg-support-lib....395
algorithm statement....395
all-day statement....298
all-tcp statement....396
allow-dns-reply statement....396
allow-duplicates statement....1221
allow-email (virus-detect)....397
allow-email statement
    (Security Fallback Block)....397
allow-icmp-without-flow statement....398
always-send statement....398
analysis statement....399
annex....174
anomaly statement....399
anti-spam statement (feature-profile)....400
anti-spam statement (utm-policy)....400
anti-virus statement
    (Security Feature Profile)....401
anti-virus statement (utm-policy)....405
apn (gtp)....406
appfw-rule statement....1223

appfw-rule-set statement....1222
application (potential violation) statement....407
application (Security IDP)....409
application identification
services....1142
application identification services
nested application settings....1165
application statement
(application identification)....1139, 1164
(Security Application-Level DDoS)....408
(Security Custom Attack)....408
(Security Policies)....409
application-ddos....411
application-ddos statement....410
application-firewall statement....412, 737
(Security Policies)....413
application-group statement....1141
application-identification statement....413
application-level DDoS rule statement....895
application-protocol statement....58
application-proxy statement
utm....414
application-screen statement
(H323)....414
(MGCP)....415
(SCCP)....416
(SIP)....417
application-services....418
application-services statement
(Security Policies)....420
application-system-cache statement....1144
application-system-cache-timeout
statement....1145
application-tracking statement....421
zones....421
application-traffic-control statement....115
Application Services....422
Applications Configurations Statement
Hierarchy....55
apply-groups statement....174
arbitration-inter-frame-space statement
WLAN....1310
arp-resp statement....175
assemble statement statement....11
associate-timeout statement....422
attach statement....423
attack-threshold statement....423
attack-type (Security IDP)....428
attack-type statement
(Security Anomaly)....425
(Security Chain)....426
(Security Signature)....432
attacks statement
(Security Exempt Rulebase)....424
(Security IPS Rulebase)....425
audible statement
security alarms....436
auth-entry statement....1224
authentication statement....436, 437
authentication-algorithm statement....438, 439
authentication-method statement....175, 440
authentication-order statement....12
authentication-source statement....441
authorization statement....1203
auto-re-enrollment statement....441
automatic statement....442

## B

BA classifier....116
background-queue statement
WLAN....1311
bandwidth (radio-router)....176
banner statement
(FTP, HTTP, Telnet)....12
(Web authentication)....13
base-distinguished-name statement....14
beacon-interval statement
WLAN....1311
bearer-bandwidth-limit statement....176
best-effort-queue statement
WLAN....1312
bind-interface statement....442
block-command statement....443
block-content-type statement....443
block-extension statement....444
block-message....444
block-mime statement....445
braces, in configuration statements....l
brackets
angle, in syntax descriptions....xlix
square, in configuration statements....l
bridge domain
routing interface....74
VLAN identifier....76
VLAN identifier list....77
bridge statement....446


Copyright © 2013, Juniper Networks, Inc.

Bridge-Domains Configuration Statement Hierarchy....71
bridge-domains statement....72
bridge-options statement....73
broadcast-multicast-rate-limit statement
WLAN....1313
bundle statement....177

## C

c-timeout statement....447
ca-identity statement....447
ca-profile statement....448, 1145
ca-profile-name statement....449
cache....449
cache-prune-chunk-size statement....451
cache-size statement
(Security)....451
call-flood statement....452
captive-portal statement....1146
captive-portal statement (Unified Access Control policy)....1147
capture-file statement....453
category (web filtering)....456
category statement
(Security Dynamic Attack Group)....454
(Security Logging)....455
cellular-options statement....178
certificate statement....462
certificate-id statement....462
certificate-verification....1148
certificates
PKI
local certificates, loading manually....1516
certificates statement....463
certification-authority statement....464
chain statement....465
challenge-password statement....466
channel statement
WLAN....1314
Chassis Configuration Statement Hierarchy....79
ciphers....1225
class name....119
Class-of-Service Configuration Statement Hierarchy....109
classifiers (Cos)....116
clear chassis cluster control-plane statistics command....1358
clear chassis cluster data-plane statistics command....1359
clear chassis cluster failover-count command....1360
clear chassis cluster ip-monitoring failure-count....1362
clear chassis cluster ip-monitoring failure-count ip-address....1363
clear chassis cluster statistics command....1364
clear dhcp client binding command....1365
clear dhcp client statistics command....1366
clear dhcp relay binding command....1367
clear dhcp relay statistics command....1368
clear dhcp server binding command....1369
clear dhcp server statistics command....1370
clear dhcpv6 server binding command....1371
clear dhcpv6 server statistics command....1372
clear firewall command....1374
clear gtp tunnels command....1375
clear interfaces statistics swfabx command....1376
clear lacp statistics interfaces command....1377
clear network-access requests pending command....1378
clear network-access requests statistics command....1379
clear network-access securid-node-secret-file command....1380
clear oam ethernet connectivity-fault-management path-database command....1381
clear oam ethernet connectivity-fault-management statistics command....1382
clear security alarms command....1383
clear security alg h323 counters command....1386
clear security alg ike-esp-nat command....1387
clear security alg mgcp calls command....1388
clear security alg mgcp counters command....1389
clear security alg sccp calls command....1390
clear security alg sccp counters command....1391
clear security alg sip calls command....1392
clear security alg sip counters command....1393
clear security application-firewall rule-set statistics....1394
clear security application-firewall rule-set statistics logical-system....1395
clear security datapath-debug counters command....1396
clear security dns-cache command....1397
clear security dynamic-vpn all command....1398
clear security dynamic-vpn user command....1399
clear security firewall-authentication history address command....1401

Copyright © 2013, Juniper Networks, Inc.

clear security firewall-authentication history command....1400
clear security firewall-authentication history identifier command....1402
clear security firewall-authentication users address command....1404
clear security firewall-authentication users command....1403
clear security firewall-authentication users identifier command....1405
clear security flow ip-action command....1406
clear security flow session all command....1408
clear security flow session application command....1409
clear security flow session destination-port command....1411
clear security flow session destination-prefix command....1412
clear security flow session family ....1414
clear security flow session interface command....1415
clear security flow session protocol command....1416
clear security flow session resource-manager command....1418
clear security flow session session-identifier command....1422
clear security flow session source-port command....1423
clear security flow session source-prefix command....1424
clear security flow statistics....1426
clear security gprs sctp counters command....1427
clear security group-vpn member ike security-associations command....1430
clear security group-vpn member ipsec security-assocations command....1431
clear security group-vpn member kek security-assocations command....1432
clear security group-vpn server command....1433
clear security idp ....1434
clear security idp application-ddos cache....1435
clear security idp attack table command....1436
clear security idp counters application-identification command....1437
clear security idp counters dfa command....1438
clear security idp counters flow command....1439
clear security idp counters http-decoder command....1440
clear security idp counters ips command....1441
clear security idp counters log command....1442
clear security idp counters packet command....1443
clear security idp counters policy-manager command....1444
clear security idp counters tcp-reassembler command....1445
clear security idp ssl-inspection session-id-cache command....1446
clear security ike respond-bad-spi-count command....1447
clear security ike security-associations command....1448
clear security ipsec security-associations command....1450
clear security ipsec statistics command....1452
clear security log file command....1456
clear security logcommand....1454
clear security nat incoming-table command....1457
clear security nat source persistent-nat-table command....1458
clear security nat statistics destination pool command....1459
clear security nat statistics destination rule command....1460
clear security nat statistics source pool command....1461
clear security nat statistics source rule command....1462
clear security nat statistics static rule command....1463
clear security pki key-pair command....1464
clear security pki local-certificate command....1465
clear security policies hit-count command....1466
clear security policies statistics command....1467
clear security screen statistics command....1468
clear security screen statistics interface command....1469
clear security screen statistics zone command....1470
clear security user-identification local-authentication-table command....1471
clear security utm anti-spam statistics....1472
clear security utm antivirus statistics....1473
clear security utm content-filtering statistics....1474
clear security utm session....1475
clear security utm web-filtering statistics....1476
clear services application-identification application-statistics command....1477


