# ZyWALL / USG (ZLD) Series

Security Firewalls

Version: 4.10

Edition 1, 05/2014

# CLI Reference Guide

| Default Login Details | |
|---|---|
| LAN Port IP Address | http://192.168.1.1 |
| User Name | admin |
| Password | 1234 |

Copyright © 2014 ZyXEL Communications Corporation

This is a Reference Guide for a series of products intended for people who want to configure ZLD-based ZyWALL / USGs via Command Line Interface (CLI).



Some commands or command options in this guide may not be available in your product. See your product's User's Guide for a list of supported features. Every effort has been made to ensure that the information in this guide is accurate.

Please refer to www.zyxel.com for product specific User Guides and product certifications.



Do not use commands not documented in this guide.

### How To Use This Guide

- Read Chapter 1 on page 21 for how to access and use the CLI (Command Line Interface).
- Read Chapter 2 on page 35 to learn about the CLI user and privilege modes.

### Related Documentation

- Quick Start Guide
  The Quick Start Guide shows how to connect the ZyWALL / USG and access the Web Configurator wizards. (See the wizard real time help for information on configuring each screen.) It also contains a connection diagram and package contents list.
- User's Guide
  The User's Guide explains how to use the Web Configurator to configure the ZyWALL / USG.



It is recommended you use the Web Configurator to configure the ZyWALL / USG.

**Introduction** ..... **19**

Command Line Interface ..... 21
User and Privilege Modes ..... 35

**Reference** ..... **39**

Object Reference ..... 41
Status ..... 43
Registration ..... 47
AP Management ..... 55
Wireless LAN Profiles ..... 58
Interfaces ..... 69
Trunks ..... 113
Route ..... 119
Routing Protocol ..... 129
Zones ..... 133
DDNS ..... 137
Virtual Servers ..... 141
HTTP Redirect ..... 145
ALG ..... 149
UPnP ..... 153
IP/MAC Binding ..... 157
FirewallSecure Policy ..... 159
Web Authentication ..... 169
IPSec VPN ..... 177
SSL VPN ..... 187
L2TP VPN ..... 193
Application Patrol ..... 199
Anti-Virus ..... 209
IDP Commands ..... 217
Content Filtering ..... 235
Anti-Spam ..... 247
Device HA ..... 257
User/Group ..... 265
Addresses ..... 273
Services ..... 279
Schedules ..... 283
AAA Server ..... 285
Authentication Objects ..... 291
Certificates ..... 295
ISP Accounts ..... 300
SSL Application ..... 302
Endpoint Security ..... 305

DHCPv6 Objects ..... 312
System ..... 315
System Remote Management ..... 321
File Manager ..... 335
Logs ..... 353
Reports and Reboot ..... 359
Session Timeout ..... 365
Diagnostics ..... 367
Packet Flow Explore ..... 369
Packet Flow Filter ..... 373
Maintenance Tools ..... 377
Watchdog Timer ..... 383

# Table of Contents

**Table of Contents** ..... **5**

**Part I: Introduction** ..... **19**

**Chapter 1**
**Command Line Interface** ..... **21**

1.1 Overview ..... 21
1.1.1 The Configuration File ..... 21
1.2 Accessing the CLI ..... 21
1.2.1 Console Port ..... 22
1.2.2 Web Configurator Console ..... 23
1.2.3 Telnet ..... 25
1.2.4 SSH (Secure SHell) ..... 25
1.3 How to Find Commands in this Guide ..... 25
1.4 How Commands Are Explained ..... 26
1.4.1 Background Information (Optional) ..... 26
1.4.2 Command Input Values (Optional) ..... 26
1.4.3 Command Summary ..... 26
1.4.4 Command Examples (Optional) ..... 26
1.4.5 Command Syntax ..... 26
1.4.6 Changing the Password ..... 27
1.5 CLI Modes ..... 27
1.6 Shortcuts and Help ..... 28
1.6.1 List of Available Commands ..... 28
1.6.2 List of Sub-commands or Required User Input ..... 28
1.6.3 Entering Partial Commands ..... 29
1.6.4 Entering a ? in a Command ..... 29
1.6.5 Command History ..... 29
1.6.6 Navigation ..... 29
1.6.7 Erase Current Command ..... 29
1.6.8 The no Commands ..... 29
1.7 Input Values ..... 30
1.8 Ethernet Interfaces ..... 33
1.9 Saving Configuration Changes ..... 33
1.10 Logging Out ..... 34

**Chapter 2**
**User and Privilege Modes** ..... **35**

2.1 User And Privilege Modes ..... 35
2.1.1 Debug Commands ..... 36

**Part II: Reference ..... 39**

**Chapter 3**
**Object Reference ..... 41**

3.1 Object Reference Commands ..... 41
3.1.1 Object Reference Command Example ..... 42

**Chapter 4**
**Status ..... 43**

**Chapter 5**
**Registration ..... 47**

5.1 myZyXEL.com Overview ..... 47
5.1.1 Subscription Services Available on the ZyWALL / USG ..... 47
5.2 Registration Commands ..... 48
5.2.1 Command Examples ..... 49
5.3 Country Code ..... 50

**Chapter 6**
**AP Management ..... 55**

6.1 AP Management Overview ..... 55
6.2 AP Management Commands ..... 55
6.2.1 AP Management Commands Example ..... 57

**Chapter 7**
**Wireless LAN Profiles ..... 58**

7.1 Wireless LAN Profiles Overview ..... 58
7.2 AP Profile Commands ..... 58
7.2.1 AP Profile Commands Example ..... 62
7.3 SSID Profile Commands ..... 63
7.3.1 SSID Profile Example ..... 65
7.4 Security Profile Commands ..... 65
7.4.1 Security Profile Example ..... 67
7.5 MAC Filter Profile Commands ..... 67
7.5.1 MAC Filter Profile Example ..... 68

**Chapter 8**
**Interfaces ..... 69**

8.1 Interface Overview ..... 69

8.1.1 Types of Interfaces ..... 69
8.1.2 Relationships Between Interfaces ..... 72
8.2 Interface General Commands Summary ..... 73
8.2.1 Basic Interface Properties and IP Address Commands ..... 73
8.2.2 IGMP Proxy Commands ..... 80
8.2.3 DHCP Setting Commands ..... 81
8.2.4 Interface Parameter Command Examples ..... 85
8.2.5 RIP Commands ..... 86
8.2.6 OSPF Commands ..... 86
8.2.7 Connectivity Check (Ping-check) Commands ..... 88
8.3 Ethernet Interface Specific Commands ..... 89
8.3.1 MAC Address Setting Commands ..... 89
8.3.2 Port Grouping Commands ..... 90
8.4 Virtual Interface Specific Commands ..... 92
8.4.1 Virtual Interface Command Examples ..... 92
8.5 PPPoE/PPTP Specific Commands ..... 92
8.5.1 PPPoE/PPTP Interface Command Examples ..... 94
8.6 Cellular Interface Specific Commands ..... 94
8.6.1 Cellular Status ..... 97
8.6.2 Cellular Interface Command Examples ..... 99
8.7 Tunnel Interface Specific Commands ..... 100
8.7.1 Tunnel Interface Command Examples ..... 101
8.8 USB Storage Specific Commands ..... 101
8.8.1 USB Storage General Commands Example ..... 102
8.9 WLAN Specific Commands ..... 102
8.9.1 WLAN General Commands ..... 103
8.9.2 WLAN Interface Commands ..... 104
8.9.3 WLAN MAC Filter Commands ..... 107
8.10 VLAN Interface Specific Commands ..... 107
8.10.1 VLAN Interface Command Examples ..... 108
8.11 Bridge Specific Commands ..... 108
8.11.1 Bridge Interface Command Examples ..... 109
8.12 Auxiliary Interface Specific Commands ..... 110
8.12.1 Auxiliary Interface Command Examples ..... 110

**Chapter 9**
**Trunks ..... 113**

9.1 Trunks Overview ..... 113
9.2 Trunk Scenario Examples ..... 113
9.3 Trunk Commands Input Values ..... 114
9.4 Trunk Commands Summary ..... 114
9.5 Trunk Command Examples ..... 115
9.6 Link Sticking ..... 116

9.7 Link Sticking Commands Summary ..... 117
9.8 Link Sticking Command Example ..... 117

**Chapter 10**
**Route ..... 119**

10.1 Policy Route ..... 119
10.2 Policy Route Commands ..... 119
10.2.1 Assured Forwarding (AF) PHB for DiffServ ..... 124
10.2.2 Policy Route Command Example ..... 124
10.3 IP Static Route ..... 125
10.4 Static Route Commands ..... 126
10.4.1 Static Route Commands Examples ..... 127

**Chapter 11**
**Routing Protocol ..... 129**

11.1 Routing Protocol Overview ..... 129
11.2 Routing Protocol Commands Summary ..... 129
11.2.1 RIP Commands ..... 130
11.2.2 General OSPF Commands ..... 130
11.2.3 OSPF Area Commands ..... 131
11.2.4 Virtual Link Commands ..... 131
11.2.5 Learned Routing Information Commands ..... 132
11.2.6 show ip route Command Example ..... 132

**Chapter 12**
**Zones ..... 133**

12.1 Zones Overview ..... 133
12.2 Zone Commands Summary ..... 134
12.2.1 Zone Command Examples ..... 135

**Chapter 13**
**DDNS ..... 137**

13.1 DDNS Overview ..... 137
13.2 DDNS Commands Summary ..... 138
13.3 DDNS Commands Example ..... 139

**Chapter 14**
**Virtual Servers ..... 141**

14.1 Virtual Server Overview ..... 141
14.1.1 1:1 NAT and Many 1:1 NAT ..... 141
14.2 Virtual Server Commands Summary ..... 141
14.2.1 Virtual Server Command Examples ..... 143
14.2.2 Tutorial - How to Allow Public Access to a Server ..... 144

**Chapter 15**
**HTTP Redirect ..... 145**

15.1 HTTP Redirect Overview ..... 145
15.1.1 Web Proxy Server ..... 145
15.2 HTTP Redirect Commands ..... 146
15.2.1 HTTP Redirect Command Examples ..... 147

**Chapter 16**
**ALG ..... 149**

16.1 ALG Introduction ..... 149
16.2 ALG Commands ..... 150
16.3 ALG Commands Example ..... 151

**Chapter 17**
**UPnP ..... 153**

17.1 UPnP and NAT-PMP Overview ..... 153
17.2 UPnP and NAT-PMP Commands ..... 153
17.3 UPnP & NAT-PMP Commands Example ..... 154

**Chapter 18**
**IP/MAC Binding ..... 157**

18.1 IP/MAC Binding Overview ..... 157
18.2 IP/MAC Binding Commands ..... 157
18.3 IP/MAC Binding Commands Example ..... 158

**Chapter 19**
**FirewallSecure Policy ..... 159**

19.1 FirewallSecure Policy Overview ..... 159
19.2 FirewallSecure Policy Commands ..... 160
19.2.1 Firewall Sub-Commands ..... 163
19.2.2 Firewall Command Examples ..... 164
19.3 Session Limit Commands ..... 165

**Chapter 20**
**Web Authentication ..... 169**

20.1 Web Authentication Overview ..... 169
20.2 Web Authentication Commands ..... 169
20.2.1 web-auth login setting Sub-commands ..... 170
20.2.2 web-auth policy Sub-commands ..... 172
20.2.3 web-auth user-agreement Sub-commands ..... 173
20.2.4 Web Authentication Policy Insert Command Example ..... 173
20.3 SSO Overview ..... 174
20.3.1 SSO Configuration Commands ..... 174

20.3.2 SSO Show Commands ..... 175
20.3.3 Command Setup Sequence Example ..... 175

**Chapter 21**
**IPSec VPN ..... 177**

21.1 IPSec VPN Overview ..... 177
21.2 IPSec VPN Commands Summary ..... 178
21.2.1 IKE SA Commands ..... 179
21.2.2 IPSec SA Commands (except Manual Keys) ..... 180
21.2.3 IPSec SA Commands (for Manual Keys) ..... 183
21.2.4 VPN Concentrator Commands ..... 183
21.2.5 VPN Configuration Provisioning Commands ..... 184
21.2.6 SA Monitor Commands ..... 185

**Chapter 22**
**SSL VPN ..... 187**

22.1 SSL Access Policy ..... 187
22.1.1 SSL Application Objects ..... 187
22.1.2 SSL Access Policy Limitations ..... 187
22.2 SSL VPN Commands ..... 187
22.2.1 SSL VPN Commands ..... 188
22.2.2 Setting an SSL VPN Rule Tutorial ..... 189

**Chapter 23**
**L2TP VPN ..... 193**

23.1 L2TP VPN Overview ..... 193
23.2 IPSec Configuration ..... 193
23.2.1 Using the Default L2TP VPN Connection ..... 194
23.3 Policy Route ..... 194
23.4 L2TP VPN Commands ..... 195
23.4.1 L2TP VPN Commands ..... 195
23.5 L2TP VPN Example ..... 196
23.5.1 Configuring the Default L2TP VPN Gateway Example ..... 197
23.5.2 Configuring the Default L2TP VPN Connection Example ..... 197
23.5.3 Configuring the L2TP VPN Settings Example ..... 197
23.5.4 Configuring the Policy Route for L2TP Example ..... 198

**Chapter 24**
**Application Patrol ..... 199**

24.1 Application Patrol Overview ..... 199
24.2 Application Patrol Commands Summary ..... 199
24.2.1 Pre-defined Application Commands ..... 200
24.2.2 Rule Commands for Pre-defined Applications ..... 200

24.2.3 Exception Commands for Pre-defined Applications ..... 202
24.2.4 Other Application Commands ..... 203
24.2.5 Rule Commands for Other Applications ..... 203
24.2.6 General Commands for Application Patrol ..... 204

**Chapter 25**
**Anti-Virus ..... 209**

25.1 Anti-Virus Overview ..... 209
25.2 Anti-virus Commands ..... 209
25.2.1 General Anti-virus Commands ..... 210
25.2.2 Zone to Zone Anti-virus Rules ..... 210
25.2.3 White and Black Lists ..... 212
25.2.4 Signature Search Anti-virus Command ..... 213
25.3 Update Anti-virus Signatures ..... 214
25.3.1 Update Signature Examples ..... 215
25.4 Anti-virus Statistics ..... 215
25.4.1 Anti-virus Statistics Example ..... 216

**Chapter 26**
**IDP Commands ..... 217**

26.1 Overview ..... 217
26.2 General IDP Commands ..... 217
26.2.1 IDP Activation ..... 217
26.3 IDP Profile Commands ..... 218
26.3.1 Global Profile Commands ..... 218
26.3.2 IDP Zone to Zone Rules ..... 219
26.3.3 Editing/Creating IDP Signature Profiles ..... 220
26.3.4 Editing/Creating Anomaly Profiles ..... 220
26.3.5 Editing System Protect ..... 224
26.3.6 Signature Search ..... 224
26.4 IDP Custom Signatures ..... 227
26.4.1 Custom Signature Examples ..... 228
26.5 Update IDP Signatures ..... 231
26.5.1 Update Signature Examples ..... 232
26.6 IDP Statistics ..... 232
26.6.1 IDP Statistics Example ..... 233

**Chapter 27**
**Content Filtering ..... 235**

27.1 Content Filtering Overview ..... 235
27.2 Content Filtering Policies ..... 235
27.3 External Web Filtering Service ..... 235
27.4 Content Filtering Reports ..... 235

27.5 Content Filter Command Input Values ....236
27.6 General Content Filter Commands ....237
27.7 Content Filter Filtering Profile Commands ....239
27.8 Content Filter URL Cache Commands ....241
27.9 Content Filtering Statistics ....242
27.9.1 Content Filtering Statistics Example ....243
27.10 Content Filtering Commands Example ....243

**Chapter 28**
**Anti-Spam ....247**

28.1 Anti-Spam Overview ....247
28.2 Anti-Spam Commands ....247
28.2.1 General Anti-Spam Commands ....247
28.2.2 Zone to Zone Anti-spam Rules ....248
28.2.3 White and Black Lists ....250
28.2.4 DNSBL Anti-Spam Commands ....252
28.3 Anti-Spam Statistics ....255
28.3.1 Anti-Spam Statistics Example ....256

**Chapter 29**
**Device HA ....257**

29.1 Device HA Overview ....257
29.1.1 Before You Begin ....258
29.2 General Device HA Commands ....258
29.3 Active-Passive Mode Device HA ....258
29.4 Active-Passive Mode Device HA Commands ....259
29.4.1 Active-Passive Mode Device HA Commands ....259
29.4.2 Active-Passive Mode Device HA Command Example ....261
29.5 Legacy Mode (VRRP) Device HA ....261
29.6 Legacy Mode (VRRP) Device HA Commands ....262
29.6.1 VRRP Group Commands ....262
29.6.2 VRRP Synchronization Commands ....263
29.6.3 Link Monitoring Commands ....263

**Chapter 30**
**User/Group ....265**

30.1 User Account Overview ....265
30.1.1 User Types ....265
30.2 User/Group Commands Summary ....266
30.2.1 User Commands ....266
30.2.2 User Group Commands ....267
30.2.3 User Setting Commands ....267
30.2.4 Force User Authentication Commands ....269

30.2.5 Additional User Commands ..... 271

**Chapter 31**
**Addresses ..... 273**

31.1 Address Overview ..... 273
31.2 Address Commands Summary ..... 273
31.2.1 Address Object Commands ..... 274
31.2.2 Address Group Commands ..... 276

**Chapter 32**
**Services ..... 279**

32.1 Services Overview ..... 279
32.2 Services Commands Summary ..... 279
32.2.1 Service Object Commands ..... 279
32.2.2 Service Group Commands ..... 280

**Chapter 33**
**Schedules ..... 283**

33.1 Schedule Overview ..... 283
33.2 Schedule Commands Summary ..... 283
33.2.1 Schedule Command Examples ..... 284

**Chapter 34**
**AAA Server ..... 285**

34.1 AAA Server Overview ..... 285
34.2 Authentication Server Command Summary ..... 285
34.2.1 ad-server Commands ..... 285
34.2.2 ldap-server Commands ..... 286
34.2.3 radius-server Commands ..... 287
34.2.4 radius-server Command Example ..... 287
34.2.5 aaa group server ad Commands ..... 287
34.2.6 aaa group server ldap Commands ..... 288
34.2.7 aaa group server radius Commands ..... 289
34.2.8 aaa group server Command Example ..... 290

**Chapter 35**
**Authentication Objects ..... 291**

35.1 Authentication Objects Overview ..... 291
35.2 aaa authentication Commands ..... 291
35.2.1 aaa authentication Command Example ..... 292
35.3 test aaa Command ..... 292
35.3.1 Test a User Account Command Example ..... 292

**Chapter 36**
**Certificates ..... 295**

36.1 Certificates Overview ..... 295
36.2 Certificate Commands ..... 295
36.3 Certificates Commands Input Values ..... 295
36.4 Certificates Commands Summary ..... 296
36.5 Certificates Commands Examples ..... 299

**Chapter 37**
**ISP Accounts ..... 300**

37.1 ISP Accounts Overview ..... 300
37.1.1 PPPoE and PPTP Account Commands ..... 300
37.1.2 Cellular Account Commands ..... 301

**Chapter 38**
**SSL Application ..... 302**

38.1 SSL Application Overview ..... 302
38.1.1 SSL Application Object Commands ..... 302
38.1.2 SSL Application Command Examples ..... 304

**Chapter 39**
**Endpoint Security ..... 305**

39.1 Endpoint Security Overview ..... 305
39.1.1 Endpoint Security Commands Summary ..... 306
39.1.2 Endpoint Security Object Commands ..... 306
39.1.3 Endpoint Security Object Command Example ..... 309

**Chapter 40**
**DHCPv6 Objects ..... 312**

40.1 DHCPv6 Object Commands Summary ..... 312
40.1.1 DHCPv6 Object Commands ..... 312
40.1.2 DHCPv6 Object Command Examples ..... 313