Copyright © 2013, Juniper Networks, Inc.

clear services application-identification application-statistics cumulative command....1478
clear services application-identification application-statistics interval command....1479
clear services application-identification application-system-cache command....1480
clear services application-identification counter command....1419, 1428, 1481
clear services application-identification counter ssl-encrypted-sessions command....1482
clear services ssl proxy statistics command....1483
clear system login lockout command....1484
clear wlan access-point neighbors command....1486
clear-threshold statement....466
client-group statement....15
client-identifier (dhcp-client) statement....179
client-identifier statement....179
client-idle-timeout statement....15
client-list-name statement....1204
client-name-filter statement....16
client-session-timeout statement....16
clients statement....467
cluster statement....84
co-location statement
security....467
code statement....468
code-points statement....117
comments, in configuration statements....l
compression-device statement....180
condition statement....236
config-check statement....468
configuration-file statement....17
connection-flood statement....469
connection-rate-threshold statement....469
connections-limit statement....470
console statement
WLAN....1314
container statement....471
content-decompression-max-memory-kb statement....472
content-decompression-max-ratio statement....473
content-filtering....474
content-filtering (utm-policy)....475
content-size statement....476
(Security Antivirus Sophos Engine)....477
content-size-limit statement....478
context statement
(Security Application-Level DDoS)....479
(Security Custom Attack)....479
control-link-recovery statement....85
control-ports statement....86
conventions
notice icons....xlviii
text and syntax....xlix
corrupt-file statement....480
count statement....17
(Security Custom Attack)....480
(Security Policies)....481
country statement
WLAN....1315
cpu statement....1226
credit (radio-router)....180
crl statement....482
cryptographic-self-test statement....483
curly braces, in configuration statements....l
custom-attack statement....484
custom-attack-group statement....489
custom-attack-groups (Security IDP)....489
custom-attacks statement....490
custom-block-message....490
custom-ciphers....1149
custom-message statement
(Security Content Filtering)....491
(Security Email Notify)....491
(Security Fallback Block)....492
(Security Fallback Non-Block)....493
(Security Virus Detection)....494
custom-message-subject (email-notify) statement....494
custom-message-subject statement
(Security Fallback Block)....495
(Security Fallback Non-Block)....496
(Security Virus Detection)....497
custom-objects....498
custom-tag-string....499
custom-url-category....500
customer support....l
contacting JTAC....l

## D

daily statement....299
data-length statement....501
data-rate statement....181
datapath-debug
security....502

Copyright © 2013, Juniper Networks, Inc.

datapath-debug statement....502
day-of-month statement....1227
day-of-week statement....1228
dead-peer-detection statement....503
decompress-layer statement....504
decompress-layer-limit statement....504
decryption-failures statement....505
default....506
default (web-filtering fallback-settings)....508
default statement....118
(Security Antivirus....506
(Security Antivirus Sophos Engine)....507
default-policy statement....509
default-profile statement....18
default-rule statement....510
demand-circuit statement
RIP....261
deny statement
(Security Policies)....510
(SIP)....511
description statement....59, 300, 515, 516, 518, 519
(Security IDP Policy)....513
(Security Policies)....517
Address Book....512
NAT Pool....514
destination statement
(Destination NAT Services Gateway)....520
(Security IP Headers Attack)....521
destination-address statement
(destination NAT )....522
(Security IDP Policy)....523
(Security Policies Flag)....525
(Security Policies)....524
(Source NAT)....526, 527
destination-address-name statement
(Destination NAT)....527
destination-except statement....528
destination-ip potential violation statement....529
destination-ip statement....530
destination-ip-based statement....530
destination-nat statement
(Destination NAT Services Gateway)....531
destination-port statement....60
(Destination NAT)....531
(Security Signature Attack)....532
(Source NAT)....532
destination-threshold statement....533
detect-shellcode statement....534
detector statement....534
df-bit statement....535
dh-group statement....536
dhcp statement....181
dhcp-attributes statement IPv4....19
dhcp-attributes statement IPv6....20
dhcp-client statement....182
dhcp-local-server....1231
dhcpv6....1229
direction statement
(Security Custom Attack)....537
(Security Dynamic Attack Group)....538
disable....539
disable statement....228, 262
disable-call-id-hiding statement....539
disable-dot11d statement
WLAN....1317
display-host (virus-detection)....540
display-host statement
(Security Fallback Block)....540
distinguished-name statement....21, 541
dlv ....1234, 1277
DNS ....1235
dns statement....542
dns-proxy....1236
DNSSEC ....1234, 1237
docsis
profile....189, 215
documentation
comments on....l
domain-name statement....21
domain-type statement....73
dot1x statement
WLAN....1317
dot1x-supplicant statement
WLAN....1318
download
application-identification package....1150
download-profile (ftp antivirus utm-profile)....543
download-profile (ftp content-filtering
utm-profile)....543
drop statement
(GTP)....544
(SCTP)....549
dscp-rewrite....551, 1151
dslite-softwire-initiator statement....1238
dtim-period statement
WLAN....1318
duration statement....228
dynamic statement....552


Copyright © 2013, Juniper Networks, Inc.

dynamic-application statement....552
dynamic-application-group statement....553
dynamic-attack-group statement....554
dynamic-attack-groups (Security IDP)....555
dynamic-call-admission-control statement....183
dynamic-dns....1239
dynamic-vpn statement....556

## E

early-ageout statement....557
email-notify statement....557
enable....558
enable statement
  gtp
    gprs....558
enable-all-qmodules statement....559
enable-flow-tracing
  Services....1151
enable-heuristics statement....1152
enable-packet-pool statement....559
enable-session-cache....1152
encapsulation statement....184
encryption statement....560
encryption-algorithm statement....561
encryption-failures statement....562
endpoint-registration-timeout statement....562
engine-not-ready statement....563
  (Security Antivirus Sophos Engine)....564
enrollment statement....565
ENTER AN INDEX ENTRY. wireless-wan....1193
establish-tunnels statement....566
ethernet statement
  WLAN....1319
Event-Options Configuration Statement Hierarchy....141
event-rate statement....566
exception statement
  (Security Antivirus Mime Whitelist)....567
exception statement (content-filter block-mime)....567
exclude statement....301, 568
exclude-context-values statement....569
expression statement....570
external statement
  WLAN....1320
external-interface statement
  (IKE Gateway)....571, 1114
  (Manual Security Association)....571

## F

fabric-options statement....185
fail statement....22
fallback-block statement
  (Security Antivirus)....572
fallback-non-block statement
  (Security Antivirus)....573
fallback-options statement
  (Security Antivirus Juniper Express Engine)....574
  (Security Antivirus Kaspersky Lab Engine)....575
  (Security Antivirus Sophos Engine)....576
fallback-settings (web-filtering juniper-local)....577
fallback-settings (web-filtering surf-control-integrated)....576
fallback-settings (web-filtering websense-redirect)....577
false-positives statement....578
family bridge statement....186
family inet statement....187
family inet6 statement....188
family statement....579
feature-profile....580
fifo-max-size....586
file *See* security log
  Services....1153
filename-extension....588
files
  Services....1153
filters statement....589
fin-no-ack statement....590
FIPS self-tests....1240
  manually executing....1543
  periodic....1267
  periodic, day of the month....1227
  periodic, day of the week....1228
  periodic, monthly....1254
  periodic, start time....1282
Firewall Configuration Statement Hierarchy....143
firewall filters
  statistics
    clearing....2059
    displaying....2186, 2259
firewall-authentication statement....23
  (Security Policies)....591
  (Security)....590
firewall-authentication-service statement....1241
firewall-user statement....24

Copyright © 2013, Juniper Networks, Inc.

first-update statement....591
first-update-interval statement....592
fixed-multicast-rate statement
WLAN....1321
flag
Services....1154
flag statement....1196
flood statement
(ICMP)....593
(UDP)....594
flow statement
(Security Flow)....595
(Security IDP)....597
flow-control statement....190
flow-gate statement....1242
flow-session statement....1243
font conventions....xlix
force-ip-reassembly statement....597
force-upgrade statement....598
format statement, first use....598
format statement, second use....599
forwarding-classes (Cos)....119
Forwarding-Options Configuration Statement Hierarchy....149
forwarding-options statement....600
forwarding-process....601
FPC
status, displaying....1601
fragment statement....601
fragmentation-threshold statement
WLAN....1321
framing statement....86
friday statement....302
from statement....602
from-zone statement
(Security IDP Policy)....602
(Security Policies)....603
fru-poweron-sequence....87
ftp
anti-virus
utm-policy....607
content-filtering
utm-policy....607
ftp statement....24, 606
functional-zone statement....608

## G

gatekeeper statement....609
gateway statement....612
(IKE)....611
(Manual Security Association)....612
group VPN member IKE....609
group VPN server IKE....610
general-authentication-service statement....1244
Gi interface....630
global statement
(Security Policies)....614
global-config
Services....1157
global-mac-limit statement....262
global-mac-table-aging-time statement....263
global-no-mac-learning statement....263
global-threshold statement....88
global-weight statement....89
Gp interface....630
gprs statement....616, 628
gprs-gtp-profile statement
(Security Policies)....619
gprs-sctp-profile statement
(Security Policies)....619
gratuitous-arp-count statement....90
gre-in statement....620
gre-out statement....621
group statement....1245
group VPN....622
group-members statement....624
group-profile statement....25
group-vpn statement
security....625
Groups Configuration Statement Hierarchy....157
gsm-options statement....191
gtp statement....628
gtp-in-gtp-denied statement....630
guard-band statement....229

## H

h323 statement....631
handshake-timeout statement....632
hardware
supported platforms....xlviii
hash-key statement....154
hash-table-size....633
header-length statement....633
heartbeat-interval statement....91
heartbeat-threshold statement....92
high-availability....634
high-watermark statement....634


Copyright © 2013, Juniper Networks, Inc.

hit-rate-threshold statement....636
hold-down-interval statement....93
host....638
host (Security Logging) statement....637
host statement
(Security IDP Sensor Configuration)....637
ssh-known-hosts....640
host-address-base statement....638
host-inbound-traffic statement....639
hostkey-algorithm....1246
hostname statement....641
http statement....26
http-profile (content-filtering utm-policy)....642
http-profile (web-filtering utm-policy)....642
http-redirect statement
WLAN....1322
hub-assist statement....192

## I

icmp statement
(Security IDP Custom Attack)....643
(Security IDP Signature Attack)....644
(Security Screen)....645
icmp-code statement....64
icmp-type statement....64
icmpv6 (Security IDP)....645
identification statement
(Security ICMP Headers)....646
(Security IP Headers)....646
idle-time statement....647
idp potential violation statement....657
idp statement....648
(Security Policies)....647
idp-policy statement....658, 1247
ids-option statement....661
ignore-memory-overflow statement....662
ignore-reassembly-memory-overflow |
no-ignore-reassembly-memory-overflow....663
ignore-reassembly-overflow statement....663
ignore-regular-expression statement....664
ike statement
(IPsec VPN)....669
(Security)....665
group VPN....668
member....667
ike-phase1-failures statement....670
ike-phase2-failures statement....671
ike-policy statement....672
ike-user-type statement....672
imap-profile (antivirus utm-policy)....673
imap-profile (content-filtering utm-policy)....673
imsi-prefix
(GTP)....751
inactive-media-timeout statement
(MGCP)....674
(SCCP)....674
(SIP)....675
inactivity-timeout statement....65, 675
include-destination-address statement....676
Index is the statement name. Example - action
statement....97, 632, 937
inet statement....676
inet6 (IKE Gateway) statement....678
inet6 statement....677
infranet-controller statement....1158
inline-tap....678
install....679
install-interval statement....679
intelligent-prescreening statement....680
interface
Source NAT....682
interface (Cos)....123
interface statement....94, 230, 264, 683, 1159, 1248
(ARP Proxy Security NAT)....681
(NDP Proxy Security NAT)....681
(source NAT)....682
bridge domain....74
interface-monitor statement....95
interface-traceoptions statement
DHCP local server....1249
Interfaces Configuration Statement Hierarchy....159
interfaces statement....684
interval statement....193, 231, 1160
(IKE)....686
(Security Antivirus)....685
(Security IDP)....686
ip statement
(Security IDP Custom Attack)....687
(Security Screen)....688
ip-action statement
(Security Application-Level DDoS)....691
(Security IDP Rulebase IPS)....692
ip-block statement....693
ip-close statement....693
ip-connection-rate-limit statement....694
ip-flags statement....695
ip-monitoring statement....96
ip-notify statement....695

Copyright © 2013, Juniper Networks, Inc.

ip-sweep statement....696
ipc....697
ips statement....698
ipsec
group VPN member....701
ipsec statement....699
group VPN
server....702
ipsec-group-vpn statement
(Security Policies)....702
ipsec-policy statement....703
ipsec-sa statement....704
ipsec-vpn statement
(Dynamic VPNs)....705
(Security Flow)....705
(Security Policies)....706
ipv4 statement
(Security IDP Signature Attack)....690
ipv6 (Security IDP)....706
iso statement....707

## J

juniper-enhanced....708
juniper-express-engine statement....709
juniper-local....710

## K

kaspersky-lab-engine statement....711
KATs (known answer tests)....1240
manually executing....1543
periodic....1267
periodic, day of the month....1227
periodic, day of the week....1228
periodic, monthly....1254
periodic, start time....1282
key-exchange....1251
key-generation-self-test statement....712
key-protection statement....713
(Security IDP Sensor Configuration)....713
known answer tests *See* KATs