**Chapter 41**
**System ..... 315**

41.1 System Overview ..... 315
41.2 Customizing the WWW Login Page ..... 315
41.3 Host Name Commands ..... 317
41.4 Time and Date ..... 317
41.4.1 Date/Time Commands ..... 318
41.5 Console Port Speed ..... 318
41.6 DNS Overview ..... 319
41.6.1 Domain Zone Forwarder ..... 319

41.6.2 DNS Commands ..... 319
41.6.3 DNS Command Example ..... 320

**Chapter 42**
**System Remote Management ..... 321**

42.1 Remote Management Overview ..... 321
42.1.1 Remote Management Limitations ..... 321
42.1.2 System Timeout ..... 321
42.2 Common System Command Input Values ..... 322
42.3 HTTP/HTTPS Commands ..... 322
42.3.1 HTTP/HTTPS Command Examples ..... 324
42.4 SSH ..... 324
42.4.1 SSH Implementation on the ZyWALL / USG ..... 324
42.4.2 Requirements for Using SSH ..... 324
42.4.3 SSH Commands ..... 325
42.4.4 SSH Command Examples ..... 325
42.5 Telnet ..... 326
42.6 Telnet Commands ..... 326
42.6.1 Telnet Commands Examples ..... 326
42.7 Configuring FTP ..... 327
42.7.1 FTP Commands ..... 327
42.7.2 FTP Commands Examples ..... 328
42.8 SNMP ..... 328
42.8.1 Supported MIBs ..... 328
42.8.2 SNMP Traps ..... 328
42.8.3 SNMP Commands ..... 329
42.8.4 SNMP Commands Examples ..... 330
42.9 ICMP Filter ..... 330
42.10 Dial-in Management ..... 331
42.10.1 AT Command Strings ..... 331
42.10.2 DTR Signal ..... 331
42.10.3 Response Strings ..... 331
42.10.4 Dial-in Management Commands ..... 331
42.11 Vantage CNM ..... 332
42.11.1 Vantage CNM Commands ..... 332
42.12 Language Commands ..... 334
42.13 IPv6 Commands ..... 334

**Chapter 43**
**File Manager ..... 335**

43.1 File Directories ..... 335
43.2 Configuration Files and Shell Scripts Overview ..... 335
43.2.1 Comments in Configuration Files or Shell Scripts ..... 336

43.2.2 Errors in Configuration Files or Shell Scripts ..... 337
43.2.3 ZyWALL / USG Configuration File Details ..... 337
43.2.4 Configuration File Flow at Restart ..... 338
43.3 File Manager Commands Input Values ..... 338
43.4 File Manager Commands Summary ..... 339
43.5 File Manager Command Examples ..... 340
43.6 FTP File Transfer ..... 340
43.6.1 Command Line FTP File Upload ..... 340
43.6.2 Command Line FTP Configuration File Upload Example ..... 341
43.6.3 Command Line FTP File Download ..... 341
43.6.4 Command Line FTP Configuration File Download Example ..... 342
43.7 ZyWALL / USG File Usage at Startup ..... 342
43.8 Notification of a Damaged Recovery Image or Firmware ..... 343
43.9 Restoring the Recovery Image ..... 344
43.10 Restoring the Firmware ..... 346
43.11 Restoring the Default System Database ..... 348
43.11.1 Using the atkz -u Debug Command ..... 350

**Chapter 44**
**Logs ..... 353**

44.1 Log Commands Summary ..... 353
44.1.1 Log Entries Commands ..... 354
44.1.2 System Log Commands ..... 354
44.1.3 Debug Log Commands ..... 355
44.1.4 E-mail Profile Commands ..... 356
44.1.5 Console Port Logging Commands ..... 358

**Chapter 45**
**Reports and Reboot ..... 359**

45.1 Report Commands Summary ..... 359
45.1.1 Report Commands ..... 359
45.1.2 Report Command Examples ..... 360
45.1.3 Session Commands ..... 360
45.1.4 Packet Size Statistics Commands ..... 360
45.2 Email Daily Report Commands ..... 361
45.2.1 Email Daily Report Example ..... 362
45.3 Reboot ..... 364

**Chapter 46**
**Session Timeout ..... 365**

**Chapter 47**
**Diagnostics ..... 367**

47.1 Diagnostics ..... 367

47.2 Diagnosis Commands ..... 367
47.3 Diagnosis Commands Example ..... 367

**Chapter 48**
**Packet Flow Explore ..... 369**

48.1 Packet Flow Explore ..... 369
48.2 Packet Flow Explore Commands ..... 369
48.3 Packet Flow Explore Commands Example ..... 370

**Chapter 49**
**Packet Flow Filter ..... 373**

49.1 Packet Flow Filter ..... 373
49.2 Packet Flow Filter Commands ..... 373
49.3 Packet Flow Filter Commands Examples ..... 374

**Chapter 50**
**Maintenance Tools ..... 377**

50.1 Maintenance Command Examples ..... 379
50.1.1 Packet Capture Command Example ..... 380

**Chapter 51**
**Watchdog Timer ..... 383**

51.1 Hardware Watchdog Timer ..... 383
51.2 Software Watchdog Timer ..... 383
51.3 Application Watchdog ..... 384
51.3.1 Application Watchdog Commands Example ..... 385

**List of Commands (Alphabetical) ..... 387**

# PART I
# Introduction

# 1

# Command Line Interface

This chapter describes how to access and use the CLI (Command Line Interface).

## 1.1 Overview

If you have problems with your ZyWALL / USG, customer support may request that you issue some of these commands to assist them in troubleshooting.

**Use of undocumented commands or misconfiguration can damage the ZyWALL / USG and possibly render it unusable.**

### 1.1.1 The Configuration File

When you configure the ZyWALL / USG using either the CLI (Command Line Interface) or the web configurator, the settings are saved as a series of commands in a configuration file on the ZyWALL / USG. You can store more than one configuration file on the ZyWALL / USG. However, only one configuration file is used at a time.

You can perform the following with a configuration file:

- Back up ZyWALL / USG configuration once the ZyWALL / USG is set up to work in your network.
- Restore ZyWALL / USG configuration.
- Save and edit a configuration file and upload it to multiple ZyWALL / USGs (of the same model) in your network to have the same settings.

Note: You may also edit a configuration file using a text editor.

## 1.2 Accessing the CLI

You can access the CLI using a terminal emulation program on a computer connected to the console port, from the web configurator or access the ZyWALL / USG using Telnet or SSH (Secure SHell).

Note: The ZyWALL / USG might force you to log out of your session if reauthentication time, lease time, or idle timeout is reached. See Chapter 30 on page 265 for more information about these settings.

## 1.2.1 Console Port

The default settings for the console port are as follows.

**Table 1** Managing the ZyWALL / USG: Console Port

| SETTING | VALUE |
|---|---|
| Speed | 115200 bps |
| Data Bits | 8 |
| Parity | None |
| Stop Bit | 1 |
| Flow Control | Off |

When you turn on your ZyWALL / USG, it performs several internal tests as well as line initialization. You can view the initialization information using the console port.

- Garbled text displays if your terminal emulation program's speed is set lower than the ZyWALL / USG's.
- No text displays if the speed is set higher than the ZyWALL / USG's.
- If changing your terminal emulation program's speed does not get anything to display, restart the ZyWALL / USG.
- If restarting the ZyWALL / USG does not get anything to display, contact your local customer support.

**Figure 1** Console Port Power-on Display

```
FLASH: AMD 16M

BootModule Version: V1.14 | 07/09/2010 11:00:00
DRAM: Size = 256 Mbytes

Kernel Version: V2.6.25.4 | 2011-10-28 00:25:30
ZLD Version: V3.00(BDR.0)b9 | 2011-10-28 14:41:45

Press any key to enter debug mode within 1 seconds.
.....................
```

After the initialization, the login screen displays.

**Figure 2** Login Screen

```
Welcome to ZyWALL USG 620W

Username:
```

Enter the user name and password at the prompts.

Note: The default login username is **admin** and password is **1234**. The username and password are case-sensitive.

## 1.2.2 Web Configurator Console

Note: Before you can access the CLI through the web configurator, make sure your computer supports the Java Runtime Environment. You will be prompted to download and install the Java plug-in if it is not already installed.

When you access the CLI using the web console, your computer establishes a SSH (Secure SHell) connection to the ZyWALL / USG. Follow the steps below to access the web console.

1 Log into the web configurator.

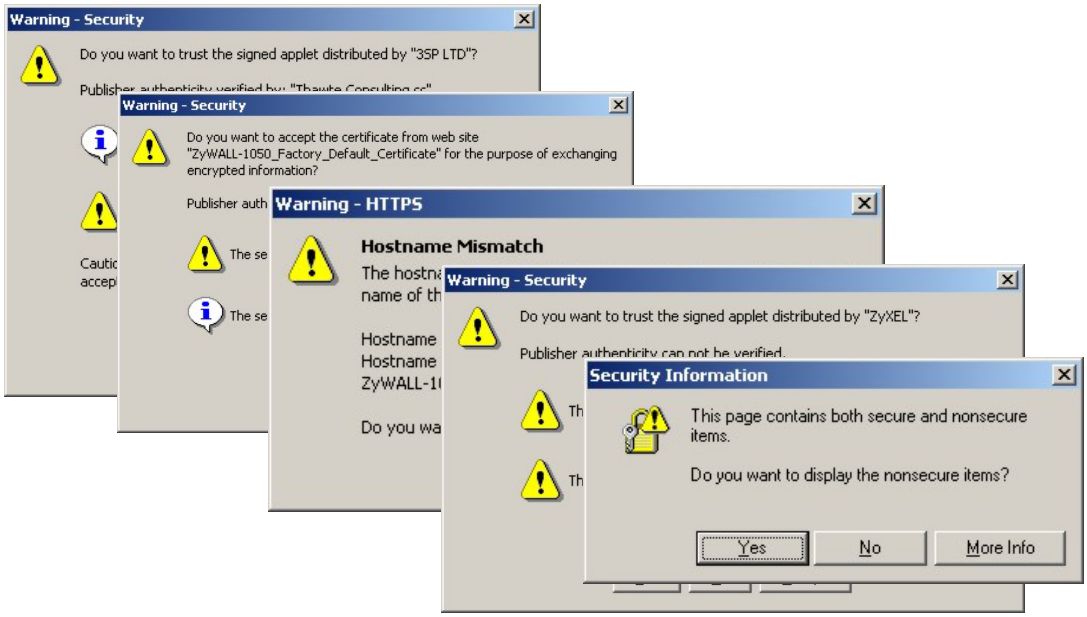
2 Click the **Console** icon in the top-right corner of the web configurator screen.

3 If the Java plug-in is already installed, skip to step 4.

Otherwise, you will be prompted to install the Java plug-in. If the prompt does not display and the screen remains gray, you have to download the setup program.

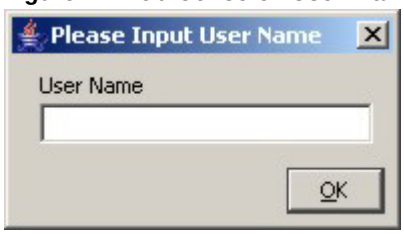
4 The web console starts. This might take a few seconds. One or more security screens may display. Click **Yes** or **Always**.

**Figure 3** Web Console: Security Warnings




Finally, the **User Name** screen appears.

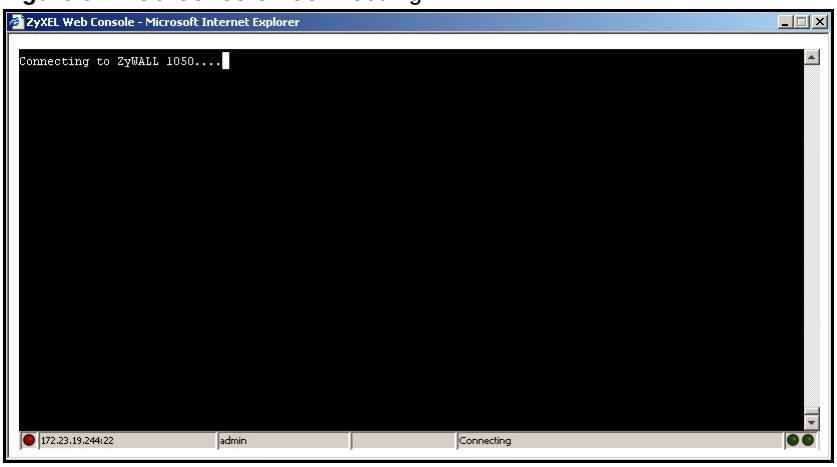
**Figure 4** Web Console: User Name




5 Enter the user name you want to use to log in to the console. The console begins to connect to the ZyWALL / USG.

Note: The default login username is **admin**. It is case-sensitive.

**Figure 5** Web Console: Connecting



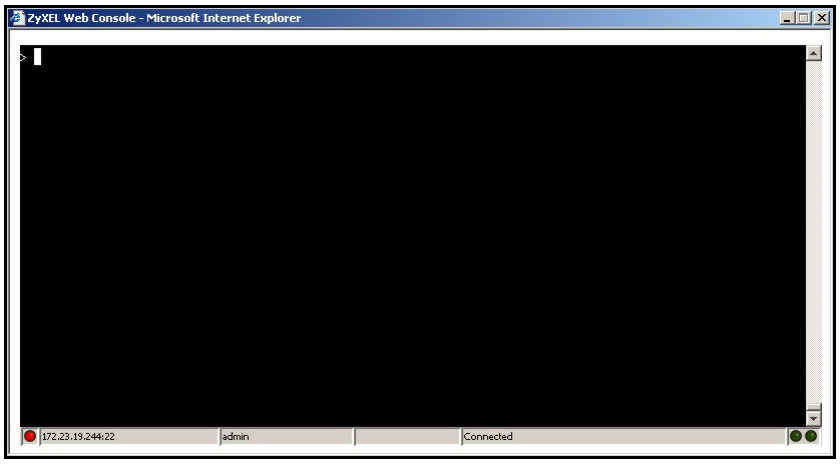

Then, the **Password** screen appears.

**Figure 6** Web Console: Password




6 Enter the password for the user name you specified earlier, and click **OK**. If you enter the password incorrectly, you get an error message, and you may have to close the console window and open it again. If you enter the password correctly, the console screen appears.

**Figure 7** Web Console




7 To use most commands in this User's Guide, enter `configure terminal`. The prompt should change to `Router(config)#`.

### 1.2.3 Telnet

Use the following steps to Telnet into your ZyWALL / USG.

1 If your computer is connected to the ZyWALL / USG over the Internet, skip to the next step. Make sure your computer IP address and the ZyWALL / USG IP address are on the same subnet.

2 In Windows, click **Start** (usually in the bottom left corner) and **Run**. Then type `telnet` and the ZyWALL / USG's IP address. For example, enter `telnet 192.168.1.1` (the default management IP address).

3 Click **OK**. A login screen displays. Enter the user name and password at the prompts.

Note: The default login username is **admin** and password is **1234**. The username and password are case-sensitive.

### 1.2.4 SSH (Secure SHell)

You can use an SSH client program to access the CLI. The following figure shows an example using a text-based SSH client program. Refer to the documentation that comes with your SSH program for information on using it.

Note: The default login username is **admin** and password is **1234**. The username and password are case-sensitive.

**Figure 8** SSH Login Example

```
C:\>ssh2 admin@192.168.1.1
Host key not found from database.
Key fingerprint:
xolor-takel-fipef-zevit-visom-gydog-vetan-bisol-lysob-cuvun-muxex
You can get a public key's fingerprint by running
% ssh-keygen -F publickey.pub
on the keyfile.
Are you sure you want to continue connecting (yes/no)? yes

Host key saved to C:/Documents and Settings/user/Application Data/SSH/hostkeys/
ey_22_192.168.1.1.pub
host key for 192.168.1.1, accepted by user Tue Aug 09 2005 07:38:28
admin's password:
Authentication successful.
```

## 1.3 How to Find Commands in this Guide

You can simply look for the feature chapter to find commands. In addition, you can use the List of Commands (Alphabetical) at the end of the guide. This section lists the commands in alphabetical order that they appear in this guide.

If you are looking at the CLI Reference Guide electronically, you might have additional options (for example, bookmarks or **Find...**) as well.

# 1.4 How Commands Are Explained

Each chapter explains the commands for one keyword. The chapters are divided into the following sections.

## 1.4.1 Background Information (Optional)

Note: See the User's Guide for background information about most features.

This section provides background information about features that you cannot configure in the web configurator. In addition, this section identifies related commands in other chapters.

## 1.4.2 Command Input Values (Optional)

This section lists common input values for the commands for the feature in one or more tables

## 1.4.3 Command Summary

This section lists the commands for the feature in one or more tables.

## 1.4.4 Command Examples (Optional)

This section contains any examples for the commands in this feature.

## 1.4.5 Command Syntax

The following conventions are used in this User's Guide.

- A command or keyword in `courier new` must be entered literally as shown. Do not abbreviate.
- Values that you need to provide are in *italics*.
- Required fields that have multiple choices are enclosed in curly brackets { }.
- A range of numbers is enclosed in angle brackets <>.
- Optional fields are enclosed in square brackets [].
- The | symbol means OR.

For example, look at the following command to create a TCP/UDP service object.

`service-object` *`object-name`* `{tcp | udp} {eq <1..65535> | range <1..65535> <1..65535>}`

1. Enter `service-object` exactly as it appears.
2. Enter the name of the object where you see *`object-name`*.
3. Enter `tcp` or `udp`, depending on the service object you want to create.
4. Finally, do one of the following.
   - Enter `eq` exactly as it appears, followed by a number between 1 and 65535.

- Enter `range` exactly as it appears, followed by two numbers between 1 and 65535.

### 1.4.6 Changing the Password

It is highly recommended that you change the password for accessing the ZyWALL / USG. See Section 30.2 on page 266 for the appropriate commands.

## 1.5 CLI Modes

You run CLI commands in one of several modes.

**Table 2** CLI Modes

| | USER | PRIVILEGE | CONFIGURATION | SUB-COMMAND |
|---|---|---|---|---|
| What **Guest** users can do | Unable to access | Unable to access | Unable to access | Unable to access |
| What **User** users can do | • Look at (but not run) available commands | Unable to access | Unable to access | Unable to access |
| What **Limited-Admin** users can do | • Look at system information (like **Status** screen)<br>• Run basic diagnostics | • Look at system information (like **Status** screen)<br>• Run basic diagnostics | Unable to access | Unable to access |
| What **Admin** users can do | • Look at system information (like **Status** screen)<br>• Run basic diagnostics | • Look at system information (like **Status** screen)<br>• Run basic diagnostics | • Configure simple features (such as an address object)<br>• Create or remove complex parts (such as an interface) | • Configure complex parts (such as an interface) in the ZyWALL / USG |
| How you enter it | Log in to the ZyWALL / USG | Type **enable** in **User** mode | Type **configure terminal** in **User** or **Privilege** mode | Type the command used to create the specific part in **Configuration** mode |
| What the prompt looks like | `Router>` | `Router#` | `Router(config)#` | (varies by part)<br>`Router(zone)#`<br>`Router(config-if-ge)#`<br>`...` |
| How you exit it | Type **exit** | Type **disable** | Type **exit** | Type **exit** |

See Chapter 30 on page 265 for more information about the user types. **User** users can only log in, look at (but not run) the available commands in **User** mode, and log out. **Limited-Admin** users can look at the configuration in the web configurator and CLI, and they can run basic diagnostics in the CLI. **Admin** users can configure the ZyWALL / USG in the web configurator or CLI.

At the time of writing, there is not much difference between **User** and **Privilege** mode for admin users. This is reserved for future use.

# 1.6 Shortcuts and Help

## 1.6.1 List of Available Commands

A list of valid commands can be found by typing ? or [TAB] at the command prompt. To view a list of available commands within a command group, enter <command> ? or <command> [TAB].