## L

l2-learning statement....264
lacp statement....193
land statement....714
large statement....714
latency (radio-router)....194
ldap-options statement....27
ldap-server statement....28
lease-time (dhcp-client) statement....195
level
Services ....1160
licenses
displaying....2250
lifetime-kilobytes statement....715
lifetime-seconds statement
group VPN....715
IKE....716
IPsec....716
limit....719
limit statement
(SCTP)....718
cache
security log....717
limit-session statement....719
link statement....28
link-speed statement....196
list statement
(Security Antivirus Mime Whitelist)....720
list statement (content-filter block-mime)....720
load-balance statement....237
load-distribution statement....721
local statement....721, 722
local-address statement
group VPN
member....722
local-authentication-table statement....441, 723
local-certificate statement....724
local-identity statement....725
lockout-period statement....1252
log....1454
Services ....1161
log file....1456
log statement
(GTP)....728
(SCTP)....730
(Security IDP Policy)....729
(Security IDP)....729
(Security Logging)....726
(Security Policies)....730
log-attacks statement....731
log-create statement....731
log-errors statement....732
log-supercede-min statement....732
logical-system statement....1252
Logical-Systems Configuration Statement
Hierarchy....223
logical-systems statement....225


Copyright © 2013, Juniper Networks, Inc.

login lockout....1484, 2262
login statement....29
loopback statement....196
low latency....1942
low-watermark statement....733

## M

mac-authentication-type statement
WLAN....1324
macs....1253
management statement....231, 734
management-vlan statement
WLAN....1324
manual statement....735
manuals
comments on....l
match
Services....1162
match statement
(Destination NAT Services Gateway)....738
(Security IDP Policy)....739
(Security Policies)....740
(Security Rulebase DDoS)....741
(Source NAT Services Gateway)....742
max-checked-bytes statement....1162
max-context-values statement....743
max-flow-mem statement....743
max-logs-operate statement....744
max-packet-mem statement....745
max-packet-memory statement....745
max-retrans-time statement....265
max-session-number statement....746
max-sessions statement....1163
(Security Packet Log)....746
max-tcp-session-packet-memory statement....747
max-time-report statement....747
max-timers-poll-ticks statement....748
max-udp-session-packet-memory statement....748
maximize-alg-sessions....418
maximize-cp-sessions....418
maximize-idp-sessions....418, 749
maximum-burst statement
WLAN....1325
maximum-cache-size statement....749
maximum-call-duration statement....750
maximum-capture-size
security log....750
maximum-contention-window statement
WLAN....1326
maximum-message-length statement....751
maximum-power statement....232
maximum-stations statement
WLAN....1325
max–message-length (gtp)....744
media-source-port-any statement....752
member statement
(Security IDP)....754
group VPN....753
member-interfaces statement....197
mesh-group statement....288, 289
message-flood statement
(H323)....755
(MGCP)....756
mgcp statement....757
MIBs
SNMP object values, displaying....2244
mime-pattern....758
mime-whitelist statement....759
minimum-contention-window statement
WLAN....1326
minimum-links statement....198
min–message-length statement
(GTP)....760
mode (Security Logging) statement....763
mode statement
(Forwarding Options)....761
(Policy)....762
WLAN....1327
monday statement....303
month statement....1254
mpls statement....764
msrpc statement....765
mss statement
(Security IDP)....766
multicast-scope statement....238

## N

name-server statement
WLAN....1327
nat statement
(Services Gateway Configuration)....767
nat-cone-binding statement....1255
nat-destination-pool statement....1256
nat-destination-rule statement....1257
nat-keepalive statement....770
nat-nopat-address statement....1258

Copyright © 2013, Juniper Networks, Inc.

nat-pat-address statement....1259
nat-pat-portnum statement....1260
nat-port-ol-ipnumber statement....1261
nat-source-pool statement....1262
nat-source-rule statement....1263
nat-static-rule statement....1264
native-vlan-id statement....199
negate statement....771
neighbor-discovery statement....266
neighbor-discovery-router-advertisement statement....30
nested-application (Security IDP)....771
nested-application services....1165
nested-application-system-cache....1166
network-security statement....1265
next-hop-tunnel statement....199
no-acknowledgement statement
WLAN....1328
no-allow-icmp-without-flow statement....398
no-anti-replay statement....772
no-application-identification statement....1166
no-application-system-cache statement
(Services)....1167
no-auto-power-save statement
WLAN....1328
no-autoupdate statement....772
no-broadcast-ssid statement
WLAN....1329
no-detect-shellcode statement....534
no-enable-all-qmodules statement....559
no-enable-packet-pool statement....559
no-flow-control statement....190
no-ignore-memory-overflow statement....662
no-ignore-regular-expression statement....664
no-include-destination-address statement....676
no-intelligent-prescreening statement....773
no-log-errors statement....732
no-loopback statement....196
no-nat-traversal statement....773
no-notify-mail-recipient statement....774
no-notify-mail-sender statement
(Security Fallback Block)....775
(Security Virus Detection)....776
no-notify-mail-sender statement (content-filtering notification-options)....774
no-policy-cold-synchronization statement....776
no-policy-lookup-cache statement....816
no-process-ignore-s2c statement....834
no-process-override statement....835
no-remote-trace
Services....1167
no-reset-on-policy statement....884
no-sbl-default-server statement....777
no-sequence-check statement....777
no-short-guard-interval-supported statement
WLAN....1329
no-source-filtering statement....214
no-syn-check statement....778
no-syn-check-in-tunnel statement....778
no-unframed option....216
no-uri-check statement....779
no-wifi-multimedia statement
WLAN....1329
node statement
(Cluster)....83, 97
(Redundancy-Group)....98
node-terminate-count statement....266
node-terminate-interval statement....267
non-cryptographic-self-test statement....779
notice icons....xlviii
notification....781
notification statement....780
notification-options statement
(Security Antivirus)....782
notification-options statement (content-filtering)....783
notify-mail-recipient statement....783
notify-mail-sender statement
(Security Fallback Block)....784
notify-mail-sender statement (content-filtering notification-options)....784
ntp-sever statement
WLAN....1330
number statement....785

## O

on-link-submet-only-statement....267
optimized statement....786
option statement
(Security IDP)....786
order statement
(Security IDP)....787
out-of-resources statement....787
(Security Antivirus Sophos Engine)....788
over-limit....788
overflow-pool statement
;(Source NAT Services Gateway....789


Copyright © 2013, Juniper Networks, Inc.