**Figure 9** Help: Available Commands Example 1

```
Router> ?
<cr>
apply
atse
clear
configure
------------------[Snip]--------------------
shutdown
telnet
test
traceroute
write
Router>
```

**Figure 10** Help: Available Command Example 2

```
Router> show ?
<wlan ap interface>
aaa
access-page
account
ad-server
address-object
------------------[Snip]--------------------
wlan
workspace
zone
Router> show
```

## 1.6.2 List of Sub-commands or Required User Input

To view detailed help information for a command, enter <command> <sub command> ?.

**Figure 11** Help: Sub-command Information Example

```
Router(config)# ip telnet server ?
;
<cr>
port
rule
|
Router(config)# ip telnet server
```

**Figure 12** Help: Required User Input Example

```
Router(config)# ip telnet server port ?
<1..65535>
Router(config)# ip telnet server port
```

## 1.6.3 Entering Partial Commands

The CLI does not accept partial or incomplete commands. You may enter a unique part of a command and press [TAB] to have the ZyWALL / USG automatically display the full command.

For example, if you enter **config** and press [TAB] , the full command of **configure** automatically displays.

If you enter a partial command that is not unique and press [TAB], the ZyWALL / USG displays a list of commands that start with the partial command.

**Figure 13** Non-Unique Partial Command Example

```
Router# c [TAB]
clear      configure  copy
Router# co [TAB]
configure  copy
```

## 1.6.4 Entering a ? in a Command

Typing a ? (question mark) usually displays help information. However, some commands allow you to input a ?, for example as part of a string. Press [CTRL+V] on your keyboard to enter a ? without the ~~ZyWALL~~ZyWALL / USG treating it as a help query.

## 1.6.5 Command History

The ZyWALL / USG keeps a list of commands you have entered for the current CLI session. You can use any commands in the history again by pressing the up (↑) or down (↓) arrow key to scroll through the previously used commands and press [ENTER].

## 1.6.6 Navigation

Press [CTRL]+A to move the cursor to the beginning of the line. Press [CTRL]+E to move the cursor to the end of the line.

## 1.6.7 Erase Current Command

Press [CTRL]+U to erase whatever you have currently typed at the prompt (before pressing [ENTER]).

## 1.6.8 The no Commands

When entering the no commands described in this document, you may not need to type the whole command. For example, with the "`[no] mss <536..1452>`" command, you use "`mss 536`" to specify the MSS value. But to disable the MSS setting, you only need to type "`no mss`" instead of "no mss 536".

# 1.7 Input Values

You can use the ? or [TAB] to get more information about the next input value that is required for a command. In some cases, the next input value is a string whose length and allowable characters may not be displayed in the screen. For example, in the following example, the next input value is a string called <description>.

```
Router# configure terminal
Router(config)# interface ge1
Router(config-if-ge)# description
<description>
```

When you use the example above, note that ZyWALL / USG USG 200 and below models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.

The following table provides more information about input values like <description>.

**Table 3** Input-Value Formats for Strings in CLI Commands

| TAG | # VALUES | LEGAL VALUES |
|---|---|---|
| * | 1 | * |
| *all* | -- | ALL |
| *authentication key* | Used in IPSec SA | |
| | 32-40<br>16-20 | "0x" or "0X" + 32-40 hexadecimal values<br>alphanumeric or ;\|`~!@#$%^&*()_+\\{}':,./<>=- |
| | Used in MD5 authentication keys for RIP/OSPF and text authentication key for RIP | |
| | 0-16 | alphanumeric or _- |
| | Used in text authentication keys for OSPF | |
| | 0-8 | alphanumeric or _- |
| *certificate name* | 1-31 | alphanumeric or ;`~!@#$%^&()_+[\]{}',.=- |
| *community string* | 0-63 | alphanumeric or .-<br>first character: alphanumeric or - |
| *connection_id* | 1+ | alphanumeric or -_: |
| *contact* | 1-61 | alphanumeric, spaces, or '()+,/:=?;!*#@$_%-. |
| *country code* | 0 or 2 | alphanumeric |
| *custom signature file name* | 0-30 | alphanumeric or _-.<br>first character: letter |
| *description* | Used in keyword criteria for log entries | |
| | 1-64 | alphanumeric, spaces, or '()+,/:=?;!*#@$_%-. |
| | Used in other commands | |
| | 1-61 | alphanumeric, spaces, or '()+,/:=?;!*#@$_%- |
| *distinguished name* | 1-511 | alphanumeric, spaces, or .@=,_- |

**Table 3** Input-Value Formats for Strings in CLI Commands (continued)

| TAG | # VALUES | LEGAL VALUES |
|---|---|---|
| *domain name* | Used in content filtering | |
| | 0+ | lower-case letters, numbers, or .- |
| | Used in ip dns server | |
| | 0-247 | alphanumeric or .-<br>first character: alphanumeric or - |
| | Used in domainname, ip dhcp pool, and ip domain | |
| | 0-254 | alphanumeric or ._-<br>first character: alphanumeric or - |
| *email* | 1-63 | alphanumeric or .@_- |
| *e-mail* | 1-64 | alphanumeric or .@_- |
| *encryption key* | 16-64<br>8-32 | "0x" or "0X" + 16-64 hexadecimal values<br>alphanumeric or ;\|`~!@#$%^&*()_+\\{}':,./<>=- |
| *file name* | 0-31 | alphanumeric or _- |
| *filter extension* | 1-256 | alphanumeric, spaces, or '()+,/:=?;!*#@$_%.- |
| *fqdn* | Used in ip dns server | |
| | 0-252 | alphanumeric or .-<br>first character: alphanumeric or - |
| | Used in ip ddns, time server, device HA, VPN, certificates, and interface ping check | |
| | 0-254 | alphanumeric or .-<br>first character: alphanumeric or - |
| *full file name* | 0-256 | alphanumeric or _/.- |
| *hostname* | Used in hostname command | |
| | 0-63 | alphanumeric or .-_<br>first character: alphanumeric or - |
| | Used in other commands | |
| | 0-252 | alphanumeric or .-<br>first character: alphanumeric or - |
| *import configuration file* | 1-26+".conf" | alphanumeric or ;`~!@#$%^&()_+[]{}',.=-<br>add ".conf" at the end |
| *import shell script* | 1-26+".zysh" | alphanumeric or ;`~!@#$%^&()_+[]{}',.=-<br>add ".zysh" at the end |
| *initial string* | 1-64 | alphanumeric, spaces, or '()+,/:=!*#@$_%-.& |
| *isp account password* | 0-63 | alphanumeric or `~!@#$%^&*()_\-+={}\|\;:'<,>./ |
| *isp account username* | 0-30 | alphanumeric or -_@$./ |
| ipv6_addr | | An IPv6 address. The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address 2001:0db8:1a2b:0015:0000:0000:1a2f:0000.<br><br>IPv6 addresses can be abbreviated in two ways:<br><br>Leading zeros in a block can be omitted. So 2001:0db8:1a2b:0015:0000:0000:1a2f:0000 can be written as 2001:db8:1a2b:15:0:0:1a2f:0.<br><br>Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So 2001:0db8:0000:0000:1a2f:0000:0000:0015 can be written as 2001:0db8::1a2f:0000:0000:0015, 2001:0db8:0000:0000:1a2f::0015, 2001:db8::1a2f:0:0:15 or 2001:db8:0:0:1a2f::15. |

**Table 3** Input-Value Formats for Strings in CLI Commands (continued)

| TAG | # VALUES | LEGAL VALUES |
|---|---|---|
| *key length* | -- | 512, 768, 1024, 1536, 2048 |
| *license key* | 25 | "S-" + 6 upper-case letters or numbers + "-" + 16 upper-case letters or numbers |
| *mac address* | -- | aa:bb:cc:dd:ee:ff (hexadecimal) |
| *mail server fqdn* | | lower-case letters, numbers, or -. |
| *name* | 1-31 | alphanumeric or _- |
| *notification message* | 1-81 | alphanumeric, spaces, or '()+,/:=?;!*#@$_%- |
| *password: less than 15 chars* | 1-15 | alphanumeric or `~!@#$%^&*()_\-+={}\|\;:'<,>./ |
| *password: less than 8 chars* | 1-8 | alphanumeric or ;/?:@&=+$\.-_!~*'()%,#$ |
| *password* | Used in user and ip ddns | |
| | 1-63 | alphanumeric or `~!@#$%^&*()_-+={}\|\;:'<,>./ |
| | Used in e-mail log profile SMTP authentication | |
| | 1-63 | alphanumeric or `~!@#$%^&*()_-+={}\|\;:'<>./ |
| | Used in device HA synchronization | |
| | 1-63 | alphanumeric or ~#%^*_-={}:,. |
| | Used in registration | |
| | 6-20 | alphanumeric or .@_- |
| *phone number* | 1-20 | numbers or ,+ |
| *preshared key* | 16-64 | "0x" or "0X" + 16-64 hexadecimal values<br>alphanumeric or ;\|`~!@#$%^&*()_+\{}':,./<>=- |
| *profile name* | 0-30 | alphanumeric or _-<br>first character: letters or _- |
| *proto name* | 1-16 | lower-case letters, numbers, or - |
| *protocol name* | 0-30 | alphanumeric or _-<br>first character: letters or _- |
| *quoted string less than 127 chars* | 1-255 | alphanumeric, spaces, or ;/?:@&=+$\.-_!~*'()%, |
| *quoted string less than 63 chars* | 1-63 | alphanumeric, spaces, or ;/?:@&=+$\.-_!~*'()% |
| *quoted string* | 0+ | alphanumeric, spaces, or punctuation marks<br>enclosed in double quotation marks (")<br>must put a backslash (\) before double quotation marks that are part of input value itself |
| *service name* | 0-63 | alphanumeric or -_@$./ |
| *spi* | 2-8 | hexadecimal |
| *string less than 15 chars* | 1-15 | alphanumeric or -_ |
| *string: less than 63 chars* | 1-63 | alphanumeric or `~!@#$%^&*()_-+={}\|\;:'<,>./ |
| *string* | 1+ | alphanumeric or -_@ |
| *subject* | 1-61 | alphanumeric, spaces, or '()+,./:=?;!*#@$_%- |
| *system type* | 0-2 | hexadecimal |
| *timezone [-+]hh* | -- | -12 through +12 (with or without "+") |

**Table 3** Input-Value Formats for Strings in CLI Commands (continued)

| TAG | # VALUES | LEGAL VALUES |
|---|---|---|
| *url* | 1-511 | alphanumeric or '()+,/:.=?;!*#@$_%- |
| *url* | Used in content filtering redirect | |
| | "http://"+<br>"https://"+ | alphanumeric or ;/?:@&=+$\.-_!~*'()%,<br>starts with "http://" or "https://"<br>may contain one pound sign (#) |
| | Used in other content filtering commands | |
| | "http://"+ | alphanumeric or ;/?:@&=+$\.-_!~*'()%,<br>starts with "http://"<br>may contain one pound sign (#) |
| *user name* | Used in VPN extended authentication | |
| | 1-31 | alphanumeric or _- |
| | Used in other commands | |
| | 0-30 | alphanumeric or _-<br>first character: letters or _- |
| *username* | 6-20 | alphanumeric or .@_-<br>registration |
| *user name* | 1+ | alphanumeric or -_.<br>logging commands |
| *user@domainname* | 1-80 | alphanumeric or .@_- |
| *vrrp group name: less than 15 chars* | 1-15 | alphanumeric or _- |
| *week-day sequence, i.e. 1=first,2=second* | 1 | 1-4 |
| *xauth method* | 1-31 | alphanumeric or _- |
| *xauth password* | 1-31 | alphanumeric or ;\|`~!@#$%^&*()_+\{}':,./<>=- |
| *mac address* | 0-12 (even number) | hexadecimal<br>for example: aa aabbcc aabbccddeeff |

# 1.8 Ethernet Interfaces

How you specify an Ethernet interface depends on the ZyWALL / USG model.

- For the ZyWALL / USG USG 300 and above, use ge*x*, *x* = 1~N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model.
- The ZyWALL / USG USG 200 and below models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.

# 1.9 Saving Configuration Changes

Use the `write` command to save the current configuration to the ZyWALL / USG.

Note: Always save the changes before you log out after each management session. All unsaved changes will be lost after the system restarts.

# 1.10 Logging Out

Enter the `exit` or `end` command in configure mode to go to privilege mode.

Enter the `exit` command in user mode or privilege mode to log out of the CLI.

# 2

# User and Privilege Modes

This chapter describes how to use these two modes.

## 2.1 User And Privilege Modes

This is the mode you are in when you first log into the CLI. (Do not confuse ‘user mode’ with types of user accounts the ZyWALL / USG uses. See Chapter 30 on page 265 for more information about the user types. ‘User’ type accounts can only run ‘exit’ in this mode. However, they may need to log into the device in order to be authenticated for ‘user-aware’ policies, for example a firewall rule that a particular user is exempt from or a VPN tunnel that only certain people may use.)

Type ‘enable’ to go to ‘privilege mode’. No password is required. All commands can be run from here except those marked with an asterisk. Many of these commands are for trouble-shooting purposes, for example the htm (hardware test module) and debug commands. Customer support may ask you to run some of these commands and send the results if you need assistance troubleshooting your device.

For admin logins, all commands are visible in ‘user mode’ but not all can be run there. The following table displays which commands can be run in ‘user mode’. All commands can be run in ‘privilege mode’.

**The `htm` and `psm` commands are for ZyXEL’s internal manufacturing process.**

**Table 4** User (U) and Privilege (P) Mode Commands

| COMMAND | MODE | DESCRIPTION |
|---|---|---|
| `apply` | P | Applies a configuration file. |
| `atse` | U/P | Displays the seed code |
| `clear` | U/P | Clears system or debug logs or DHCP binding. |
| `configure` | U/P | Use ‘configure terminal’ to enter configuration mode. |
| `copy` | P | Copies configuration files. |
| `debug (*)` | U/P | For support personnel only! The device needs to have the debug flag enabled. |
| `delete` | P | Deletes configuration files. |
| `details` | P | Performs diagnostic commands. |
| `diag` | P | Provided for support personnel to collect internal system information. It is not recommended that you use these. |
| `diag-info` | P | Has the ZyWALL / USG create a new diagnostic file. |
| `dir` | P | Lists files in a directory. |
| `disable` | U/P | Goes from privilege mode to user mode |
| `enable` | U/P | Goes from user mode to privilege mode |

**Table 4** User (U) and Privilege (P) Mode Commands (continued)

| COMMAND | MODE | DESCRIPTION |
|---|---|---|
| exit | U/P | Goes to a previous mode or logs out. |
| htm | U/P | Goes to htm (hardware test module) mode for testing hardware components. You may need to use the htm commands if your customer support Engineer asks you to during troubleshooting.<br><br>Note: These commands are for ZyXEL's internal manufacturing process. |
| interface | U/P | Dials or disconnects an interface. |
| no packet-trace | U/P | Turns off packet tracing. |
| nslookup | U/P | Resolves an IP address to a host name and vice-versa. |
| packet-trace | U/P | Performs a packet trace. |
| ping | U/P | Pings an IP address or host name. |
| ping6 | U/P | Pings an IPv6 address or a host name. |
| psm | U/P | Goes to psm (product support module) mode for setting product parameters. You may need to use the htm commands if your customer support Engineer asks you to during troubleshooting.<br><br>Note: These commands are for ZyXEL's internal manufacturing process. |
| reboot | P | Restarts the device. |
| release | P | Releases DHCP information from an interface. |
| rename | P | Renames a configuration file. |
| renew | P | Renews DHCP information for an interface. |
| run | P | Runs a script. |
| setenv | U/P | Turns stop-on-error on (terminates booting if an error is found in a configuration file) or off (ignores configuration file errors and continues booting). |
| show | U/P | Displays command statistics. See the associated command chapter in this guide. |
| shutdown | P | Writes all d data to disk and stops the system processes. It does not turn off the power. |
| telnet | U/P | Establishes a connection to the TCP port number 23 of the specified host name or IP address. |
| test aaa | U/P | Tests whether the specified user name can be successfully authenticated by an external authentication server. |
| traceroute | P | Traces the route to the specified host name or IP address. |
| traceroute6 | P | Traces the route to the specified host name or IPv6 address. |
| write | P | Saves the current configuration to the ZyWALL / USG. All unsaved changes are lost after the ZyWALL / USG restarts. |

Subsequent chapters in this guide describe the configuration commands. User/privilege mode commands that are also configuration commands (for example, 'show') are described in more detail in the related configuration command chapter.

## 2.1.1 Debug Commands

Debug commands marked with an asterisk (*) are not available when the debug flag is on and are for ZyXEL service personnel use only. The debug commands follow a Linux-based syntax, so if there

is a Linux equivalent, it is displayed in this chapter for your reference. You must know a command listed here well before you use it. Otherwise, it may cause undesired results.

**Table 5** Debug Commands

| COMMAND SYNTAX | DESCRIPTION | LINUX COMMAND EQUIVALENT |
|---|---|---|
| debug alg | FTP/SIP ALG debug commands | |
| debug anti-spam | Anti-Spam debug commands | |
| debug app | Application patrol debug command | |
| debug app show l7protocol (*) | Shows app patrol protocol list | > cat /etc/l7_protocols/ protocol.list |
| debug ca (*) | Certificate debug commands | |
| debug content-filter | Content Filtering debug commands | |
| debug device-ha (*) | Device HA debug commands | |
| debug eps | Endpoint security debug commands | |
| debug force-auth (*) | Authentication policy debug commands | |
| debug gui (*) | GUI cgi related debug commands | |
| debug gui (*) | Web Configurator related debug commands | |
| debug hardware (*) | Hardware debug commands | |
| debug idp | IDP debug commands | |
| debug idp-av | IDP and Anti-Virus debug commands | |
| debug interface | Interface debug commands | |
| debug interface ifconfig [interface] | Shows system interfaces detail | > ifconfig [interface] |
| debug interface-group | Port grouping debug commands | |
| debug ip dns | DNS debug commands | |
| debug ip virtual-server | Virtual Server (NAT) debug commands | |
| debug ipsec | IPSec VPN debug commands | |
| debug logging | System logging debug commands | |
| debug manufacture | Manufacturing related debug commands | |
| debug myzyxel server (*) | Myzyxel.com debug commands | |
| debug network arpignore (*) | Enable/Display the ignoring of ARP responses for interfaces which don't own the IP address | cat /proc/sys/net/ipv4/conf/*/ arp_ignore |
| debug no myzyxel server (*) | Set the myZyXEL.com registration/update server to the official site | |
| debug policy-route (*) | Policy route debug command | |
| debug reset content-filter profiling | Content Filtering debug commands | |
| debug service-register | Service registration debug command | |
| debug show content-filter server | Category-based content filtering debug command | |
| debug show myzyxel server status | Myzyxel.com debug commands | |
| debug show ipset | Lists the ZyWALL / USG's received cards | |
| debug show myzyxel server status | Myzyxel.com debug commands | |
| debug sslvpn | SSL VPN debug commands | |

**Table 5** Debug Commands (continued)

| COMMAND SYNTAX | DESCRIPTION | LINUX COMMAND EQUIVALENT |
|---|---|---|
| `debug system ipv6` | IPv6 debug commands | |
| `debug [cmdexec\|corefile\|ip \|kernel\|mac-id-rewrite\|observer\|switch \|system\|zyinetpkt\|zysh-ipt-op] (*)` | ZLD internal debug commands | |
| `debug update server (*)` | Update server debug command | |

# PART II
# Reference

# 3

# Object Reference

This chapter describes how to use object reference commands.

## 3.1 Object Reference Commands

The object reference commands are used to see which configuration settings reference a specific object. You can use this table when you want to delete an object because you have to remove references to the object first.

**Table 6** `show reference` Commands

| COMMAND | DESCRIPTION |
|---|---|
| `show reference object username [username]` | Displays which configuration settings reference the specified user object. |
| `show reference object address [object_name]` | Displays which configuration settings reference the specified address object. |
| `show reference object address6 [object_name]` | Displays which configuration settings reference the specified IPv6 address object. |
| `show reference object eps [object_name]` | Displays which configuration settings reference the specified endpoint security object. |
| `show reference object service [object_name]` | Displays which configuration settings reference the specified service object. |
| `show reference object schedule [object_name]` | Displays which configuration settings reference the specified schedule object. |
| `show reference object interface [interface_name \| virtual_interface_name]` | Displays which configuration settings reference the specified interface or virtual interface object. |
| `show reference object aaa authentication [default \| auth_method]` | Displays which configuration settings reference the specified AAA authentication object. |
| `show reference object ca category {local\|remote} [cert_name]` | Displays which configuration settings reference the specified authentication method object. |
| `show reference object account pppoe [object_name]` | Displays which configuration settings reference the specified PPPoE account object. |
| `show reference object account pptp [object_name]` | Displays which configuration settings reference the specified PPTP account object. |
| `show reference object sslvpn application [object_name]` | Displays which configuration settings reference the specified SSL VPN application object. |
| `show reference object crypto map [crypto_name]` | Displays which configuration settings reference the specified VPN connection object. |
| `show reference object isakmp policy [isakmp_name]` | Displays which configuration settings reference the specified VPN gateway object. |
| `show reference object sslvpn policy [object_name]` | Displays which configuration settings reference the specified SSL VPN object. |

**Table 6** `show reference` Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| `show reference object zone [object_name]` | Displays which configuration settings reference the specified zone object. |
| `show reference object dhcp6-lease-object [object_name]` | Displays which configuration settings reference the specified DHCPv6 lease object. |
| `show reference object dhcp6-request-object [object_name]` | Displays which configuration settings reference the specified DHCPv6 request object. |
| `show reference object-group username [username]` | Displays which configuration settings reference the specified user group object. |
| `show reference object-group address [object_name]` | Displays which configuration settings reference the specified address group object. |
| `show reference object-group address6 [object_name]` | Displays which configuration settings reference the specified IPv6 address group object. |
| `show reference object-group service [object_name]` | Displays which configuration settings reference the specified service group object. |
| `show reference object-group interface [object_name]` | Displays which configuration settings reference the specified trunk object. |
| `show reference object-group aaa ad [group_name]` | Displays which configuration settings reference the specified AAA AD group object. |
| `show reference object-group aaa ldap [group_name]` | Displays which configuration settings reference the specified AAA LDAP group object. |
| `show reference object-group aaa radius [group_name]` | Displays which configuration settings reference the specified AAA RADIUS group object. |

## 3.1.1 Object Reference Command Example

This example shows how to check which configuration is using an address object named LAN1_SUBNET. For the command output, firewall rule 3 named LAN1-to-USG-2000 is using the address object.

```
Router(config)# show reference object address LAN1_SUBNET

LAN1_SUBNET References:
Category
Rule Priority        Rule Name
Description
================================================================================
Firewall
3                    N/A
LAN1-to-USG-2000
Router(config)#
```

# 4

# Status

This chapter explains some commands you can use to display information about the ZyWALL / USG's current operational state.

**Table 7** Status Show Commands

| COMMAND | DESCRIPTION |
|---|---|
| show boot status | Displays details about the ZyWALL / USG's startup state. |
| show comport status | Displays whether the console and auxiliary ports are on or off. |
| show cpu status | Displays the CPU utilization. |
| show disk | Displays the disk utilization. |
| show extension-slot | Displays the status of the extension card slot and USB ports and the names of devices connected to them. |
| show fan-speed | Displays the current fan speed. |
| show led status | Displays the status of each LED on the ZyWALL / USG. |
| show mac | Displays the ZyWALL / USG's MAC address. |
| show mem status | Displays what percentage of the ZyWALL / USG's memory is currently being used. |
| show ram-size | Displays the size of the ZyWALL / USG's on-board RAM. |
| show redundant-power status | Displays the status of the ZyWALL / USG's power modules. The ZyWALL / USG has two power modules. It can continue operating on a single power module if one fails. |
| show serial-number | Displays the serial number of this ZyWALL / USG. |
| show socket listen | Displays the ZyWALL / USG's listening ports |
| show socket open | Displays the ports that are open on the ZyWALL / USG. |
| show system uptime | Displays how long the ZyWALL / USG has been running since it last restarted or was turned on. |
| show version | Displays the ZyWALL / USG's model, firmware and build information. |

Here are examples of the commands that display the CPU and disk utilization.

```
Router(config)# show cpu status
CPU utilization: 0 %
CPU utilization for 1 min: 0 %
CPU utilization for 5 min: 0 %
Router(config)# show disk
;       <cr>    |
Router(config)# show disk
No. Disk                Size(MB)        Usage
================================================================================
1   image               67              83%
2   onboard flash       163             15%
```

Here are examples of the commands that display the fan speed, MAC address, memory usage, RAM size, and serial number.

```
Router(config)# show fan-speed
FAN1(F00)(rpm): limit(hi)=6500, limit(lo)=1400, max=6650, min=6642, avg=6644
FAN2(F01)(rpm): limit(hi)=6500, limit(lo)=1400, max=6809, min=6783, avg=6795
FAN3(F02)(rpm): limit(hi)=6500, limit(lo)=1400, max=6683, min=6666, avg=6674
FAN4(F03)(rpm): limit(hi)=6500, limit(lo)=1400, max=6633, min=6617, avg=6627
Router(config)# show mac
MAC address: 28:61:32:89:37:61-28:61:32:89:37:67
Router(config)# show mem status
memory usage: 39%
Router(config)# show ram-size
ram size: 510MB
Router(config)# show serial-number
serial number: S060Z12020460
```

Here is an example of the command that displays the listening ports.

```
Router(config)# show socket listen
No.   Proto Local_Address         Foreign_Address       State
================================================================================
1     tcp   0.0.0.0:2601          0.0.0.0:0             LISTEN
2     tcp   0.0.0.0:2602          0.0.0.0:0             LISTEN
3     tcp   127.0.0.1:10443       0.0.0.0:0             LISTEN
4     tcp   0.0.0.0:2604          0.0.0.0:0             LISTEN
5     tcp   0.0.0.0:80            0.0.0.0:0             LISTEN
6     tcp   127.0.0.1:8085        0.0.0.0:0             LISTEN
7     tcp   1.1.1.1:53            0.0.0.0:0             LISTEN
8     tcp   172.23.37.205:53      0.0.0.0:0             LISTEN
9     tcp   10.0.0.8:53           0.0.0.0:0             LISTEN
10    tcp   172.23.37.240:53      0.0.0.0:0             LISTEN
11    tcp   192.168.1.1:53        0.0.0.0:0             LISTEN
12    tcp   127.0.0.1:53          0.0.0.0:0             LISTEN
13    tcp   0.0.0.0:21            0.0.0.0:0             LISTEN
14    tcp   0.0.0.0:22            0.0.0.0:0             LISTEN
15    tcp   127.0.0.1:953         0.0.0.0:0             LISTEN
16    tcp   0.0.0.0:443           0.0.0.0:0             LISTEN
17    tcp   127.0.0.1:1723        0.0.0.0:0             LISTEN
```

Here is an example of the command that displays the open ports.

```
Router(config)# show socket open
No.   Proto Local_Address          Foreign_Address        State
==========================================================================
1     tcp   172.23.37.240:22       172.23.37.10:1179      ESTABLISHED
2     udp   127.0.0.1:64002        0.0.0.0:0
3     udp   0.0.0.0:520            0.0.0.0:0
4     udp   0.0.0.0:138            0.0.0.0:0
5     udp   0.0.0.0:138            0.0.0.0:0
6     udp   0.0.0.0:138            0.0.0.0:0
7     udp   0.0.0.0:138            0.0.0.0:0
8     udp   0.0.0.0:138            0.0.0.0:0
9     udp   0.0.0.0:138            0.0.0.0:0
10    udp   0.0.0.0:138            0.0.0.0:0
11    udp   0.0.0.0:32779          0.0.0.0:0
12    udp   192.168.1.1:4500       0.0.0.0:0
13    udp   1.1.1.1:4500           0.0.0.0:0
14    udp   10.0.0.8:4500          0.0.0.0:0
15    udp   172.23.37.205:4500     0.0.0.0:0
16    udp   172.23.37.240:4500     0.0.0.0:0
17    udp   127.0.0.1:4500         0.0.0.0:0
18    udp   127.0.0.1:63000        0.0.0.0:0
19    udp   127.0.0.1:63001        0.0.0.0:0
20    udp   127.0.0.1:63002        0.0.0.0:0
21    udp   0.0.0.0:161            0.0.0.0:0
22    udp   127.0.0.1:63009        0.0.0.0:0
23    udp   192.168.1.1:1701       0.0.0.0:0
24    udp   1.1.1.1:1701           0.0.0.0:0
25    udp   10.0.0.8:1701          0.0.0.0:0
26    udp   172.23.37.205:1701     0.0.0.0:0
27    udp   172.23.37.240:1701     0.0.0.0:0
28    udp   127.0.0.1:1701         0.0.0.0:0
29    udp   127.0.0.1:63024        0.0.0.0:0
30    udp   127.0.0.1:30000        0.0.0.0:0
31    udp   1.1.1.1:53             0.0.0.0:0
32    udp   172.23.37.205:53       0.0.0.0:0
33    udp   10.0.0.8:53            0.0.0.0:0
34    udp   172.23.37.240:53       0.0.0.0:0
35    udp   192.168.1.1:53         0.0.0.0:0
36    udp   127.0.0.1:53           0.0.0.0:0
37    udp   0.0.0.0:67             0.0.0.0:0
38    udp   127.0.0.1:63046        0.0.0.0:0
39    udp   127.0.0.1:65097        0.0.0.0:0
40    udp   0.0.0.0:65098          0.0.0.0:0
41    udp   192.168.1.1:500        0.0.0.0:0
42    udp   1.1.1.1:500            0.0.0.0:0
43    udp   10.0.0.8:500           0.0.0.0:0
44    udp   172.23.37.205:500      0.0.0.0:0
45    udp   172.23.37.240:500      0.0.0.0:0
46    udp   127.0.0.1:500          0.0.0.0:0
```

Here are examples of the commands that display the system uptime and model, firmware, and build information.

```
Router> show system uptime
system uptime: 04:18:00
Router> show version
ZyXEL Communications Corp.
model           : ZyWALL USG 1100
firmware version: 2.20(AQQ.0)b3
BM version      : 1.08
build date      : 20140901-01-21 01:18:06
```

This example shows the current LED states on the ZyWALL / USG. The **SYS** LED lights on and green. The **AUX** and **HDD** LEDs are both off.

```
Router> show led status
sys: green
aux: off
hdd: off
Router>
```

# 5

# Registration

This chapter introduces myzyxel.com and shows you how to register the ~~ZyWALL~~ZyWALL / USG for IDP/AppPatrol, anti-virus, content filtering, and SSL VPN services using commands.

## 5.1 myZyXEL.com Overview

myZyXEL.com is ZyXEL's online services center where you can register your ZyWALL / USG and manage subscription services available for the ZyWALL / USG.

Note: You need to create an account before you can register your device and activate the services at myZyXEL.com.

You can directly create a myZyXEL.com account, register your ZyWALL / USG and activate a service using the **Licensing > Registration** screens. Alternatively, go to http://www.myZyXEL.com with the ZyWALL / USG's serial number and LAN MAC address to register it. Refer to the web site's on-line help for details.

Note: To activate a service on a ZyWALL / USG, you need to access myZyXEL.com via that ZyWALL / USG.

### 5.1.1 Subscription Services Available on the ZyWALL / USG

The ZyWALL / USG can use anti-virus, anti-spam, IDP/AppPatrol (Intrusion Detection and Prevention and application patrol), SSL VPN, and content filtering subscription services.

- The ZyWALL / USG's anti-virus packet scanner uses the signature files on the ZyWALL / USG to detect virus files. Your ZyWALL / USG scans files transmitting through the enabled interfaces into the network. Subscribe to signature files for ZyXEL's anti-virus engine or one powered by Kaspersky. After the service is activated, the ZyWALL / USG can download the up-to-date signature files from the update server (http://myupdate.zywall.zyxel.com).

  When using the trial, you can switch from one engine to the other in the **Registration** screen. There is no limit on the number of times you can change the anti-virus engine selection during the trial, but you only get a total of one anti-virus trial period (not a separate trial period for each anti-virus engine). After the service is activated, the ZyWALL / USG can download the up-to-date signature files from the update server (http://myupdate.zywall.zyxel.com).

  After the trial expires, you need to purchase an iCard for the anti-virus engine you want to use and enter the PIN number (license key) in the **Registration > Service** screen. You must use the ZyXEL anti-virus iCard for the ZyXEL anti-virus engine and the Kaspersky anti-virus iCard for the Kaspersky anti-virus engine. If you were already using an iCard anti-virus subscription, any remaining time on your earlier subscription is automatically added to the new subscription. Even if the earlier iCard anti-virus subscription was for a different anti-virus engine. For example,

suppose you purchase a one-year Kaspersky engine anti-virus service subscription and use it for six months. Then you purchase a one-year ZyXEL engine anti-virus service subscription and enter the iCard's PIN number (license key) in the **Registration > Service** screen. The one-year ZyXEL engine anti-virus service subscription is automatically extended to 18 months.

- The IDP and application patrol features use the IDP/AppPatrol signature files on the ZyWALL / USG. IDP detects malicious or suspicious packets and responds immediately. Application patrol conveniently manages the use of various applications on the network. After the service is activated, the ZyWALL / USG can download the up-to-date signature files from the update server (http://myupdate.zywall.zyxel.com).
- SSL VPN tunnels provide secure network access to remote users. You can purchase and enter a license key to have the ZyWALL / USG use more SSL VPN tunnels.
- The content filter allows or blocks access to web sites. Subscribe to category-based content filtering to block access to categories of web sites based on content. Your ZyWALL / USG accesses an external database that has millions of web sites categorized based on content. You can have the ZyWALL / USG block, block and/or log access to web sites based on these categories.
- You will get automatic e-mail notification of new signature releases from mySecurityZone after you activate the IDP/AppPatrol service. You can also check for new signatures at http://mysecurity.zyxel.com.

See the respective chapters for more information about these features.

Note: To update the signature file or use a subscription service, you have to register the ZyWALL / USG and activate the corresponding service at myZyXEL.com (through the ZyWALL / USG).

# 5.2 Registration Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 8** Input Values for General Registration Commands

| LABEL | DESCRIPTION |
|---|---|
| *user_name* | The user name of your myZyXEL.com account. You must use six to 20 alphanumeric characters (and the underscore). Spaces are not allowed. |
| *password* | The password for the myZyXEL.com account. You must use six to 20 alphanumeric characters (and the underscore). Spaces are not allowed. |

The following table describes the commands available for registration. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 9** Command Summary: Registration

| COMMAND | DESCRIPTION |
|---|---|
| `device-register checkuser` *user_name* | Checks if the user name exists in the myZyXEL.com database. |
| `device-register username` *user_name* `password` *password* `[e-mail` *user@domainname*`] [country-code` *country_code*`] [reseller-name` *name*`] [reseller-mail` *email-address*`] [reseller-phone` *phone-number*`] [vat` *vat-number*`]` | Registers the device with an existing account or creates a new account and registers the device at one time.<br>*country_code*: see Table 10 on page 50 |

**Table 9** Command Summary: Registration (continued)

| COMMAND | DESCRIPTION |
|---|---|
| service-register checkexpire | Gets information of all service subscriptions from myZyXEL.com and updates the status table. |
| service-register service-type standard license-key *key_value* | Activates a standard service subscription with the license key. |
| service-register service-type trial service {content-filter\|idp} | Activates the content filter or IDP trial service subscription. |
| service-register service-type trial service all {kav\|zav} | Activates all of the trial service subscriptions, including Kaspersky or ZyXEL anti-virus. |
| service-register service-type trial service av {kav\|zav} | Activates a Kaspersky or ZyXEL anti-virus trial service subscription. |
| service-register service-type trial av-engine {kav\|zav} | Changes from one anti-virus engine to the other. |
| show device-register status | Displays whether the device is registered and account information. |
| show service-register reseller-info | Displays your seller's information that you have entered when registration. |
| show service-register server-type | Displays the type of the register server to which your ZyWALL / USG is connected. |
| show service-register status {all\|idp\|av\|sslvpn\|sslvpn-status} | Displays service license information. |
| show service-register status content-filter { bluecoat \| commtouch } | Displays BlueCoat or Commtouch service license information. |
| show service-register content-filter-engine | Displays which external web filtering service the ZyWALL / USG is set to use for content filtering. |
| service-register content-filter-engine { bluecoat \| commtouch } | Sets whether the ZyWALL / USG uses BlueCoat or Commtouch for content filtering. |
| service-register service-type trial service as | Activates the Anti-Spam trial service subscription. |
| show service-register status as | Displays whether the Anti-Spam service is registered and account information. |
| debug service-register erase service as | Removes the ZyWALL / USG's Anti-Spam service registration. |

## 5.2.1 Command Examples

The following commands allow you to register your device with an existing account or create a new account and register the device at one time, and activate a trial service subscription.

```
Router# configure terminal
Router(config)# device-register username alexctsui password 123456
Router(config)# service-register service-type trial service content-filter
```

The following command displays the account information and whether the device is registered.

```
Router# configure terminal
Router(config)# show device-register status
username               : example
password               : 123456
device register status : yes
expiration self check  : no
```

The following command displays the service registration status and type and how many days remain before the service expires.

```
Router# configure terminal
Router(config)# show service-register status all
Service              Status       Type     Count    Expiration
==========================================================================
IDP Signature        Licensed     Standard N/A      176
Anti-Virus           Not Licensed None     N/A      0
SSLVPN               Not Licensed None     5        N/A
Content-Filter       Not Licensed None     N/A      0
```

The following command displays the seller details you have entered on the ZyWALL / USG.

```
Router# configure terminal
Router(config)# show service-register reseller-info
seller's name: ABC
seller's e-mail: abc@example.com
seller's contact number: 12345678
vat number:
```

# 5.3 Country Code

The following table displays the number for each country.