overrides statement
DHCP local server....1266

P
packet-action statement....268
packet-filter statement
security....790
packet-log statement....791
(Security IDP Sensor Configuration)....792
pair-policy statement....793
parentheses, in syntax descriptions....l
pass-through statement....31, 794
password statement....32, 1168
(Security Antivirus)....795
password-file statement....795
pattern statement
(Security IDP)....796
pattern-update statement
(Security Antivirus)....797
peer-certificate-type statement....798
pending-sess-queue-length statement....798
perfect-forward-secrecy statement....799
performance statement....800
periodic self-tests *See* FIPS self-tests; KATs
periodic statement....200, 1267
permit statement
(Security Policies)....802
persistent NAT....801
permit-command statement....803
persistent-nat statement....804
pic-mode....98
pic-mode (channel) statement....99
pic-mode statement....100
ping-death statement....804
pki statement....805
pki-local-certificate statement....1268
PoE configuration statement hierarchy....227
policers, displaying....2139
policies statement....807
policies, displaying....2089
policy potential violation statement....811
policy statement....1269
(IKE)....812
policy statement:
(Security Policies)....814
policy-lookup-cache statement....816
policy-match statement....817
Policy-Options Configuration Statement
Hierarchy....235
policy-rematch statement....818
policy-with-count statement....1270
pool
....820
pool statement....33
(Destination NAT Services Gateway)....818
(Source NAT )....819
pool-default-port-range statement....820
pool-utilization-alarm statement....821
pop3-profile (antivirus utm-policy)....821
pop3-profile (content-filtering utm-policy)....822
port (web filtering)....823
port statement....823, 1169
(LDAP)....34
(RADIUS)....35
(Security Antivirus)....822
port-overloading....824
port-overloading-factor statement....824
port-randomization statement
(source NAT)....825
port-scan statement....826
post-attack statement....827
post-attack-timeout statement....827
potential violation source-ip statement....966
potential-violation....828
ppp-over-ether statement....200
pptp statement....829
pre-attack statement....830
pre-filter-shellcode statement....830
pre-shared-key statement....831
predefined-attack-groups statement....831
predefined-attacks statement....832
preempt statement....101
preference statement
ES-IS....268
preferred-ciphers
Services ....1169
prefix statement....35, 201
priority statement....101, 233
process-ignore-s2c statement....834
process-override statement....835
process-port statement....835
processes
restarting....1564
products statement....836
profile
Services ....1170
profile (antispam sbl)....836
profile (web-filtering juniper-enhanced)....846

Copyright © 2013, Juniper Networks, Inc.

profile (web-filtering juniper-local)....847
profile (web-filtering
surf-control-integrated)....848
profile (web-filtering websense-redirect)....849
profile statement....36
(GTP)....841
(SCTP)....843
(Security Antivirus Juniper Express
Engine)....837
(Security Antivirus Kaspersky Lab
Engine)....839
(Security Sophos Engine Antivirus)....845
profile statement (content-filtering)....840
profiles statement....201
promiscuous-mode statement....202
propagate-settings statement....1271
proposal statement....851, 852
proposal statements
group VPN server IKE....850
proposal-set statement
(IKE)....853
(IPsec)....854
proposals statement....855
protect statement....856
protection statement
WLAN....1330
protocol statement....66
(IPsec)....861
(Manual Security Association)....862
(Security IDP IP Headers)....857
(Security IDP Signature Attack)....858
(Source NAT)....856, 862
protocol-binding statement....863
protocol-command....864
protocol-name statement....865
protocol-version
Services ....1171
Protocols Configuration Statement Hierarchy....239
protocols statement
(Interface Host-Inbound Traffic)....868
(Zone Host-Inbound Traffic)....866
proxy
Services ....1172
proxy statement
(Security Antivirus)....869
proxy-arp statement
(Security NAT)....870
proxy-identity statement....870
proxy-ndp statement
(Security NAT)....871

## Q

quality (radio-router)....202
quality-of-service statement
WLAN....1331
quarantine-message....871

## R

r2cp statement....269
radio statement....270
WLAN....1333
radio-interface statement....270
radio-off statement
WLAN....1336
radio-options statement
WLAN....1337
radio-router....203
radius-options statement....37
radius-server statement....38
raise-threshold statement....872
range statement....39
rate-limit
(GTP)....873
rate-limiters statement....128
re-assembler statement....873
re-enroll-trigger-time-percentage statement....874
re-generate-keypair....450
re-generate-keypair statement....874
real statement....875
recommended statement....875
recommended-action statement....876
reconfigure statement
DHCP local server....1272
redirect-traffic statement....1173, 1174
redirect-wx statement
(Application Services)....877
redundancy-group statement....102, 204
redundant-ether-options statement....205
redundant-parent statement
(Fast Ethernet Options)....205
(Gigabit Ethernet Options)....206
refresh-timeout statement....877
regexp statement....878
reject statement....878
reject-timeout statement....879
remote statement....879
remote-exceptions statement....880


Copyright © 2013, Juniper Networks, Inc.

remote-identity statement....881
remote-protected-resources statement....882
remove-ie statement
(GTP)....882
renegotiation
Services ....1175
replay-attacks statement....883
request chassis cluster failover node
command....1488
request chassis cluster failover reset
command....1489
request modem wireless activate iota
command....1492
request modem wireless activate manual
command....1493
request modem wireless activate otasp
command....1495
request modem wireless gsm sim-unblock
command....1496
request modem wireless gsm sim-unlock
command....1497
request pppoe connect command....1498
request pppoe disconnect command....1499
request security datapath-debug capture start
command....1500
request security datapath-debug capture stop
command....1501
request security idp security-package download
command....1502
request security idp security-package install
command....1504
request security idp ssl-inspection key add
command....1506
request security idp ssl-inspection key delete
command....1508
request security idp storage-cleanup
command....1510
request security ike debug-disable command....1511
request security ike debug-enable command....1512
request security pki ca-certificate verify
command....1513
request security pki local-certificate
generate-self-signed command....1514
request security pki local-certificate load
command....1516
request security pki local-certificate verify
command....1517
request security pki verify-integrity-status
command....1518
request security user-identification
local-authentication-table delete
command....1521
request security user-identification
local-authorization-table add command....1519
request security utm anti-virus
juniper-express-engine....1522
request security utm anti-virus
kaspersky-lab-engine....1523
request security utm anti-virus
sophos-engine....1524
Request services application identification
download command....1527
Request services application identification
download status command....1528
request services application-identification
application command....1525
request services application-identification group
command....1529
request services application-identification install
command....1530
request services application-identification install
status command....1531
request services application-identification uninstall
command....1532
request services application-identification uninstall
status command....1533
request system autorecovery state
command....1534
request system download abort command....1537
request system download clear command....1538
request system download pause command....1539
request system download resume
command....1540
request system download start command....1541
request system fips self-test command....1543
request system firmware upgrade command....1542
request system license update command....1545
request system partition compact-flash
command....1546
request system services dhcp command....1547
request system snapshot....1548
request system software abort in-service-upgrade
command....1549
issu....1490
request system software add ....1550
request system software in-service-upgrade
command....1551
request system software reboot....1556

Copyright © 2013, Juniper Networks, Inc.

request system software rollback....1557
request wan-acceleration login command....1558
request wireless-wan adapter firmware upgrade command....1561
request wlan access-point firmware upgrade command....1559
request wlan access-point restart command....1560
reset statement
(Security IDP)....883
reset-on-policy statement....884
resource (radio-router)....206
resource-manager statement....884
respond-bad-spi statement....885
restart command....1564
restart-path statement
(GTP)....886
restarting
software processes....1564
retain-hold-resource statement....886
reth-count statement....103
retransmission-interval (dhcp-client) statement....208
retransmission-interval statement....208
retry statement
(LDAP)....39
(RADIUS)....40
retry-count statement....104
retry-interval statement....104
reverse ssh....1273
reverse ssh port....1273
reverse telnet....1274
reverse telnet port....1274
revert-interval statement
(LDAP)....40
(RADIUS)....41
revocation-check statement....887
RIP
demand circuit retransmission timer....265
roaming-mode statement....209
root-ca
Services ....1175
root-logical-system statement....1275
route-active-on statement....238
route-change-timeout statement....887
routing-instance
pki....888
routing-instance statement
(Destination NAT Services Gateway)....888
(LDAP)....41
(RADIUS)....42
(Source NAT Services Gateway)....889
Routing-Instances Configuration Statement Hierarchy....277
routing-interface statement....74
Routing-Options Configuration Statement Hierarchy....291
rpc statement....892
rpc-program-number statement....67
rsh statement....893
rst-invalidate-session statement....893
rst-sequence-check statement....894
rts-threshold statement
WLAN....1338
rtsp statement....894
rule statement
(destination NAT)....896
(Security DDoS Rulebase)....895
(Security Exempt Rulebase)....897
(Security IPS Rulebase)....898
(Source NAT)....900
rule-set statement
(Source NAT )....903
destination NAT....902
rule-sets statement....131
rulebase-ddos statement....907
rulebase-exempt statement....908
rulebase-ips statement....909
run-mode statement....1275