**Table 10** Country Codes

| COUNTRY CODE | COUNTRY NAME | COUNTRY CODE | COUNTRY NAME |
|---|---|---|---|
| 001 | Afghanistan | 002 | Albania |
| 003 | Algeria | 004 | American Samoa |
| 005 | Andorra | 006 | Angola |
| 007 | Anguilla | 008 | Antarctica |
| 009 | Antigua & Barbuda | 010 | Argentina |
| 011 | Armenia | 012 | Aruba |
| 013 | Ascension Island | 014 | Australia |
| 015 | Austria | 016 | Azerbaijan |
| 017 | Bahamas | 018 | Bahrain |
| 019 | Bangladesh | 020 | Barbados |
| 021 | Belarus | 022 | Belgium |

**Table 10** Country Codes (continued)

| COUNTRY CODE | COUNTRY NAME | COUNTRY CODE | COUNTRY NAME |
|---|---|---|---|
| 023 | Belize | 024 | Benin |
| 025 | Bermuda | 026 | Bhutan |
| 027 | Bolivia | 028 | Bosnia and Herzegovina |
| 029 | Botswana | 030 | Bouvet Island |
| 031 | Brazil | 032 | British Indian Ocean Territory |
| 033 | Brunei Darussalam | 034 | Bulgaria |
| 035 | Burkina Faso | 036 | Burundi |
| 037 | Cambodia | 038 | Cameroon |
| 039 | Canada | 040 | Cape Verde |
| 041 | Cayman Islands | 042 | Central African Republic |
| 043 | Chad | 044 | Chile |
| 045 | China | 046 | Christmas Island |
| 047 | Cocos (Keeling) Islands | 048 | Colombia |
| 049 | Comoros | 050 | Congo, Democratic Republic of the |
| 051 | Congo, Republic of | 052 | Cook Islands |
| 053 | Costa Rica | 054 | Cote d'Ivoire |
| 055 | Croatia/Hrvatska | 056 | Cyprus |
| 057 | Czech Republic | 058 | Denmark |
| 059 | Djibouti | 060 | Dominica |
| 061 | Dominican Republic | 062 | East Timor |
| 063 | Ecuador | 064 | Egypt |
| 065 | El Salvador | 066 | Equatorial Guinea |
| 067 | Eritrea | 068 | Estonia |
| 069 | Ethiopia | 070 | Falkland Islands (Malvina) |
| 071 | Faroe Islands | 072 | Fiji |
| 073 | Finland | 074 | France |
| 075 | France (Metropolitan) | 076 | French Guiana |
| 077 | French Polynesia | 078 | French Southern Territories |
| 079 | Gabon | 080 | Gambia |
| 081 | Georgia | 082 | Germany |
| 083 | Ghana | 084 | Gibraltar |
| 085 | Great Britain | 086 | Greece |
| 087 | Greenland | 088 | Grenada |
| 089 | Guadeloupe | 090 | Guam |
| 091 | Guatemala | 092 | Guernsey |
| 093 | Guinea | 094 | Guinea-Bissau |
| 095 | Guyana | 096 | Haiti |
| 097 | Heard and McDonald Islands | 098 | Holy See (City Vatican State) |
| 099 | Honduras | 100 | Hong Kong |
| 101 | Hungary | 102 | Iceland |

**Table 10** Country Codes (continued)

| COUNTRY CODE | COUNTRY NAME | COUNTRY CODE | COUNTRY NAME |
|---|---|---|---|
| 103 | India | 104 | Indonesia |
| 105 | Ireland | 106 | Isle of Man |
| 107 | Italy | 108 | Jamaica |
| 109 | Japan | 110 | Jersey |
| 111 | Jordan | 112 | Kazakhstan |
| 113 | Kenya | 114 | Kiribati |
| 115 | Korea, Republic of | 116 | Kuwait |
| 117 | Kyrgyzstan | 118 | Lao People's Democratic Republic |
| 119 | Latvia | 120 | Lebanon |
| 121 | Lesotho | 122 | Liberia |
| 123 | Liechtenstein | 124 | Lithuania |
| 125 | Luxembourg | 126 | Macau |
| 127 | Macedonia, Former Yugoslav Republic | 128 | Madagascar |
| 129 | Malawi | 130 | Malaysia |
| 131 | Maldives | 132 | Mali |
| 133 | Malta | 134 | Marshall Islands |
| 135 | Martinique | 136 | Mauritania |
| 137 | Mauritius | 138 | Mayotte |
| 139 | Mexico | 140 | Micronesia, Federal State of |
| 141 | Moldova, Republic of | 142 | Monaco |
| 143 | Mongolia | 144 | Montserrat |
| 145 | Morocco | 146 | Mozambique |
| 147 | Namibia | 148 | Nauru |
| 149 | Nepal | 150 | Netherlands |
| 151 | Netherlands Antilles | 152 | New Caledonia |
| 153 | New Zealand | 154 | Nicaragua |
| 155 | Niger | 156 | Nigeria |
| 157 | Niue | 158 | Norfolk Island |
| 159 | Northern Mariana Islands | 160 | Norway |
| 161 | Not Determined | 162 | Oman |
| 163 | Pakistan | 164 | Palau |
| 165 | Panama | 166 | Papua New Guinea |
| 167 | Paraguay | 168 | Peru |
| 169 | Philippines | 170 | Pitcairn Island |
| 171 | Poland | 172 | Portugal |
| 173 | Puerto Rico | 174 | Qatar |
| 175 | Reunion Island | 176 | Romania |
| 177 | Russian Federation | 178 | Rwanda |
| 179 | Saint Kitts and Nevis | 180 | Saint Lucia |
| 181 | Saint Vincent and the Grenadines | 182 | San Marino |

**Table 10** Country Codes (continued)

| COUNTRY CODE | COUNTRY NAME | COUNTRY CODE | COUNTRY NAME |
|---|---|---|---|
| 183 | Sao Tome and Principe | 184 | Saudi Arabia |
| 185 | Senegal | 186 | Seychelles |
| 187 | Sierra Leone | 188 | Singapore |
| 189 | Slovak Republic | 190 | Slovenia |
| 191 | Solomon Islands | 192 | Somalia |
| 193 | South Africa | 194 | South Georgia and the South Sandwich Islands |
| 185 | Spain | 196 | Sri Lanka |
| 197 | St Pierre and Miquelon | 198 | St. Helena |
| 199 | Suriname | 200 | Svalbard and Jan Mayen Islands |
| 201 | Swaziland | 202 | Sweden |
| 203 | Switzerland | 204 | Taiwan |
| 205 | Tajikistan | 206 | Tanzania |
| 207 | Thailand | 208 | Togo |
| 209 | Tokelau | 210 | Tonga |
| 211 | Trinidad and Tobago | 212 | Tunisia |
| 213 | Turkey | 214 | Turkmenistan |
| 215 | Turks and Caicos Islands | 216 | Tuvalu |
| 217 | US Minor Outlying Islands | 218 | Uganda |
| 219 | Ukraine | 220 | United Arab Emirates |
| 221 | United Kingdom | 222 | United States |
| 223 | Uruguay | 224 | Uzbekistan |
| 225 | Vanuatu | 226 | Venezuela |
| 227 | Vietnam | 228 | Virgin Islands (British) |
| 229 | Virgin Islands (USA) | 230 | Wallis And Futuna Islands |
| 231 | Western Sahara | 232 | Western Samoa |
| 233 | Yemen | 234 | Yugoslavia |
| 235 | Zambia | 236 | Zimbabwe |

# 6

# AP Management

This chapter shows you how to configure wireless AP management options on your ZyWALL / USG.

## 6.1 AP Management Overview

The ZyWALL / USG allows you to remotely manage all of the Access Points (APs) on your network. You can manage a number of APs without having to configure them individually as the ZyWALL / USG automatically handles basic configuration for you.

The commands in this chapter allow you to add, delete, and edit the APs managed by the ZyWALL / USG by means of the CAPWAP protocol. An AP must be moved from the wait list to the management list before you can manage it. If you do not want to use this registration mechanism, you can disable it and then any newly connected AP is registered automatically.

## 6.2 AP Management Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 11** Input Values for General AP Management Commands

| LABEL | DESCRIPTION |
|---|---|
| *ap_mac* | The Ethernet MAC address of the managed AP. Enter 6 hexidecimal pairs separated by colons. You can use 0-9, a-z and A-Z. |
| *ap_model* | The model name of the managed AP, such as NWA5160N, NWA5560-N, NWA5550-N, NWA5121-NI or NWA5123-NI. |
| *slot_name* | The slot name for the AP's on-board wireless LAN card. Use either *slot1* or *slot2*. (The NWA5560-N supports up to 2 radio slots.) |
| *profile_name* | The wireless LAN radio profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *ap_description* | The AP description. This is strictly used for reference purposes and has no effect on any other settings. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *sta_mac* | The MAC address of the wireless client. Enter 6 hexidecimal pairs separated by colons. You can use 0-9, a-z and A-Z. |

The following table describes the commands available for AP management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 12** Command Summary: AP Management

| COMMAND | DESCRIPTION |
|---|---|
| `capwap ap add ap_mac [ap_model]` | Adds the specified AP to the ZyWALL / USG for management. If manual add is disabled, this command can still be used; if you add an AP before it connects to the network, then this command simply preconfigures the management list with that AP's information. |
| `capwap ap kick {all \| ap_mac}` | Removes the specified AP (*ap_mac*) or all connected APs (*all*) from the management list. Doing this removes the AP(s) from the management list.<br>If the ZyWALL / USG is set to automatically add new APs to the AP management list, then any kicked APs are added back to the management list as soon as they reconnect. |
| `capwap ap reboot ap_mac` | Forces the specified AP (*ap_mac*) to restart. Doing this severs the connections of all associated stations. |
| `capwap ap ap_mac` | Enters the sub-command mode for the specified AP. |
| `slot_name ap-profile profile_name` | Sets the radio (*slot_name*) to AP mode and assigns a created profile to the radio. |
| `no slot_name ap-profile` | Removes the AP mode profile assignment for the specified radio (*slot_name*). |
| `description ap_description` | Sets the description for the specified AP. |
| `[no] force vlan` | Sets whether or not the ZyWALL / USG changes the AP's management VLAN to match the one you configure using the `vlan` sub-command. The management VLAN on the ZyWALL / USG and AP must match for the ZyWALL / USG to manage the AP. |
| `vlan <1..4094> {tag \| untag}` | Sets the VLAN ID for the specified AP as well as whether packets sent to and from that ID are tagged or untagged. |
| `exit` | Exits the sub-command mode for the specified AP. |
| `capwap manual-add {enable \| disable}` | Allows the ZyWALL / USG to either automatically add new APs to the network (*disable*) or wait until you manually confirm them (*enable*). |
| `capwap show statistic` | Displays statistics about the wireless radio transmitters in each of the APs connected to the ZyWALL / USG. |
| `capwap station kick sta_mac` | Forcibly disconnects the specified station from the network. |
| `show capwap ap wait-list` | Displays a list of connected but as-of-yet unmanaged APs. This is known as the 'wait list'. |
| `show capwap ap ap_mac slot_name detail` | Displays details for the specified radio (*slot_name*) on the specified AP (*ap_mac*). |
| `show capwap ap {all \| ap_mac}` | Displays the management list (*all*) or whether the specified AP is on the management list (*ap_mac*). |
| `show capwap ap {all \| ap_mac} config status` | Displays whether or not any AP's configuration or the specified AP's configuration is in conflict with the ZyWALL / USG's settings for the AP and displays the settings in conflict if there are any. |
| `show capwap ap all statistics` | Displays radio statistics for all APs on the management list. |
| `show capwap manual-add` | Displays the current manual add option. |
| `show capwap station all` | Displays information for all stations connected to the APs on the management list. |

## 6.2.1 AP Management Commands Example

The following example shows you how to add an AP to the management list, and then edit it.

```
Router# show capwap ap wait-list
index: 1
  IP: 192.168.1.35, MAC: 00:11:11:11:11:FE
  Model: NWA5160N, Description: AP-00:11:11:11:11:FE
index: 2
  IP: 192.168.1.36, MAC: 00:19:CB:00:BB:03
  Model: NWA5160N, Description: AP-00:19:CB:00:BB:03
Router# configure terminal
Router(config)# capwap ap add 00:19:CB:00:BB:03
Router(config)# capwap ap 00:19:CB:00:BB:03
Router(AP 00:19:CB:00:BB:03)# slot1 ap-profile approf01
Router(AP 00:19:CB:00:BB:03)# exit
Router(config)# show capwap ap all
index: 1
  Status: RUN
  IP: 192.168.1.37, MAC: 40:4A:03:05:82:1E
  Description: AP-404A0305821E
  Model: NWA5160N
  R1 mode: AP, R1Prof: default
  R2 mode: AP, R2Prof: n/a
  Station: 0, RadioNum: 2
  Mgnt. VLAN ID: 1, Tag: no
  WTP VLAN ID: 1, WTP Tag: no
  Force VLAN: disable
  Firmware Version: 2.25(AAS.0)b2
  Recent On-line Time: 08:43:04 2013/05/24
  Last Off-line Time: N/A

Router(config)# show capwap ap 40:4A:03:05:82:1E slot1 detail
index: 1
  SSID: ZyXEL, BSSID: 40:4A:03:05:82:1F
  SecMode: NONE, Forward Mode: Local Bridge, Vlan: 1

Router(config)# show capwap ap all statistics
index: 1
  Status: RUN, Loading: -
  AP MAC: 40:4A:03:05:82:1E
  Radio: 1, OP Mode: AP
  Profile: default, MAC: 40:4A:03:05:82:1F
  Description: AP-404A0305821E
  Model: NWA5160N
  Band: 2.4GHz, Channel: 6
  Station: 0
  RxPkt: 4463, TxPkt: 38848
  RxFCS: 1083323, TxRetry: 198478
```

# 7

# Wireless LAN Profiles

This chapter shows you how to configure wireless LAN profiles on your ZyWALL / USG.

## 7.1 Wireless LAN Profiles Overview

The managed Access Points designed to work explicitly with your ZyWALL / USG do not have on-board configuration files, you must create “profiles” to manage them. Profiles are preset configurations that are uploaded to the APs and which manage them. They include: Radio and Monitor profiles, SSID profiles, Security profiles, and MAC Filter profiles. Altogether, these profiles give you absolute control over your wireless network.

## 7.2 AP Profile Commands

The radio profile commands allow you to set up configurations for the radios onboard your various APs.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 13** Input Values for General Radio and Monitor Profile Commands

| LABEL | DESCRIPTION |
|---|---|
| *radio_profile_name* | The radio profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *wlan_role* | Sets the wireless LAN radio operating mode. At the time of writing, you can use *ap* for Access Point. |
| *wireless_channel_2g* | Sets the 2 GHz channel used by this radio profile. The channel range is 1 - 14.<br><br>Note: Your choice of channel may be restricted by regional regulations. |
| wireless_channel_5g | Sets the 5 GHz channel used by this radio profile. The channel range is 36 - 165.<br><br>Note: Your choice of channel may be restricted by regional regulations. |
| *wlan_hctw* | Sets the HT channel width. Select either auto or 20m. |
| *wlan_htgi* | Sets the HT guard interval. Select either long or short. |
| *wlan_2g_basic_speed* | Sets the basic band rate for 2.4 GHz. The available band rates are 1.0, 2.0, 5.5, 11.0, 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0. |
| *wlan_2g_support_speed* | Sets the support rate for the 2.4 GHz band. The available band rates are: 1.0, 2.0, 5.5, 11.0, 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0. |

**Table 13** Input Values for General Radio and Monitor Profile Commands (continued)

| LABEL | DESCRIPTION |
|---|---|
| *wlan_mcs_speed* | Sets the HT MCS rate. The available rates are: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15. |
| *wlan_5g_basic_speed* | Sets the basic band rate for 5 GHz. The available band rates are: 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0. |
| *wlan_5g_support_speed* | Sets the support rate for the 5 GHz band. The available band rates are: 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0. |
| *chain_mask* | Sets the network traffic chain mask. The range is 1 - 7. |
| *wlan_power* | Sets the radio output power. Select 100%, 50%, 25%, or 12.5%. |
| *wlan_interface_index* | Sets the radio interface index number. The range is 1 - 8. |
| *ssid_profile* | Sets the associated SSID profile name. This name must be an existing SSID profile. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |

The following table describes the commands available for radio profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 14** Command Summary: Radio Profile

| COMMAND | DESCRIPTION |
|---|---|
| `show wlan-radio-profile {all \| radio_profile_name}` | Displays the radio profile(s).<br>*all*: Displays all profiles for the selected operating mode.<br>*radio_profile_name*: Displays the specified profile for the selected operating mode. |
| `wlan-radio-profile rename radio_profile_name1 radio_profile_name2` | Gives an existing radio profile (*radio_profile_name1*) a new name (*radio_profile_name2*). |
| `[no] wlan-radio-profile radio_profile_name` | Enters configuration mode for the specified radio profile. Use the `no` parameter to remove the specified profile. |
| `[no] activate` | Makes this profile active or inactive. |
| `role ap` | Sets the operating mode of the radio in this profile. |
| `rssi-dbm <-20~-76>` | When using the RSSI threshold, set a minimum client signal strength for connecting to the AP. -20 dBm is the strongest signal you can require and -76 is the weakest. |
| `[no] rssi-thres` | Sets whether or not to use the Received Signal Strength Indication (RSSI) threshold to ensure wireless clients receive good throughput. This allows only wireless clients with a strong signal to connect to the AP. |
| `band {2.4G \|5G} [band-mode {11n \| bg \| a}]` | Sets the radio band (2.4 GHz or 5 GHz) and band mode for this profile. Band mode details:<br>For 2.4 GHz, `11n` lets IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n clients associate with the AP.<br>For 2.4 GHz, `bg` lets IEEE 802.11b and IEEE 802.11g clients associate with the AP.<br>For 5 GHz, `11n` lets IEEE 802.11a and IEEE 802.11n clients associate with the AP.<br>For 5 GHz, `a` lets only IEEE 802.11a clients associate with the AP. |
| `[no] disable-dfs-switch` | Makes the DFS switch active or inactive. By default this is inactive. |

**Table 14** Command Summary: Radio Profile (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] dot11n-disable-coexistence | Fixes the channel bandwidth as 40 MHz. The no command has the AP automatically choose 40 MHz if all the clients support it or 20 MHz if some clients only support 20 MHz. |
| [no] ctsrts <0..2347> | Sets or removes the RTS/CTS value for this profile.<br>Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions).<br>A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off.<br>The default is 2347. |
| [no] frag <256..2346> | Sets or removes the fragmentation value for this profile.<br>The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent.<br>The default is 2346. |
| dtim-period <1..255> | Sets the DTIM period for this profile.<br>Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.<br>The default is 1. |
| beacon-interval <40..1000> | Sets the beacon interval for this profile.<br>When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. This value can be set from 40ms to 1000ms. A high value helps save current consumption of the access point.<br>The default is 100. |
| [no] ampdu | Activates MPDU frame aggregation for this profile. Use the *no* parameter to disable it.<br>Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates.<br>By default this is enabled. |
| limit-ampdu <100..65535> | Sets the maximum frame size to be aggregated.<br>By default this is 50000. |
| subframe-ampdu <2..64> | Sets the maximum number of frames to be aggregated each time.<br>By default this is 32. |

**Table 14** Command Summary: Radio Profile (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] amsdu | Activates MPDU frame aggregation for this profile. Use the *no* parameter to disable it.<br>Mac Service Data Unit (MSDU) aggregation collects Ethernet frames without any of their 802.11n headers and wraps the header-less payload in a single 802.11n MAC header. This method is useful for increasing bandwidth throughput. It is also more efficient than A-MPDU except in environments that are prone to high error rates.<br>By default this is enabled. |
| limit-amsdu <2290..4096> | Sets the maximum frame size to be aggregated.<br>The default is 4096. |
| [no] multicast-to-unicast | "Multicast to unicast" broadcasts wireless multicast traffic to all wireless clients as unicast traffic to provide more reliable transmission. The data rate changes dynamically based on the application's bandwidth requirements. Although unicast provides more reliable transmission of the multicast traffic, it also produces duplicate packets.<br>The no command turns multicast to unicast off to send wireless multicast traffic at the rate you specify with the 2g-multicast-speed or 5g-multicast-speed command. |
| [no] block-ack | Makes block-ack active or inactive. Use the *no* parameter to disable it. |
| ch-width *wlan_htcw* | Sets the channel width for this profile. |
| guard-interval *wlan_htgi* | Sets the guard interval for this profile.<br>The default for this is *short*. |
| 2g-basic-speed *wlan_2g_basic_speed* | Sets the 2.4 GHz basic band rates.<br>The default is 1.0 2.0 5.5 11.0. |
| 2g-channel *wireless_channel_2g* | Sets the broadcast band for this profile in the 2.4 GHz frequency range. The default is 6. |
| 2g-mcs-speed {disable \| *wlan_mcs_speed*} | Disables or sets the 2.4 GHz HT MCS rate.<br>The default is 0~15. |
| 2g-multicast-speed *wlan_2g_support_speed* | When you disable multicast to unicast, use this command to set the data rate { 1.0 \| 2.0 \| … } in Mbps for 2.4 GHz multicast traffic. |
| 2g-support-speed {disable \| *wlan_2g_support_speed*} | Disables or sets the 2.4 GHz support rate.<br>The default is 1.0~54.0. |
| 5g-basic-speed *wlan_5g_basic_speed* | Sets the 5 GHz basic band rate.<br>The default is 6.0 12.0 24.0. |
| 5g-channel *wireless_channel_5g* | Sets the broadcast band for this profile in the 5 GHz frequency range. The default is 36. |
| 5g-mcs-speed {disable \| *wlan_mcs_speed*} | Disables or sets the 5 GHz HT MCS rate.<br>The default is 0~15. |
| 5g-multicast-speed {*wlan_5g_basic_speed*} | When you disable multicast to unicast, use this command to set the data rate { 6.0 \| 9.0 \| … } in Mbps for 5 GHz multicast traffic. |