## S

saturday statement....304
sbl....910
sbl-default-server statement....911
scan-extension statement....911
scan-mode statement....912
scan-options statement
(Security Antivirus Juniper Express Engine)....912
(Security Antivirus Kaspersky Lab Engine)....913
(Security Antivirus Sophos Engine)....913
sccp statement....914
scheduler statement....305, 1276
scheduler-name statement....915
schedulers statement....306
scope statement
(Security IDP Chain Attack)....915
(Security IDP Custom Attack)....916


Copyright © 2013, Juniper Networks, Inc.

screen statement
(Security)....917
(Zones)....919
sctp statement....422, 632, 920
search statement....42
search-filter statement....43
secondary-server statement....1197
secret statement....43
Secure Neighbor Discovery
neighbor-discovery statement....266
securid-server statement....44
security
alarms....436, 483, 670, 1383, 1753
log....1454
log file....1456
Security Configuration Statement Hierarchy....315
security statement
WLAN....1339
security-log-percent-full
security alarms....921
security-package statement....922
security-profile resources statement....1281
security-profile statement....1278
security-zone statement....923
select-profile statement....209
self-test statement....1240
self-tests
FIPS *See* FIPS self-tests
sensor-configuration statement....925
separator statement....45
sequence-check-required statement....927
sequence-number statement
(Security IDP ICMP Headers)....927
(Security IDP TCP Headers)....928
server....931
server address statement....210
server statement
(Security Antivirus)....928
group VPN....929
server-certificate
Services ....1176
server-certificate-subject statement....1176
server-connectivity....932
server-member-communication statement....933
server-port statement....271
service statement
(DDoS)....934
(Security Dynamic Attack Group)....935
(Security IDP Anomaly Attack)....934
(Security IPsec)....935
Services Configuration Statement Hierarchy....1133
services-offload statement....105, 936
session-affinity statement....936
session-close statement....936
session-id-cache-timeout....937
session-init statement....938
session-options statement....45
session-terminate-count statement....271
session-terminate-interval statement....272
session-update-interval statement....938
sessions statement....939
sessions-per-client....939
severity
security log....943
severity statement
(Security Dynamic Attack Group)....941
(Security IDP Custom Attack)....940
(Security IDP IPS Rulebase)....942
shellcode statement....944
show (services accounting aggregation
command....2194
show accounting command....1568
show accounting profile command....1569
show accounting records command....1570
show bgp neighbor command....1571
show chassis alarms command....1576
show chassis cluster control-plane statistics
command....1578
show chassis cluster data-plane interfaces
command....1580
show chassis cluster data-plane statistics
command....1581
show chassis cluster ethernet-switching interfaces
command....1583
show chassis cluster ethernet-switching status
command....1584
show chassis cluster interfaces command....1586
show chassis cluster ip-monitoring status
redundancy-group command....1590
show chassis cluster statistics command....1593
show chassis cluster status command....1598
show chassis fpc command....1601
show chassis hardware command....1607
show chassis power....1614
show chassis power sequence....1616
show chassis routing-engine command....1617
show chassis usb storage command....1619

Copyright © 2013, Juniper Networks, Inc.

show class-of-service application-traffic-control counter command....1620
show class-of-service application-traffic-control statistics rate-limiter command....1622
show class-of-service application-traffic-control statistics rule command....1624
show class-of-service forwarding-class command....1625
show configuration chassis cluster traceoptions command....1575
show configuration smtp ....1627
show dhcpv6 server binding....1641
show dhcpv6 server statistics command....1645
show ethernet-switching mac-learning-log command....1648
show ethernet-switching table command....1651
show firewall command....1656
show gtp tunnels....1658
show igmp-snooping route command....1665
show igmp-snooping vlans command....1667
show interfaces (Aggregated Ethernet) command....1676
show interfaces command....1669
show interfaces diagnostics optics command....1693
show interfaces flow-statistics command....1688
show interfaces statistics st0.1 command....1699
show interfaces swfabx command....1698
show lacp interfaces command....1700
show lacp statistics interfaces command....1705
show modem wireless interface command....1707
show modem wireless interface firmware command....1709
show modem wireless interface network command....1711
show modem wireless interface rssi command....1713
show network-access address-assignment pool command....1714
show network-access requests pending command....1715
show network-access requests statistics command....1717
show network-access securid-node-secret-file command....1718
show oam ethernet connectivity-fault-management adjacencies command....1719
show oam ethernet connectivity-fault-management forwarding-state command....1720
show oam ethernet connectivity-fault-management interfaces command....1722
show oam ethernet connectivity-fault-management mep-database command....1723
show oam ethernet connectivity-fault-management mep-statistics command....1727
show oam ethernet connectivity-fault-management mip command....1730
show oam ethernet connectivity-fault-management path-database command....1731
show oam ethernet connectivity-fault-management routes command....1733
show oam ethernet link-fault-management command....1735
show poe controller command....1740
show poe interface command....1741
show poe telemetries interface....1743
show pppoe interfaces command....1745
show pppoe statistics command....1749
show schedulers command....1751
show security alarms command....1753
show security alg h323 counters command....1758
show security alg ike-esp-nat summary command....1760
show security alg mgcp calls command....1761
show security alg mgcp counters command....1763
show security alg mgcp endpoints command....1766
show security alg msrpc command....1768
show security alg sccp calls command....1770
show security alg sccp counters command....1772
show security alg sip calls command....1774
show security alg sip counters command....1776
show security alg sip rate command....1781
show security alg sip transactions command....1783
show security alg status command....1785
show security application-firewall rule-set command....1787
show security application-firewall rule-set logical-system....1789
show security application-tracking counters command....1792
show security datapath-debug capture....1793
show security datapath-debug counter....1794
show security dns-cache command....1795
show security dynamic-policies command....1797
show security dynamic-vpn client version....1802
show security dynamic-vpn users....1803
show security dynamic-vpn users terse....1804


Copyright © 2013, Juniper Networks, Inc.

show security firewall-authentication history address command....1807
show security firewall-authentication history command....1805
show security firewall-authentication history identifier command....1810
show security firewall-authentication users address command....1815
show security firewall-authentication users command....1813
show security firewall-authentication users identifier command....1818
show security flow cp-session command....1821
show security flow cp-session destination-port command....1823
show security flow cp-session destination-prefix command....1825
show security flow cp-session family command....1827
show security flow cp-session protocol command....1829
show security flow cp-session source-port command....1831
show security flow cp-session source-prefix command....1833
show security flow gate brief node command....1839
show security flow gate command....1835
show security flow gate destination-port command....1845
show security flow gate destination-prefix command....1849
show security flow gate family command....1853
show security flow gate protocol command....1856
show security flow gate source-port command....1860
show security flow gate source-prefix command....1864
show security flow gate summary node command....1868
show security flow ip-action....1874
show security flow session application command....1884
show security flow session application-firewall command....1889
show security flow session brief node command....1896
show security flow session command....1879
show security flow session destination-port command....1900
show security flow session destination-prefix command....1904
show security flow session extensive node command....1909
show security flow session fast-forward command....1942
show security flow session interface command....1922
show security flow session protocol command....1931
show security flow session resource-manager command....1937
show security flow session session-identifier command....1947
show security flow session source-port command....1951
show security flow session source-prefix command....1955
show security flow session summary family command....1959
show security flow session summary fast-forward command....1967
show security flow session summary node command....1961
show security flow session tunnel command....1971
show security gprs sctp association command....1980
show security gprs sctp counters command....1981
show security group-vpn member ike security-associations command....1983
show security group-vpn member ipsec security-associations command....1987
show security group-vpn member kek security-associations command....1990
show security group-vpn server ike security-associations command....1993
show security group-vpn server ipsec security-associations command....1997
show security group-vpn server kek security-associations command....2001
show security group-vpn server registered-members command....2005
show security idp active-policy command....2007
show security idp application-ddos command....2008

Copyright © 2013, Juniper Networks, Inc.

show security idp application-identification application-system-cache command....2265, 2267
show security idp attack description command....2010
show security idp attack detail command....2011
show security idp attack table command....2013
show security idp counters application-ddos command....2014
show security idp counters application-identification command....2017
show security idp counters dfa command....2019
show security idp counters flow command....2020
show security idp counters ips command....2024
show security idp counters log command....2027
show security idp counters packet command....2030
show security idp counters packet-log command....2033
show security idp counters policy-manager command....2035
show security idp counters tcp-reassembler command....2036
show security idp logical-system policy-association command....2039
show security idp memory command....2040
show security idp policies....2041
show security idp policy-commit-status clear command....2043
show security idp policy-commit-status command....2042
show security idp policy-templates....2044
show security idp predefined-attacks....2045
show security idp security-package-version command....2047
show security idp ssl-inspection key command....2048
show security idp ssl-inspection session-id-cache command....2050
show security idp status command....2051
show security idp status detail....2053
show security ike active-peer command....2056
show security ike debug-status command....2057
show security ike pre-shared-key command....2058
show security ike security-associations command....2059
show security ike tunnel-map....2066
show security ipsec inactive-tunnels command....2067
show security ipsec next-hop-tunnels command....2070
show security ipsec security-associations command....2071
show security ipsec statistics command....2079
show security log command....2082
show security log file command....2086
show security match-policies command....2089
show security monitoring fpc fpc-number command....2095
show security nat destination pool command....2100
show security nat destination rule command....2102
show security nat destination summary command....2105
show security nat incoming-table command....2107
show security nat interface-nat-ports command....2109
show security nat source persistent-nat-table command....2111
show security nat source pool command....2114
show security nat source rule command....2118
show security nat source summary command....2121
show security pki ca-certificate command....2126
show security pki certificate-request command....2129
show security pki crl command....2131
show security pki local-certificate command....2134
show security policies command....2139
show security policies hit-count command....2145
show security resource-manager group active command....2147
show security resource-manager resource active command....2150
show security resource-manager settings command....2153
show security resource-manager summary command....2155
show security screen ids-option command....2156
show security screen statistics command....2159
show security shadow-policies logical-system command....2166
show security softwires ....2168
show security user-identification local-authentication-table command....2169
show security user-identification role-provision all command....2171
show security user-identification source-identity-provision all command....2172


Copyright © 2013, Juniper Networks, Inc.

show security user-identification user-provision all command....2173
show security utm anti-spam statistics....2174
show security utm anti-spam status....2175
show security utm anti-virus statistics....2176
show security utm anti-virus status....2178
show security utm content-filtering statistics....2180
show security utm session....2181
show security utm status....2182
show security utm web-filtering statistics....1659, 2183
show security utm web-filtering status....2185
show security zones command....2186
show security zones type command....2190
show services accounting aggregation template command....2195
show services accounting command....2193
show services accounting flow-detail command....2196
show services application-identification application command....2197
show services application-identification application-system-cache command....2202
show services application-identification counter command....2204
show services application-identification counter ssl-encrypted-sessions command....2206
show services application-identification group command....2208
show services application-identification statistics application-groups command....2212
show services application-identification statistics applications command....2210
show services application-identification version....2214
show services ip-monitoring status command....2215
show services rpm probe-results command....2219
show services ssl proxy statistics command....2223
show services unified-access-control authentication-table command....2224
show services unified-access-control counters command....2226
show services unified-access-control policies command....2228
show services unified-access-control roles command....2230
show services unified-access-control status command....2231
show snmp mib command....2244
show system alarms command....2246
show system autorecovery state command....2247
show system download command....2248
show system license command....2250
show system login lockout command....2262
show system security-profile command....2254
show system services dhcp client command....2259
show system services dhcp relay-statistics command....2263
show system snapshot media....2270
show system storage partitions....2271
show wan-acceleration status command....2272
show wireless-wan adapter command....2278
show wlan access-points command....2273
signature statement
  (application identification)....1177
  (Security IDP)....945
sip statement....949
sip-password statement....211
sip-user-id statement....212
size
  Services ....1181
size (web-filtering cache)....951
SMTP Configuration Statement Hierarchy....1195
smtp-profile (antispam utm-policy)....951
smtp-profile (antivirus utm-policy)....952
smtp-profile (content-filtering utm-policy)....952
SNMP
  MIB object values, displaying....2244
SNMP Configuration Statement Hierarchy....1199
sockets....953
softwires statement....954
sophos-engine statement....955
source statement
  (Security IDP IP Headers)....956
  (Source NAT Services Gateway)....957
source-address....959
source-address statement
  (Destination NAT Services Gateway)....959
  (LDAP)....46
  (RADIUS)....46
  (Security IDP Policy)....960
  (Security IDP Sensor Configuration)....960
  (Security Policies)....961
  (Source NAT Services Gateway)....962
source-address-filter statement....213

Copyright © 2013, Juniper Networks, Inc.

source-address-name statement
(Source NAT)....962, 963
source-except statement....963
source-filtering statement....214
source-identity statement....964
source-interface statement....965
source-ip-based statement....967
source-nat statement: (Source NAT Services Gateway)....968
source-port statement....67
(Security IDP)....969
source-threshold statement....970
space-time-block-coding statement
WLAN....1340
spam-action....970
speed
profile....214
spi statement....971
sql statement....972
ssh-known-hosts statement....973
ssid statement
WLAN....1340
ssl
Services....1179
ssl-encryption....974
ssl-inspection statement....974
ssl-proxy statement
(Application Services)....975
ssl-termination-profile....975
start-date statement....306
start-log statement....976
start-time statement....307, 1282
(Security IDP)....976
static statement....977
WLAN....1341
static-mac statement....75
static-wep statement
WLAN....1342
station-isolation statement....1343
station-mac-filter statement
WLAN....1343
station-queues statement
WLAN....1344
statistics (application-identification) statement....1181
statistics statement
(Security IDP)....979
stop-date statement....308
stop-time statement....309
stream
security log....980
strict-syn-check statement....980
success statement....47
sunday statement....310
sunrpc statement....981
support, technical *See* technical support
suppression statement....982
surf-control-integrated....983
sxl-retry statement....984
sxl-timeout statement....984
syn check statement....985
syn-ack-ack-proxy statement....985
syn-fin statement....986
syn-flood statement....986
syn-flood-protection-mode statement....987
syn-frag statement....987
syntax conventions....xlix
syslog-options statement
WLAN....1345
system
login lockout....1484, 2262
System Configuration Statement Hierarchy....1205
system-generated-certificate statement....1282
system-services statement
(Interface Host-Inbound Traffic)....990
(Zone Host-Inbound Traffic)....988