**Table 14** Command Summary: Radio Profile (continued)

| COMMAND | DESCRIPTION |
|---|---|
| 5g-support-speed {disable \| *wlan_5g_support_speed*} | Disables or sets the 5 GHz support rate.<br>The default is 6.0~54.0. |
| tx-mask *chain_mask* | Sets the outgoing chain mask rate. |
| rx-mask *chain_mask* | Sets the incoming chain mask rate. |
| [no] htprotection | Activates HT protection for this profile. Use the *no* parameter to disable it.<br>By default, this is disabled. |
| output-power *wlan_power* | Sets the output power for the radio in this profile.<br>The default is 100%. |
| [no] ssid-profile *wlan_interface_index ssid_profile* | Assigns an SSID profile to this radio profile. Requires an existing SSID profile. Use the no parameter to disable it. |
| exit | Exits configuration mode for this profile. |

## 7.2.1 AP Profile Commands Example

The following example shows you how to set up the radio profile named ‘RADIO01’, activate it, and configure it to use the following settings:

- 2.4G band with channel 6
- channel width of 20MHz
- a DTIM period of 2
- a beacon interval of 100ms
- AMPDU frame aggregation enabled
- an AMPDU buffer limit of 65535 bytes
- an AMPDU subframe limit of 64 frames
- AMSDU frame aggregation enabled
- an AMSDU buffer limit of 4096
- block acknowledgement enabled
- a short guard interval
- an output power of 100%

It will also assign the SSID profile labeled ‘default’ in order to create WLAN VAP (wlan-1-1) functionality within the radio profile.

```
Router(config)# wlan-radio-profile RADIO01
Router(config-profile-radio)# activate
Router(config-profile-radio)# band 2.4G
Router(config-profile-radio)# 2g-channel 6
Router(config-profile-radio)# ch-width 20m
Router(config-profile-radio)# dtim-period 2
Router(config-profile-radio)# beacon-interval 100
Router(config-profile-radio)# ampdu
Router(config-profile-radio)# limit-ampdu 65535
Router(config-profile-radio)# subframe-ampdu 64
Router(config-profile-radio)# amsdu
Router(config-profile-radio)# limit-amsdu 4096
Router(config-profile-radio)# block-ack
Router(config-profile-radio)# guard-interval short
Router(config-profile-radio)# tx-mask 5
Router(config-profile-radio)# rx-mask 7
Router(config-profile-radio)# output-power 100%
Router(config-profile-radio)# ssid-profile 1 default
```

# 7.3 SSID Profile Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 15** Input Values for General SSID Profile Commands

| LABEL | DESCRIPTION |
|---|---|
| *ssid_profile_name* | The SSID profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *ssid* | The SSID broadcast name. You may use 1-32 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive. |
| *wlan_qos* | Sets the type of QoS the SSID should use.<br>*disable*: Turns off QoS for this SSID.<br>*wmm*: Turns on QoS for this SSID. It automatically assigns Access Categories to packets as the device inspects them in transit.<br>*wmm_be*: Assigns the “best effort” Access Category to all traffic moving through the SSID regardless of origin.<br>*wmm_bk*: Assigns the “background” Access Category to all traffic moving through the SSID regardless of origin.<br>*wmm_vi*: Assigns the “video” Access Category to all traffic moving through the SSID regardless of origin.<br>*wmm_vo*: Assigns the “voice” Access Category to all traffic moving through the SSID regardless of origin. |
| vlan_iface | The VLAN interface name of the controller (in this case, it is NXC5200). The maximum VLAN interface number is product-specific; for the ZyWALL / USG, the number is 512. |
| *securityprofile* | Assigns an existing security profile to the SSID profile. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |

**Table 15** Input Values for General SSID Profile Commands (continued)

| LABEL | DESCRIPTION |
|---|---|
| *macfilterprofile* | Assigns an existing MAC filter profile to the SSID profile. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *description2* | Sets the description of the profile. You may use up to 60 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive. |

The following table describes the commands available for SSID profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 16** Command Summary: SSID Profile

| COMMAND | DESCRIPTION |
|---|---|
| `show wlan-ssid-profile {all \| ssid_profile_name}` | Displays the SSID profile(s).<br>*all*: Displays all profiles for the selected operating mode.<br>*ssid_profile_name*: Displays the specified profile for the selected operating mode. |
| `wlan-ssid-profile rename ssid_profile_name1 ssid_profile_name2` | Gives an existing SSID profile (*ssid_profile_name1*) a new name (*ssid_profile_name2*). |
| `[no] wlan-ssid-profile ssid_profile_name` | Enters configuration mode for the specified SSID profile. Use the *no* parameter to remove the specified profile. |
| `[no] block-intra` | Enables intra-BSSID traffic blocking. Use the `no` parameter to disable it in this profile.<br>By default this is disabled. |
| `[no] hide` | Prevents the SSID from being publicly broadcast. Use the `no` parameter to re-enable public broadcast of the SSID in this profile.<br>By default this is disabled. |
| `ssid` | Sets the SSID. This is the name visible on the network to wireless clients. Enter up to 32 characters, spaces and underscores are allowed.<br>The default SSID is 'ZyXEL'. |
| `qos wlan_qos` | Sets the type of QoS used by this SSID. |
| `vlan-id <1..4094>` | Applies to each SSID profile that uses `localbridge`. If the VLAN ID is equal to the AP's native VLAN ID then traffic originating from the SSID is not tagged.<br>The default VLAN ID is 1. |
| `[no] vlan-support` | Sets the ZyWALL / USG to tag traffic from the local Virtual AP (VAP) with the VLAN ID specified in this SSID profile.<br>The `no` command sets the ZyWALL / USG to not tag traffic from the local Virtual AP (VAP) with the VLAN ID. |
| `security securityprofile` | Assigns the specified security profile to this SSID profile. |
| `[no] macfilter macfilterprofile` | Assigns the specified MAC filtering profile to this SSID profile. Use the `no` parameter to remove it.<br>By default, no MAC filter is assigned. |
| `exit` | Exits configuration mode for this profile. |

### 7.3.1 SSID Profile Example

The following example creates an SSID profile with the name 'ZyXEL'. It makes the assumption that both the security profile (SECURITY01) and the MAC filter profile (MACFILTER01) already exist.

```
Router(config)# wlan-ssid-profile SSID01
Router(config-ssid-radio)# ssid ZyXEL
Router(config-ssid-radio)# qos wmm
Router(config-ssid-radio)# data-forward localbridge
Router(config-ssid-radio)# security SECURITY01
Router(config-ssid-radio)# macfilter MACFILTER01
Router(config-ssid-radio)# exit
Router(config)#
```

## 7.4 Security Profile Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 17** Input Values for General Security Profile Commands

| LABEL | DESCRIPTION |
|---|---|
| *security_profile_name* | The security profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *wep_key* | Sets the WEP key encryption strength. Select either *64bit* or *128bit*. |
| *wpa_key* | Sets the WPA/WPA2 pre-shared key in ASCII. You may use 8~63 alphanumeric characters. This value is case-sensitive. |
| *wpa_key_64* | Sets the WPA/WPA2 pre-shared key in HEX. You muse use 64 alphanumeric characters. |
| *secret* | Sets the shared secret used by your network's RADIUS server. |
| *auth_method* | The authentication method used by the security profile. |

The following table describes the commands available for security profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 18** Command Summary: Security Profile

| COMMAND | DESCRIPTION |
|---|---|
| `show wlan-security-profile {all \| security_profile_name}` | Displays the security profile(s).<br>*all*: Displays all profiles for the selected operating mode.<br>*security_profile_name*: Displays the specified profile for the selected operating mode. |
| `wlan-security-profile rename security_profile_name1 security_profile_name2` | Gives existing security profile (*security_profile_name1*) a new name, (*security_profile_name2*). |
| `[no] wlan-security-profile security_profile_name` | Enters configuration mode for the specified security profile. Use the *no* parameter to remove the specified profile. |
| `mode {none \| wep \| wpa \| wpa2 \| wpa2-mix}` | Sets the security mode for this profile. |

**Table 18** Command Summary: Security Profile (continued)

| COMMAND | DESCRIPTION |
|---|---|
| wep <64 \| 128> default-key <1..4> | Sets the WEP encryption strength (*64 or 128*) and the default key value (*1 ~ 4*).<br>If you select WEP-64 enter 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x11AA22BB33) for each Key used; or enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for each Key used.<br>If you select WEP-128 enter 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x00112233445566778899AABBCC) for each Key used; or enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for each Key used.<br>You can save up to four different keys. Enter the default-key (*1 ~ 4*) to save your WEP to one of those four available slots. |
| wep-auth-type {open \| share} | Sets the authentication key type to either *open* or *share*. |
| wpa-encrypt {tkip \| aes \| auto} | Sets the WPA/WPA2 encryption cipher type.<br>auto: This automatically chooses the best available cipher based on the cipher in use by the wireless client that is attempting to make a connection.<br>tkip: This is the Temporal Key Integrity Protocol encryption method added later to the WEP encryption protocol to further secure. Not all wireless clients may support this.<br>aes: This is the Advanced Encryption Standard encryption method, a newer more robust algorithm than TKIP Not all wireless clients may support this. |
| wpa-psk {*wpa_key* \| *wpa_key_64*} | Sets the WPA/WPA2 pre-shared key. |
| [no] wpa2-preauth | Enables pre-authentication to allow wireless clients to switch APs without having to re-authenticate their network connection. The RADIUS server puts a temporary PMK Security Authorization cache on the wireless clients. It contains their session ID and a pre-authorized list of viable APs.<br>Use the no parameter to disable this. |
| [no] reauth <30..30000> | Sets the interval (in seconds) between authentication requests.<br>The default is 0. |
| idle <30..30000> | Sets the idle interval (in seconds) that a client can be idle before authentication is discontinued.<br>The default is 300. |
| group-key <30..30000> | Sets the interval (in seconds) at which the AP updates the group WPA/WPA2 encryption key.<br>The default is 1800. |
| [no] dot1x-eap | Enables 802.1x secure authentication. Use the no parameter to disable it. |
| eap {external \| internal *auth_method*} | Sets the 802.1x authentication method. |
| [no] server-auth <1..2> activate | Activates server authentication. Use the no parameter to deactivate. |
| server-auth <1..2> ip address *ipv4_address* port <1..65535> secret *secret* | Sets the IPv4 address, port number and shared secret of the RADIUS server to be used for authentication. |
| [no] server-auth <1..2> | Clears the server authentication setting. |
| exit | Exits configuration mode for this profile. |

### 7.4.1 Security Profile Example

The following example creates a security profile with the name ‘SECURITY01’..

```
Router(config)# wlan-security-profile SECURITY01
Router(config-security-profile)# mode wpa2
Router(config-security-profile)# wpa-encrypt aes
Router(config-security-profile)# wpa-psk 12345678
Router(config-security-profile)# idle 3600
Router(config-security-profile)# reauth 1800
Router(config-security-profile)# group-key 1800
Router(config-security-profile)# exit
Router(config)#
```

## 7.5 MAC Filter Profile Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 19** Input Values for General MAC Filter Profile Commands

| LABEL | DESCRIPTION |
|---|---|
| *macfilter_profile_name* | The MAC filter profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *mac* | Enter six hexadecimal pairs separated by colons for the MAC address of the wireless device to which to apply the filter. |
| *description2* | Sets the description of the profile. You may use up to 60 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive. |

The following table describes the commands available for security profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 20** Command Summary: MAC Filter Profile

| COMMAND | DESCRIPTION |
|---|---|
| `show wlan-macfilter-profile {all \| macfilter_profile_name}` | Displays the security profile(s).<br>*all*: Displays all profiles for the selected operating mode.<br>*macfilter_profile_name*: Displays the specified profile for the selected operating mode. |
| `wlan-macfilter-profile rename macfilter_profile_name1 macfilter_profile_name2` | Gives an existing security profile (*macfilter_profile_name1*) a new name (*macfilter_profile_name2*). |
| `[no] wlan-macfilter-profile macfilter_profile_name` | Enters configuration mode for the specified MAC filter profile. Use the *no* parameter to remove the specified profile. |
| `filter-action {allow \| deny}` | Permits the wireless client with the MAC addresses in this profile to connect to the network through the associated SSID; select deny to block the wireless clients with the specified MAC addresses.<br>The default is set to *deny*. |

**Table 20** Command Summary: MAC Filter Profile (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] *mac* description *description2* | Sets the MAC address (with optional description) to which this profile applies. |
| exit | Exits configuration mode for this profile. |

## 7.5.1 MAC Filter Profile Example

The following example creates a MAC filter profile with the name ‘MACFILTER01’..

```
Router(config)# wlan-macfilter-profile test
Router(config-macfilter-profile test)# filter-action deny
Router(config-macfilter-profile test)# 01:02:03:04:05:06  description MAC01
Router(config-macfilter-profile test)# 01:02:03:04:05:07  description MAC02
Router(config-macfilter-profile test)# 01:02:03:04:05:08  description MAC03
Router(config-macfilter-profile)# exit
Router(config)#
```

# 8

# Interfaces

This chapter shows you how to use interface-related commands.

## 8.1 Interface Overview

In general, an interface has the following characteristics.

- An interface is a logical entity through which (layer-3) packets pass.
- An interface is bound to a physical port or another interface.
- Many interfaces can share the same physical port.
- An interface is bound to at most one zone.
- Many interface can belong to the same zone.
- Layer-3 virtualization (IP alias, for example) is a kind of interface.

Some characteristics do not apply to some types of interfaces.

### 8.1.1 Types of Interfaces

You can create several types of interfaces in the ZyWALL / USG. The types supported vary by ZyWALL / USG model.

- **Port groups** create a hardware connection between physical ports at the layer-2 (data link, MAC address) level.
- **Ethernet interfaces** are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- **VLAN interfaces** receive and send tagged frames. The ~~ZyWALL~~ZyWALL / USG automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- **Bridge interfaces** create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Unlike port groups, bridge interfaces can take advantage of some security features in the ZyWALL / USG. You can also assign an IP address and subnet mask to the bridge.
- **PPPoE/PPTP interfaces** support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE/PPTP interfaces.
- **Cellular interfaces** are for 3G WAN connections via a connected 3G device.
- **WLAN interfaces** are for wireless LAN (IEEE 802.11b/g) connections via an installed wireless LAN card.
- **Virtual interfaces** (IP alias) provide additional routing information in the ZyWALL / USG. There are three types: **virtual Ethernet interfaces**, **virtual VLAN interfaces**, and **virtual bridge interfaces**.

- The **auxiliary interface**, along with an external modem, provides an interface the ZyWALL / USG can use to dial out. This interface can be used as a backup WAN interface, for example. The auxiliary interface controls the **DIAL BACKUP** port (labeled **AUX** on some models).
- **Trunks** manage load balancing between interfaces.

Port groups, trunks, and the auxiliary interface have a lot of characteristics that are specific to each type of interface. These characteristics are listed in the following tables and discussed in more detail farther on.

**Table 21** Characteristics of Ethernet, VLAN, Bridge, PPPoE/PPTP, and Virtual Interface (ZyWALL / USG USG 300 and Above)

| CHARACTERISTICS | ETHERNET | VLAN | BRIDGE | PPPOE/PPTP | VIRTUAL |
|---|---|---|---|---|---|
| Name* | gex | vlanx | brx | pppx | ** |
| IP Address Assignment | | | | | |
| static IP address | Yes | Yes | Yes | Yes | Yes |
| DHCP client | Yes | Yes | Yes | Yes | No |
| routing metric | Yes | Yes | Yes | Yes | Yes |
| Interface Parameters | | | | | |
| bandwidth restrictions | Yes | Yes | Yes | Yes | Yes |
| packet size (MTU) | Yes | Yes | Yes | Yes | No |
| data size (MSS) | Yes | Yes | Yes | Yes | No |
| traffic prioritization | Yes | Yes | Yes | Yes | No |
| DHCP | | | | | |
| DHCP server | Yes | Yes | Yes | No | No |
| DHCP relay | Yes | Yes | Yes | No | No |
| Ping Check | Yes | Yes | Yes | Yes | No |

* - The format of interface names is strict. Each name consists of 2-4 letters (interface type), followed by a number (*x*, limited by the maximum number of each type of interface). For example, Ethernet interface names are ge1, ge2, ge3, ...; VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.

** - The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface ge1 are called ge1:1, ge1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the web configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual Interface Parameters

**Table 22** Ethernet, VLAN, Bridge, PPP, and Virtual Interface Characteristics (ZyWALL / USG USG 200 and Below Models)

| CHARACTERISTICS | ETHERNET | ETHERNET | ETHERNET | VLAN | BRIDGE | PPP | VIRTUAL |
|---|---|---|---|---|---|---|---|
| Name* | opt | wan1, wan2 | lan1, ext-wlan, dmz | vlan*x* | br*x* | ppp*x* | ** |
| Configurable Zone | Yes | No | No | Yes | Yes | No | No |
| IP Address Assignment | | | | | | | |
| Static IP address | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| DHCP client | Yes | Yes | No | Yes | Yes | Yes | No |
| Routing metric | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Interface Parameters | | | | | | | |
| Bandwidth restrictions | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

**Table 22** Ethernet, VLAN, Bridge, PPP, and Virtual Interface Characteristics (ZyWALL / USG USG 200 and Below Models) (continued)

| CHARACTERISTICS | ETHERNET | ETHERNET | ETHERNET | VLAN | BRIDGE | PPP | VIRTUAL |
|---|---|---|---|---|---|---|---|
| Packet size (MTU) | Yes | Yes | Yes | Yes | Yes | Yes | No |
| Data size (MSS) | Yes | Yes | Yes | Yes | Yes | Yes | No |
| DHCP | | | | | | | |
| DHCP server | Yes | No | Yes | Yes | Yes | No | No |
| DHCP relay | Yes | No | Yes | Yes | Yes | No | No |
| Connectivity Check | Yes | Yes | No | Yes | Yes | Yes | No |

* - Each name consists of 2-4 letters (interface type), followed by a number (*x*). For most interfaces, x is limited by the maximum number of the type of interface. For VLAN interfaces, x is defined by the number you enter in the VLAN name field. For example, Ethernet interface names are wan1, wan2, opt, lan1, ext-wlan, dmz; VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.

** - The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface wan1 are called wan1:1, wan1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the web configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual interface.

**Table 23** Cellular and WLAN Interface Characteristics

| CHARACTERISTICS | CELLULAR | WLAN |
|---|---|---|
| Name* | cellular*x* | wlan-*x*-*x* |
| Configurable Zone | Yes** | Yes |
| IP Address Assignment | | |
| Static IP address | Yes | Yes |
| DHCP client | Yes | No |
| Routing metric | Yes | No |
| Interface Parameters | | |
| Bandwidth restrictions | Yes | Yes |
| Packet size (MTU) | Yes | Yes |
| Data size (MSS) | Yes | Yes |
| DHCP | | |
| DHCP server | No | Yes |
| DHCP relay | No | Yes |
| Connectivity Check | Yes | No |

* - Each name consists of letters (interface type), followed by a number (*x*). For most interfaces, x is limited by the maximum number of the type of interface. For WLAN interfaces, the first number identifies the slot and the second number identifies the individual interface.

** - Cellular interfaces can be added to the WAN zone or no zone.

## 8.1.2 Relationships Between Interfaces

In the ZyWALL / USG, interfaces are usually created on top of other interfaces. Only Ethernet interfaces are created directly on top of the physical ports (or port groups). The relationships between interfaces are explained in the following table.

**Table 24** Relationships Between Different Types of Interfaces

| INTERFACE | REQUIRED PORT / INTERFACE |
|---|---|
| **auxiliary interface** | auxiliary port |
| ~~**port group**~~ | ~~physical port~~ |
| **Ethernet interface** | physical port<br>port group |
| **VLAN interface** | Ethernet interface |
| **bridge interface** | Ethernet interface*<br>WLAN interface*<br>VLAN interface* |
| **PPPoE/PPTP interface** (ZyWALL / USG USG 300 and above) | Ethernet interface*<br>VLAN interface*<br>bridge interface |
| **PPPoE/PPTP interface** (ZyWALL / USG USG 200 and below models) | WAN1, WAN2, OPT* |
| **virtual interface**<br>(virtual Ethernet interface)<br>(virtual VLAN interface)<br>(virtual bridge interface) | <br>Ethernet interface*<br>VLAN interface*<br>bridge interface |
| trunk | Ethernet interface<br>Cellular interface<br>VLAN interface<br>bridge interface<br>PPPoE/PPTP interface<br>auxiliary interface |

* - You cannot set up a PPPoE/PPTP interface, virtual Ethernet interface, or virtual VLAN interface if the underlying interface is a member of a bridge. You also cannot add an Ethernet interface or VLAN interface to a bridge if the member interface has a virtual interface or PPPoE/PPTP interface on top of it.

# 8.2 Interface General Commands Summary

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 25** Input Values for General Interface Commands

| LABEL | DESCRIPTION |
|---|---|
| *interface_name* | The name of the interface.<br>Ethernet interface: For the ZyWALL / USG USG 300 and above, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model.<br>ZyWALL / USG USG 200 and below models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.<br>virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4<br>VLAN interface: vlan*x*, *x* = 0 - 4094<br>virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 4<br>bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ZyWALL / USG model supports.<br>virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4<br>PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL / USG model supports. |
| *profile_name* | The name of the DHCP pool. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *domain_name* | Fully-qualified domain name. You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period. |

The following sections introduce commands that are supported by several types of interfaces. See Section 8.6 on page 94 for the unique commands for each type of interface.

## 8.2.1 Basic Interface Properties and IP Address Commands

This table lists basic properties and IP address commands.

**Table 26** interface General Commands: Basic Properties and IP Address Assignment

| COMMAND | DESCRIPTION |
|---|---|
| `show interface {ethernet \| vlan \| bridge \| ppp \| auxiliary} status` | Displays the connection status of the specified type of interfaces. |
| `show interface {`*`interface_name`*` \| ethernet \| vlan \| bridge \| ppp \| virtual ethernet \| virtual vlan \| virtual bridge \| auxiliary \| all}` | Displays information about the specified interface, specified type of interfaces, or all interfaces. See Section 8.6.1 on page 97 for all possible cellular status description. |
| `show ipv6 interface {`*`interface_name`*` \| all}` | Displays information about the specified IPv6 interface or all IPv6 interfaces. |
| `show ipv6 static address `*`interface`* | Displays the static IPv6 addresses configured on the specified IPv6 interface. |
| `show ipv6 nd ra status `*`config_interface`* | Displays the specified IPv6 interface's IPv6 router advertisement configuration. |

**Table 26** interface General Commands: Basic Properties and IP Address Assignment (continued)

| COMMAND | DESCRIPTION |
|---|---|
| show interface send statistics interval | Displays the interval for how often the ZyWALL / USG refreshes the sent packet statistics for the interfaces. |
| show interface summary all | Displays basic information about the interfaces. |
| show interface summary all status | Displays the connection status of the interfaces. |
| [no] interface *interface_name* | Creates the specified interface if necessary and enters sub-command mode. The no command deletes the specified interface. |
| [no] description *description* | Specifies the description for the specified interface. The no command clears the description.<br>*description*: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long. |
| [no] downstream <0..1048576> | This is reserved for future use.<br>Specifies the downstream bandwidth for the specified interface. The no command sets the downstream bandwidth to 1048576. |
| exit | Leaves the sub-command mode. |
| [no] ip address dhcp | Makes the specified interface a DHCP client; the DHCP server gives the specified interface its IP address, subnet mask, and gateway. The no command makes the IP address static IP address for the specified interface. (See the next command to set this IP address.) |
| [no] ip address *ip subnet_mask* | Assigns the specified IP address and subnet mask to the specified interface. The no command clears the IP address and the subnet mask. |
| [no] ip gateway *ip* | Adds the specified gateway using the specified interface. The no command removes the gateway. |
| ip gateway *ip* metric <0..15> | Sets the priority (relative to every gateway on every interface) for the specified gateway. The lower the number, the higher the priority. |
| [no] metric <0..15> | Sets the tunnel, PPPoE/PPTP, or cellular interface's priority relative to other interfaces. The lower the number, the higher the priority. |
| [no] mss <536..1460> | Specifies the maximum segment size (MSS) the interface is to use. MSS is the largest amount of data, specified in bytes, that the interface can handle in a single, unfragmented piece. The no command has the interface use its default MSS. |
| [no] mtu <576..1500> | Specifies the Maximum Transmission Unit, which is the maximum number of bytes in each packet moving through this interface. The ZyWALL / USG divides larger packets into smaller fragments. The no command resets the MTU to 1500. |
| [no] shutdown | Deactivates the specified interface. The no command activates it. |
| traffic-prioritize {tcp-ack\|content-filter\|dns\|ipsec-vpn\|ssl-vpn} bandwidth <0..1048576> priority <1..7> [maximize-bandwidth-usage]; | Applies traffic priority when the interface sends TCP-ACK traffic, traffic for querying the content filter, traffic for resolving domain names, or encrypted traffic for an IPSec or SSL VPN tunnel. It also sets how much bandwidth the traffic can use and can turn on maximize bandwidth usage. |
| traffic-prioritize {tcp-ack\|content-filter\|dns\|ipsec-vpn\|ssl-vpn} deactivate | Turns off traffic priority settings for when the interface sends the specified type of traffic. |
| [no] upstream <0..1048576> | Specifies the upstream bandwidth for the specified interface. The no command sets the upstream bandwidth to 1048576. |
| interface *interface_name* ipv6 | Creates the specified IPv6 interface if necessary and enters sub-command mode. |
| address *ipv6_addr_prefix* | Sets an IPv6 address with prefix for the interface. |
| gateway *ipv6_addr* metric <0..15> | Sets the specified IPv6 address's metric. |

**Table 26** interface General Commands: Basic Properties and IP Address Assignment (continued)

| COMMAND | DESCRIPTION |
|---|---|
| show interface send statistics interval | Displays the interval for how often the ZyWALL / USG refreshes the sent packet statistics for the interfaces. |
| show interface summary all | Displays basic information about the interfaces. |
| show interface summary all status | Displays the connection status of the interfaces. |
| [no] interface *interface_name* | Creates the specified interface if necessary and enters sub-command mode. The no command deletes the specified interface. |
| [no] description *description* | Specifies the description for the specified interface. The no command clears the description.<br>*description*: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long. |
| [no] downstream <0..1048576> | This is reserved for future use.<br>Specifies the downstream bandwidth for the specified interface. The no command sets the downstream bandwidth to 1048576. |
| exit | Leaves the sub-command mode. |
| [no] ip address dhcp | Makes the specified interface a DHCP client; the DHCP server gives the specified interface its IP address, subnet mask, and gateway. The no command makes the IP address static IP address for the specified interface. (See the next command to set this IP address.) |
| [no] ip address *ip subnet_mask* | Assigns the specified IP address and subnet mask to the specified interface. The no command clears the IP address and the subnet mask. |
| [no] ip gateway *ip* | Adds the specified gateway using the specified interface. The no command removes the gateway. |
| ip gateway *ip* metric <0..15> | Sets the priority (relative to every gateway on every interface) for the specified gateway. The lower the number, the higher the priority. |
| [no] metric <0..15> | Sets the tunnel, PPPoE/PPTP, or cellular interface's priority relative to other interfaces. The lower the number, the higher the priority. |
| [no] mss <536..1460> | Specifies the maximum segment size (MSS) the interface is to use. MSS is the largest amount of data, specified in bytes, that the interface can handle in a single, unfragmented piece. The no command has the interface use its default MSS. |
| [no] mtu <576..1500> | Specifies the Maximum Transmission Unit, which is the maximum number of bytes in each packet moving through this interface. The ZyWALL / USG divides larger packets into smaller fragments. The no command resets the MTU to 1500. |
| [no] shutdown | Deactivates the specified interface. The no command activates it. |
| traffic-prioritize {tcp-ack\|content-filter\|dns\|ipsec-vpn\|ssl-vpn} bandwidth <0..1048576> priority <1..7> [maximize-bandwidth-usage]; | Applies traffic priority when the interface sends TCP-ACK traffic, traffic for querying the content filter, traffic for resolving domain names, or encrypted traffic for an IPSec or SSL VPN tunnel. It also sets how much bandwidth the traffic can use and can turn on maximize bandwidth usage. |
| traffic-prioritize {tcp-ack\|content-filter\|dns\|ipsec-vpn\|ssl-vpn} deactivate | Turns off traffic priority settings for when the interface sends the specified type of traffic. |
| [no] upstream <0..1048576> | Specifies the upstream bandwidth for the specified interface. The no command sets the upstream bandwidth to 1048576. |
| interface *interface_name* ipv6 | Creates the specified IPv6 interface if necessary and enters sub-command mode. |
| address *ipv6_addr_prefix* | Sets an IPv6 address with prefix for the interface. |
| gateway *ipv6_addr* metric <0..15> | Sets the specified IPv6 address's metric. |

**Table 26** interface General Commands: Basic Properties and IP Address Assignment (continued)

| COMMAND | DESCRIPTION |
|---|---|
| enable | Turns on the IPv6 interface. |
| nd ra accept | Sets the IPv6 interface to accept IPv6 neighbor discovery router advertisement messages. |
| nd ra advertise | Sets the IPv6 interface to send IPv6 neighbor discovery router advertisement messages. |
| nd ra managed-config-flag | Turns on the flag in IPv6 router advertisements that tells hosts to use managed (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration. |
| nd ra other-config-flag | Turns on the other stateful configuration flag in IPv6 router advertisements that tells hosts to use administered (stateful) protocol to obtain autoconfiguration information other than addresses. |
| nd ra mtu <1280..1500> \| <0> | Sets the Maximum Transmission Unit (MTU) size of IPv6 packets sent on the interface. |
| nd ra hop-limit <0..255> | Sets the maximum number of hops for router advertisements and all IPv6 packets originating from the interface. |
| nd ra router-preference { low \| medium \| high } | Sets the Default Router Preference (DRP) extension metric (low, medium, or high) in the interface's IPv6 neighbor discovery router advertisement messages. |
| nd ra prefix-advertisement *ipv6_addr_prefix* [ auto { on \| off } ] [ link{ on \| off } ] [ preferred-time { <0..4294967294> \| infinity }] [valid-time{ <0..4294967294> \| infinity }] | Sets the IPv6 prefix that the ZyWALL / USG advertises to its clients, whether or not to advertise it, and how long before the prefix's preference and lifetime expire. |
| nd ra min-rtr-interval <3..1350> | Sets the minimum IPv6 router advertisement transmission interval. |
| nd ra max-rtr-interval <4..1800> | Sets the maximum IPv6 router advertisement transmission interval. |
| nd ra reachable-time <0..3600000> | Sets the amount of time a remote IPv6 node is considered reachable after a reachability confirmation event. |
| nd ra default-lifetime <4..9000> | Sets the router lifetime value is included in all IPv6 router advertisements sent out the interface. The router lifetime value should be equal to or greater than the router advertisement interval. |
| nd ra retrans-timer <0..4294967295> | Sets the IPv6 router advertisement retransmission interval in milliseconds. |
| ipv6 address *dhcp6_profile* *dhcp6_suffix_128* | Has the ZyWALL / USG obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ.<br>*dhcp6_profile*: Specify the DHCPv6 request object to use.<br>*dhcp6_suffix_128*: Specify the ending part of the IPv6 address, a slash (/), and the prefix length. The ZyWALL / USG appends it to the delegated prefix.<br>For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 for the *dhcp6_suffix_128*. |

**Table 26** interface General Commands: Basic Properties and IP Address Assignment (continued)

| COMMAND | DESCRIPTION |
|---|---|
| nd ra prefix-advertisement *dhcp6_profile dhcp6_suffix_64* | Configures the network prefix to use a delegated prefix as the beginning part of the network prefix.<br><br>*dhcp6_profile*: Specify the DHCPv6 request object to use for generating the network prefix for the network.<br><br>*dhcp6_suffix_64*: Specify the ending part of the IPv6 network address plus a slash (/) and the prefix length. The ~~ZyWALL~~ZyWALL / USG appends it to the selected delegated prefix. The combined address is the network prefix for the network.<br><br>For example, you got a delegated prefix of 2003:1234:5678/48. You want to divide it into 2003:1234:5678:1111/64 for this interface and 2003:1234:5678:2222/64 for another interface. You can use ::1111/64 and ::2222/64 for the suffix address respectively. But if you do not want to divide the delegated prefix into subnetworks, enter ::0/48 here, which keeps the same prefix length (/48) as the delegated prefix. |
| dhcp6 { server \| client \| relay upper { *config_interface* \| *ipv6_addr* } } | Sets the IPv6 interface to be a DHCPv6 server, client or relay. For relay, specify an interface from which to get the DHCPv6 server's address or the IPv6 address of a DHCPv6 server. |
| dhcp6 rapid-commit | This shortens the DHCPv6 message exchange process from four to two steps to help reduce network traffic.<br><br>Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work. |
| dhcp6 address-request | Get this interface's IPv6 address from the DHCPv6 server. |
| dhcp6 refresh-time { <600..4294967294> \| infinity } | Sets the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6. |
| dhcp6 duid { *duid* \| mac } | Specify the DHCP Unique IDentifier (DUID) of the interface or have it generated from the interface's default MAC address. |
| dhcp6-lease-object *dhcp6_profile* | For a DHCPv6 server interface, specify the profile of DHCPv6 lease settings to offer to DHCPv6 clients. |
| dhcp6-request-object *dhcp6_profile* | For a DHCPv6 client interface, specify the profile of DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. |
| interface *interface_name* no ipv6 | Enters the sub-command mode for deleting the specified IPv6 address or removing it's settings. |
| enable | Turns off the IPv6 interface. |
| address *ipv6_addr_prefix* | Removes the IPv6 interface's IPv6 prefix setting. |
| gateway | Removes the IPv6 interface's gateway setting. |
| nd ra accept | Sets the IPv6 interface to discard IPv6 neighbor discovery router advertisement messages. |
| nd ra advertise | Has the IPv6 interface not send IPv6 neighbor discovery router advertisement messages. |
| nd ra managed-config-flag | Turns off the flag in IPv6 router advertisements that tells hosts to use managed (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration. |
| nd ra other-config-flag | Turns off the other stateful configuration flag in IPv6 router advertisements that tells hosts to use administered (stateful) protocol to obtain autoconfiguration information other than addresses. |
| nd ra mtu | Removes the Maximum Transmission Unit (MTU) size setting for IPv6 packets the interface sends. |

**Table 26** interface General Commands: Basic Properties and IP Address Assignment (continued)

| COMMAND | DESCRIPTION |
|---|---|
| nd ra hop-limit | Removes the maximum number of hops setting for router advertisements and all IPv6 packets originating from the interface. |
| nd ra min-rtr-interval | Removes the minimum IPv6 router advertisement transmission interval setting. |
| nd ra max-rtr-interval | Removes the maximum IPv6 router advertisement transmission interval setting. |
| nd ra reachable-time | Sets the amount of time a remote IPv6 node is considered reachable after a reachability confirmation event to the default. |
| nd ra default-lifetime | Sets the router lifetime value included in all IPv6 router advertisements the interface sends to the default. The router lifetime value should be equal to or greater than the router advertisement interval. |
| nd ra retrans-timer | Sets the IPv6 router advertisement retransmission interval to the default. |
| ipv6 address *dhcp6_profile dhcp6_suffix_128* | Removes the specified setting for having the ZyWALL / USG obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network. |
| nd ra prefix-advertisement DHCP6_PROFILE DHCP6_SUFFIX_64 | Removes the specified setting for using a delegated prefix as the beginning part of the network prefix. |
| dhcp6 | Sets the interface's DHCPv6 setting back to the default. |
| dhcp6 address-request | Has the ZyWALL / USG not get this interface's IPv6 address from the DHCPv6 server. |
| dhcp6 rapid-commit | Has the ZyWALL / USG use the full four-step DHCPv6 message exchange process.<br><br>Note: Make sure you also disable this option in the DHCPv6 clients. |
| dhcp6-lease-object *dhcp6_profile* | Removes the specified profile of DHCPv6 lease settings to offer to DHCPv6 clients. |
| dhcp6-request-object *dhcp6_profile* | Removes the specified profile of DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. |
| interface reset {*interface_name*\|*virtual_interface_name*\|all} | Resets the interface statistics TxPkts (transmitted packets) and RxPkts (received packets) counts to 0. You can use the show interface summary all status command to see the interface statistics. |
| interface send statistics interval <15..3600> | Sets how often the ZyWALL / USG sends interface statistics to external servers. For example, syslog server and Vantage Report server. |
| show interface-name | Displays all PPP and Ethernet interface system name and user-defined name mappings. |
| interface-name {*ppp_interface* \| *ethernet_interface*} *user_defined_name* | Specifies a name for a PPP or an Ethernet interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.<br><br>*ppp_interface* \| *ethernet_interface*: This must be the system name of a PPP or an Ethernet interface. Use the show interface-name command to see the system name of interfaces.<br><br>*user_defined_name*:<br>• This name cannot be one of the follows:<br>"ethernet", "ppp", "vlan", "bridge", "virtual", "wlan", "cellular", "aux", "tunnel", "status", "summary", "all"<br>• This name cannot begin with one of the follows either:<br>"ge", "ppp", "vlan", "wlan-", "br", "cellular", "aux", "tunnel". |
| interface-rename *old_user_defined_name new_user_defined_name* | Modifies the user-defined name of a PPP or an Ethernet interface. |

### 8.2.1.1 Basic Interface Properties Command Examples

The following commands make Ethernet interface ge1 a DHCP client.

```
Router# configure terminal
Router(config)# interface ge1
Router(config-if)# ip address dhcp
Router(config-if)# exit
```

This example shows how to modify the name of interface ge4 to “VIP”. First you have to check the interface system name (ge4 in this example) on the ZyWALL / USG. Then change the name and display the result.

```
Router> show interface-name
No.  System Name     User Defined Name
================================================================================
1    ge1             ge1
2    ge2             ge2
3    ge3             ge3
4    ge4             ge4
5    ge5             ge5
Router> configure terminal
Router(config)# interface-name ge4 VIP
Router(config)# show interface-name
No.  System Name     User Defined Name
================================================================================
1    ge1             ge1
2    ge2             ge2
3    ge3             ge3
4    ge4             VIP
5    ge5             ge5
Router(config)#
```

This example shows how to change the user defined name from VIP to Partner. Note that you have to use the “interface-rename” command if you do not know the system name of the interface. To use the “interface-name” command, you have to find out the corresponding system name first (ge4 in this example). This example also shows how to change the user defined name from Partner to Customer using the “interface-name” command.

```
Router(config)# interface-rename VIP Partner
Router(config)# show interface-name
No.  System Name     User Defined Name
================================================================================
1    ge1             ge1
2    ge2             ge2
3    ge3             ge3
4    ge4             Partner
5    ge5             ge5
Router(config)#
Router(config)# interface-name ge4 Customer
Router(config)# show interface-name
No.  System Name     User Defined Name
================================================================================
1    ge1             ge1
2    ge2             ge2
3    ge3             ge3
4    ge4             Customer
5    ge5             ge5
```

This example shows how to restart an interface. You can check all interface names on the ZyWALL / USG. Then use either the system name or user-defined name of an interface (ge4 or Customer in this example) to restart it.

```
Router> show interface-name
No.  System Name     User Defined Name
================================================================================
1    ge1             ge1
2    ge2             ge2
3    ge3             ge3
4    ge4             Customer
5    ge5             ge5
Router> configure terminal
Router(config)# interface reset ge4
Router(config)# interface reset Customer
Router(config)#
```

## 8.2.2 IGMP Proxy Commands

Internet Group Management Protocol (IGMP) proxy is used for multicast routing. IGMP proxy enables the ZyWALL / USG to issue IGMP host messages on behalf of hosts that the ZyWALL / USG discovered on its IGMP-enabled interfaces. The ZyWALL / USG acts as a proxy for its hosts.