## T

t1-interval statement....991
t3-options statement
no-unframed option....216
unframed option....216
t4-interval statement....992
talk statement....993
target statement....994
tcp options statement
(Security Policies)....1002
tcp statement
(Security IDP Protocol Binding)....995
(Security IDP Signature Attack)....996
(Security Screen)....998
tcp-flags statement....999
tcp-initial-timeout statement....1000
tcp-mss statement....1001
tcp-no-flag statement....1001
tcp-rst statement....1002
tcp-session statement....1003
tcp-sweep statement....1004


Copyright © 2013, Juniper Networks, Inc.

technical support
contacting JTAC....l
telemetries statement....234
telnet statement....47
term statement....68
terminal statement....1004
termination
Services....1183
test statement
(Security IDP)....1005
test-only-mode statement....1184
tftp statement....1006
then
security application firewall....1007
then statement
(Destination NAT )....1008
(Security IDP Policy)....1009
(Security Policies)....1010
(Security Rulebase DDos)....1012
(Source NAT Services gateway)....1013
threshold (radio-router)....215
threshold statement....1015
thursday statement....311
time-binding statement....1016
time-binding-count statement....1016
time-binding-period statement....1017
time-wait-state statement....1018
timeout (web-filtering cache)....1024
timeout (web-filtering fallback-settings)....1024
timeout (web-filtering websense-redirect profile)....1023
timeout statement....1185
(GTP)....1022
(LDAP Server)....48
(RADIUS Server)....48
(Security Antivirus Fallback Options Sophos Engine)....1020
(Security Antivirus Fallback Options)....1019
(Security Antivirus Scan Options)....1021
(Security IDP Policy)....1022
(Security Screen)....1023
timeout-action statement....1186
to statement....1025
to-zone statement
(Security IDP Policy)....1025
(Security Policies)....1026
too-many-requests (web-filtering fallback-settings)....1030
too-many-requests statement
(Security Antivirus Fallback Options Sophos Engine)....1029
(Security Antivirus Fallback Options)....1028
tos statement....1031
total-length statement....1032
total-memory statement....1032
traceoptions
security log....1057
Services....1187
web-filtering....1074
traceoptions statement....49, 106, 275, 1189, 1198
(ALG)....1035
(Application Firewall)....1038
(application identification)....1188
(dynamic-vpn)....1043
(firewall-authentication)....1044
(General Authentication Service)....1287
(group VPN)....1047
(GTP)....1049
(H.323 ALG)....1051
(IKE)....1054
(IPsec)....1056
(MGCP ALG)....1059
(NAT Services Gateway)....1060
(PKI)....1062
(SCCP ALG)....1066
(Screen)....1067
(SCTP)....1069
(Security Antivirus)....1037
(Security Application Proxy)....1040
(Security Flow)....1045
(Security IDP)....1052
(Security Policies)....1064
(Security)....1033
(SIP ALG)....1071
(System Services DNS)....1285
(user identification)....1072
(UTM)....1073
(WAN Acceleration)....1289
(Wireless WAN Service)....1291
anti-spam....1036
datapath-debug....1042
DHCP local server....1283
ES-IS....273
traceoptions statement (content-filtering)....1041
tracing flags
ES-IS....273
traffic-options....1075

Copyright © 2013, Juniper Networks, Inc.

transaction-timeout statement....1075
transmit-opportunity-limit statement
WLAN....1345
transmit-power statement
WLAN....1346
transmit-rate-sets statement
WLAN....1346
trickling statement....1076
trigger statement....137
trusted-ca
Services....1190
trusted-keys ....1293
ttl statement
(Security IDP)....1077
tuesday statement....312
tunable-name statement....1078
tunable-value statement....1078
tunnel statement
(Security Policies)....1079
tunnel-queuing statement....107
type
(Security Virus Detection)....1082
web-filtering....1083
type statement
(Security Antivirus Feature Profile)....1079
(Security Dynamic Attack Group)....1081
(Security Fallback Block)....1080
(Security IDP ICMP Headers)....1081
type statement (content-filtering
notification-options)....1080

## U

uac-policy statement
(Application Services)....1083
udp statement
(Security IDP Protocol Binding)....1084
(Security IDP Signature Attack)....1085
(Security Screen)....1086
udp-anticipated-timeout....1086
udp-sweep statement....1087
unframed option ....216
unified-access-control statement....441, 1088, 1191
unknown-message statement
(H.323.ALG)....1089
(MGCP ALG)....1090
(SCCP ALG)....1091
(SIP ALG)....1092
untagged-vlan statement
WLAN....1347
update-server (dhcp-client) statement....217
upload-profile (ftp antivirus utm-profile)....1093
upload-profile (ftp content-filtering
utm-profile)....1093
urgent-pointer statement....1094
uri-check statement....1094
url statement
(Security Antivirus)....1095
(Security IDP)....1095
url-blacklist....1096
url-pattern....1097
url-whitelist (web-filtering)....1098
url-whitelist statement
(Security Antivirus)....1098
use-interface statement....217
user statement....1099
user-at-hostname statement....1099
user-groups statement....1100
user-id statement....217
user-identification statement....1100
username statement
(Security Antivirus)....1101
utm statement....1102
utm-policy....1110
utm-policy statement
(Security Policies)....1111
uuid statement....69

## V

value-hit-rate-threshold statement....1112
vdsl
profile....219
vendor-id statement....219, 220
version
(GTP)....1113
video-queue statement
WLAN....1348
virtual switch
VLAN identifier....76
virtual-access-point statement
WLAN....1349
virtual-channel-group statement....138, 276
virtual-channel-groups statement....139
virtual-channels statement....137
virus-detection statement
(Security Antivirus)....1115
vlan statement
WLAN....1350
vlan-id statement....76


Copyright © 2013, Juniper Networks, Inc.

vlan-id-list statement....77
vlan-tagging statement....190, 220
voice-queue statement
WLAN....1351
vpn statement....155, 1116
vpn-monitor statement....1117
vpn-monitor-options statement....1118

## W

wan-acceleration statement....1293
web-authentication statement....50, 221, 1119
web-filtering (feature-profile)....1120
web-management statement....1294
web-redirect statement....1122
web-redirect-to-https
Services....1123
websense-redirect (web-filtering)....1124
wednesday statement....313
weight statement....108
white-list statement....1126
whitelist
Services....1192
wildcard statement....1127
window-scale statement....1128
window-size statement....1129
winnuke statement....1129
WLAN Configuration Statement Hierarchy....1297
wpa-enterprise statement
WLAN....1352
wpa-personal statement
WLAN....1353

## X

xauth statement....1130

## Z

zone statement....1295
zones statement....1131

Copyright © 2013, Juniper Networks, Inc.

Copyright © 2013, Juniper Networks, Inc.