Enter configuration terminal mode and select an interface

**Table 27** interface Commands: IGMP Proxy Commands

| COMMAND | DESCRIPTION |
|---|---|
| [no] igmp activate | Enables IGMP proxy on this interface.<br><br>The no command disables IGMP proxy on this interface. |
| igmp direction | Setes the direction for IGMP proxy on this interface.<br><br>• downstream - enable on the interface which connects to the multicast hosts.<br>• upstream - enable on the interface which connects to a router running IGMP that is closer to the multicast server |
| igmp version <1..3> | Sets the IGMP version to be used on this ZyWALL / USG interface.. |

#### 8.2.2.1 IGMP Command Example

The following commands activate IGMP version 2 upstream on the lan1 interface.

```
Router> enable
Router#
Router# configure terminal
Router(config)# interface lan1
Router(config-if-lan1)# igmp
activate
direction
version
Router(config-if-lan1)# igmp activate
Router(config-if-lan1)# igmp direction
downstream
upstream
Router(config-if-lan1)# igmp direction upstream
Router(config-if-lan1)# igmp version
<1..3>
Router(config-if-lan1)# igmp version 2
Router(config-if-lan1)#

Router(config-if-lan1)# exit
```

### 8.2.3 DHCP Setting Commands

This table lists DHCP setting commands. DHCP is based on DHCP pools. Create a DHCP pool if you want to assign a static IP address to a MAC address or if you want to specify the starting IP address and pool size of a range of IP addresses that can be assigned to DHCP clients. There are different commands for each configuration. Afterwards, in either case, you have to bind the DHCP pool to the interface.

**Table 28** interface Commands: DHCP Settings

| COMMAND | DESCRIPTION |
|---|---|
| `show ip dhcp dhcp-options` | Shows the DHCP extended option settings. |
| `show ip dhcp pool [profile_name]` | Shows information about the specified DHCP pool or about all DHCP pools. |
| `show ip dhcp pool profile_name dhcp-options` | Shows the specified DHCP pool's DHCP extended option settings. |
| `ip dhcp pool rename profile_name profile_name` | Renames the specified DHCP pool from the first *profile_name* to the second *profile_name*. |
| `[no] ip dhcp pool profile_name` | Creates a DHCP pool if necessary and enters sub-command mode. You can use the DHCP pool to create a static entry or to set up a range of IP addresses to assign dynamically.<br>About the sub-command settings:<br>• If you use the `host` command, the ZyWALL / USG treats this DHCP pool as a static DHCP entry.<br>• If you do not use the `host` command and use the `network` command, the ZyWALL / USG treats this DHCP pool as a pool of IP addresses.<br>• If you do not use the `host` command or the `network` command, the DHCP pool is not properly configured and cannot be bound to any interface.<br>The `no` command removes the specified DHCP pool. |
| `show` | Shows information about the specified DHCP pool. |

**Table 28** interface Commands: DHCP Settings (continued)

| COMMAND | DESCRIPTION |
|---|---|
| | Use the following commands to create a static DHCP entry. If you do not use the host command, the commands that are not in this section have no effect, but you can still set them. |
| [no] host *ip* | Specifies the static IP address the ZyWALL / USG should assign. Use this command, along with hardware-address, to create a static DHCP entry.<br><br>Note: The IP address must be in the same subnet as the interface to which you plan to bind the DHCP pool.<br><br>When this command is used, the ZyWALL / USG treats this DHCP pool like a static entry, regardless of the network setting. The no command clears this field. |
| [no] hardware-address *mac_address* | Reserves the DHCP pool for the specified MAC address. Use this command, along with host, to create a static DHCP entry. The no command clears this field. |
| [no] client-identifier *mac_address* | Specifies the MAC address that appears in the DHCP client list. The no command clears this field. |
| [no] client-name *host_name* | Specifies the host name that appears in the DHCP client list. The no command clears this field.<br><br>*host_name*: You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| | Use the following commands to create a pool of IP addresses. These commands have no effect if you use the host command. You can still set them, however. |
| dhcp-option <1..254> *option_name* {boolean <0..1>\| uint8 <0..255> \| uint16 <0..65535> \| uint32 <0..4294967295> \| ip *ipv4* [ *ipv4* [ *ipv4*]] \| fqdn *fqdn* [ *fqdn* [ *fqdn*]] \| text *text* \| hex *hex* \| vivc *enterprise_id hex_s* [*enterprise_id hex_s* ] \| vivs *enterprise_id hex_s* [*enterprise_id hex_s* ] | Adds or edits a DHCP extended option for the specified DHCP pool.<br><br>*text*: String of up to 250 characters<br><br>*hex*: String of up to 250 hexadecimal pairs.<br><br>*vivc*: Vendor-Identifying Vendor Class option. A DHCP client may use this option to unambiguously identify the vendor that manufactured the hardware on which the client is running, the software in use, or an industry consortium to which the vendor belongs.<br><br>*enterprise_id*: Number <0..4294967295>.<br><br>*hex_s*: String of up to 120 hexadecimal pairs.<br><br>*vivs*: Vendor-Identifying Vendor-Specific option. DHCP clients and servers may use this option to exchange vendor-specific information. |
| no dhcp-option <1..254> | Removes the DHCP extended option for the specified DHCP pool. |
| network IP/<1..32><br>network *ip mask*<br>no network | Specifies the IP address and subnet mask of the specified DHCP pool. The subnet mask can be written in w.x.y.z format or in /<1..32> format.<br><br>Note: The DHCP pool must have the same subnet as the interface to which you plan to bind it.<br><br>The no command clears these fields. |
| [no] default-router *ip* | Specifies the default gateway DHCP clients should use. The no command clears this field. |
| [no] description *description* | Specifies a description for the DHCP pool for identification. The no command removes the description. |

**Table 28** interface Commands: DHCP Settings (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] domain-name *domain_name* | Specifies the domain name assigned to DHCP clients. The no command clears this field. |
| [no] starting-address *ip* pool-size <1..65535> | Sets the IP start address and maximum pool size of the specified DHCP pool. The final pool size is limited by the subnet mask.<br><br>Note: You must specify the network number first, and the start address must be in the same subnet.<br><br>The no command clears the IP start address and maximum pool size. |
| [no] first-dns-server {*ip* \| *interface_name* {1st-dns \| 2nd-dns \| 3rd-dns} \| ZyWALL} | Sets the first DNS server to the specified IP address, the specified interface's first, second, or third DNS server, or the ZyWALL / USG itself. The no command resets the setting to its default value. |
| [no] second-dns-server {*ip* \| *interface_name* {1st-dns \| 2nd-dns \| 3rd-dns} \| ZyWALL} | Sets the second DNS server to the specified IP address, the specified interface's first, second, or third DNS server, or the ZyWALL / USG itself. The no command resets the setting to its default value. |
| [no] third-dns-server {*ip* \| *interface_name* {1st-dns \| 2nd-dns \| 3rd-dns} \| ZyWALL} | Sets the third DNS server to the specified IP address, the specified interface's first, second, or third DNS server, or the ZyWALL / USG itself. The no command resets the setting to its default value. |
| [no] first-wins-server *ip* | Specifies the first WINS server IP address to assign to the remote users. The no command removes the setting. |
| [no] second-wins-server *ip* | Specifies the second WINS server IP address to assign to the remote users. The no command removes the setting. |
| [no] lease {<0..365> [<0..23> [<0..59>]] \| infinite} | Sets the lease time to the specified number of days, hours, and minutes or makes the lease time infinite. The no command resets the first DNS server setting to its default value. |
| interface *interface_name* | Enters sub-command mode. |
| [no] ip dhcp-pool *profile_name* | Binds the specified interface to the specified DHCP pool. You have to remove any DHCP relays first. The no command removes the binding. |
| [no] ip helper-address *ip* | Creates the specified DHCP relay. You have to remove the DHCP pool first, if the DHCP pool is bound to the specified interface. The no command removes the specified DHCP relay. |
| release dhcp *interface-name* | Releases the TCP/IP configuration of the specified interface. The interface must be a DHCP client. This command is available in privilege mode, not configuration mode. |
| renew dhcp *interface-name* | Renews the TCP/IP configuration of the specified interface. The interface must be a DHCP client. This command is available in privilege mode, not configuration mode. |
| show ip dhcp binding [*ip*] | Displays information about DHCP bindings for the specified IP address or for all IP addresses. |
| clear ip dhcp binding {*ip* \| *} | Removes the DHCP bindings for the specified IP address or for all IP addresses. |

### 8.2.3.1 DHCP Setting Command Examples

The following example uses these commands to configure DHCP pool DHCP_TEST.

```
Router# configure terminal
Router(config)# ip dhcp pool DHCP_TEST
Router(config-ip-dhcp-pool)#  network 192.168.1.0 /24
Router(config-ip-dhcp-pool)#  domain-name zyxel.com
Router(config-ip-dhcp-pool)#  first-dns-server 10.1.5.1
Router(config-ip-dhcp-pool)#  second-dns-server ge1 1st-dns
Router(config-ip-dhcp-pool)#  third-dns-server 10.1.5.2
Router(config-ip-dhcp-pool)#  default-router 192.168.1.1
Router(config-ip-dhcp-pool)#  lease 0 1 30
Router(config-ip-dhcp-pool)#  starting-address 192.168.1.10 pool-size 30
Router(config-ip-dhcp-pool)#  hardware-address 00:0F:20:74:B8:18
Router(config-ip-dhcp-pool)#  client-identifier 00:0F:20:74:B8:18
Router(config-ip-dhcp-pool)#  client-name TWtester1
Router(config-ip-dhcp-pool)# exit
Router(config)#  interface ge1
Router(config-if)# ip dhcp-pool DHCP_TEST
Router(config-if)# exit
Router(config)# show ip dhcp server status
binding interface : ge1
  binding pool    : DHCP_TEST
```

### 8.2.3.2 DHCP Extended Option Setting Command Example

The following example configures the DHCP_TEST pool with a SIP server (code 120) extended DHCP option with one IP address to provide to the SIP clients.

```
Router# configure terminal
Router(config)# ip dhcp pool DHCP_TEST
Router(config-ip-dhcp-pool)#  dhcp-option 120 sip ip 192.168.1.20
Router(config-ip-dhcp-pool)# exit
```

## 8.2.4 Interface Parameter Command Examples

This table shows an example of each interface type's sub-commands. The sub-commands vary for different interface types.

**Table 29** Examples for Different Interface Parameters

| ETHERNET | VIRTUAL INTERFACE | PPPOE/PPTP |
|---|---|---|
| Router(config)# interface wan1<br>Router(config-if-wan1)#<br>description<br>downstream<br>exit<br>ip<br>ipv6<br>mac<br>mss<br>mtu<br>no<br>ping-check<br>shutdown<br>traffic-prioritize<br>type<br>upstream<br>use-defined-mac | Router(config)# interface wan1:1<br>Router(config-if-vir)#<br>description<br>downstream<br>exit<br>ip<br>no<br>shutdown<br>upstream | Router(config)# interface wan1_ppp<br>Router(config-if-ppp)#<br>account<br>bind<br>connectivity<br>description<br>downstream<br>exit<br>ipv6<br>local-address<br>metric<br>mss<br>mtu<br>no<br>ping-check<br>remote-address<br>shutdown<br>traffic-prioritize<br>upstream |
| **CELLULAR** | **WLAN** | **VLAN** |
| Router(config)# interface cellular1<br>Router(config-if-cellular)#<br>account<br>band<br>budget<br>connectivity<br>description<br>device<br>downstream<br>encrypted-pin<br>exit<br>local-address<br>metric<br>mtu<br>network-selection<br>no<br>pin<br>ping-check<br>remote-address<br>shutdown<br>traffic-prioritize<br>upstream | Router(config)# interface wlan-1-1<br>Router(config-if-wlan)#<br>block-intra<br>description<br>downstream<br>encrypted-wep-key<br>exit<br>group-key<br>hide<br>idle<br>ip<br>mtu<br>no<br>ping-check<br>reauth<br>security<br>shutdown<br>ssid<br>station-limit<br>traffic-prioritize<br>upstream<br>wep-key | Router(config)# interface vlan1<br>Router(config-if-vlan)#<br>description<br>downstream<br>exit<br>ip<br>ipv6<br>mss<br>mtu<br>no<br>ping-check<br>port<br>shutdown<br>traffic-prioritize<br>type<br>upstream<br>vlan-id |

**Table 29** Examples for Different Interface Parameters

| BRIDGE | ~~AUXILIARY~~ | TUNNEL |
|---|---|---|
| Router(config)# interface br0<br>Router(config-if-brg)#<br>description<br>downstream<br>exit<br>ip<br>ipv6<br>join<br>mss<br>mtu<br>no<br>ping-check<br>shutdown<br>traffic-prioritize<br>type<br>upstream | ~~Router(config)# interface aux~~<br>~~Router(config-if-aux)#~~<br>~~authentication~~<br>~~description~~<br>~~dial-timeout~~<br>~~dialing-type~~<br>~~encrypted-password~~<br>~~exit~~<br>~~idle~~<br>~~initial-string~~<br>~~no~~<br>~~password~~<br>~~phone-number~~<br>~~port-speed~~<br>~~shutdown~~<br>~~traffic-prioritize~~<br>~~username~~ | downstream<br>exit<br>ip<br>ipv6<br>metric<br>mtu<br>no<br>ping-check<br>shutdown<br>traffic-prioritize<br>tunnel<br>upstream |

## 8.2.5 RIP Commands

This table lists the commands for RIP settings.

**Table 30** interface Commands: RIP Settings

| COMMAND | DESCRIPTION |
|---|---|
| `router rip` | Enters sub-command mode. |
| `[no] network` *`interface_name`* | Enables RIP for the specified interface. The `no` command disables RIP for the specified interface. |
| `[no] passive-interface` *`interface_name`* | Sets the RIP direction of the specified interface to in-only. The `no` command makes RIP bi-directional in the specified interface. |
| `[no] outonly-interface` *`interface_name`* | Sets the RIP direction of the specified interface to out-only. The `no` command makes RIP bi-directional in the specified interface. |
| `interface` *`interface_name`* | Enters sub-command mode. |
| `[no] ip rip {send \| receive} version <1..2>` | Sets the send or receive version to the specified version number. The `no` command sets the send or received version to the current global setting for RIP. See Chapter 11 on page 129 for more information about routing protocols. |
| `[no] ip rip v2-broadcast` | Enables RIP-2 packets using subnet broadcasting. The `no` command uses multi-casting. |
| `show rip {global \| interface {all \|` *`interface_name`*`}}` | Displays RIP settings. |

## 8.2.6 OSPF Commands

This table lists the commands for OSPF settings.

**Table 31** interface Commands: OSPF Settings

| COMMAND | DESCRIPTION |
|---|---|
| `router ospf` | Enters sub-command mode. |
| `[no] network` *`interface_name`* `area` *`ip`* | Makes the specified interface part of the specified area. The `no` command removes the specified interface from the specified area, disabling OSPF in this interface. |

**Table 31** interface Commands: OSPF Settings (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] passive-interface *interface_name* | Sets the OSPF direction of the specified interface to in-only. The no command makes OSPF bi-directional in the specified interface. |
| interface *interface_name* | Enters sub-command mode. |
| [no] ip ospf priority <0..255> | Sets the priority of the specified interface to the specified value. The no command sets the priority to 1. |
| [no] ip ospf cost <1..65535> | Sets the cost to route packets through the specified interface. The no command sets the cost to 10. |
| no ip ospf authentication | Disables authentication for OSPF in the specified interface. |
| ip ospf authentication | Enables text authentication for OSPF in the specified interface. |
| ip ospf authentication message-digest | Enables MD5 authentication for OSPF in the specified interface. |
| ip ospf authentication same-as-area | To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. This command makes OSPF authentication in the specified interface follow the settings in the corresponding area. |
| [no] ip ospf authentication-key *password* | Sets the simple text password for OSPF text authentication in the specified interface. The no command clears the text password.<br><br>*password*: 1-8 alphanumeric characters or underscores |
| ip ospf message-digest-key <1..255> md5 *password* | Sets the ID and password for OSPF MD5 authentication in the specified interface.<br><br>*password*: 1-16 alphanumeric characters or underscores |
| no ip ospf message-digest-key | Clears the ID and password for OSPF MD5 authentication in the specified interface. |
| [no] ip ospf hello-interval <1..65535> | Sets the number of seconds between “hello” messages to peer routers. These messages let peer routers know the ZyWALL / USG is available. The no command sets the number of seconds to 10. See ip ospf dead-interval for more information. |
| [no] ip ospf dead-interval <1..65535> | Sets the number of seconds the ZyWALL / USG waits for “hello” messages from peer routers before it assumes the peer router is not available and deletes associated routing information. The no command sets the number of seconds to 40. See ip ospf hello-interval for more information. |
| [no] ip ospf retransmit-interval <1..65535> | Sets the number of seconds the ZyWALL / USG waits for an acknowledgment in response to a link state advertisement before it re-sends the advertisement.<br><br>Link state advertisements (LSA) are used to share the link state and routing information between routers. |

## 8.2.7 Connectivity Check (Ping-check) Commands

Use these commands to have an interface regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL / USG stops routing to the gateway. The ZyWALL / USG resumes routing to the gateway the first time the gateway passes the connectivity check.

This table lists the `ping-check` commands

**Table 32** interface Commands: Ping Check

| COMMAND | DESCRIPTION |
|---|---|
| `show ping-check [`*interface_name* `| status]` | Displays information about ping check settings for the specified interface or for all interfaces.<br>`status`: displays the current connectivity check status for any interfaces upon which it is activated. |
| `[no] connectivity-check continuous-log activate` | Use this command to have the ZyWALL / USG logs connectivity check result continuously. The `no` command disables the setting. |
| `show connectivity-check continuous-log status` | Displays the continuous log setting about connectivity check. |
| `interface` *interface_name* | Enters sub-command mode. |
| `[no] ping-check activate` | Enables ping check for the specified interface. The `no` command disables ping check for the specified interface. |
| `ping-check {`*domain_name* `|` *ip* `| default-gateway}` | Specifies what the ZyWALL / USG pings for the ping check; you can specify a fully-qualified domain name, IP address, or the default gateway for the interface. |
| `ping-check {`*domain_name* `|` *ip* `| default-gateway} period <5..30>` | Specifies what the ZyWALL / USG pings for the ping check and sets the number of seconds between each ping check. |
| `ping-check {`*domain_name* `|` *ip* `| default-gateway} timeout <1..10>` | Specifies what the ZyWALL / USG pings for the ping check and sets the number of seconds the ZyWALL / USG waits for a response. |
| `ping-check {`*domain_name* `|` *ip* `| default-gateway} fail-tolerance <1..10>` | Specifies what the ZyWALL / USG pings for the ping check and sets the number of times the ZyWALL / USG times out before it stops routing through the specified interface. |
| `ping-check {`*domain_name* `|` *ip* `| default-gateway} method {icmp | tcp}` | Sets how the ZyWALL / USG checks the connection to the gateway.<br>`icmp`: ping the gateway you specify to make sure it is still available.<br>`tcp`: perform a TCP handshake with the gateway you specify to make sure it is still available. |
| `ping-check {`*domain_name* `|` *ip* `| default-gateway} port <1..65535>` | Specifies the port number to use for a TCP connectivity check. |

#### 8.2.7.1 Connectivity Check Command Example

The following commands show you how to set the WAN1 interface to use a TCP handshake on port 8080 to check the connection to IP address 1.1.1.2

```
Router# configure terminal
Router(config)# interface wan1
Router(config-if-wan1)# ping-check 1.1.1.2 method tcp port 8080
Router(config-if-wan1)# exit
Router(config)# show ping-check
Interface: wan1
Check Method: tcp
IP Address: 1.1.1.2
Period: 30
Timeout: 5
Fail Tolerance: 5
Activate: yes
Port: 8080
Router(config)#
```

# 8.3 Ethernet Interface Specific Commands

This section covers commands that are specific to Ethernet interfaces.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 33** Input Values for Ethernet Interface Commands

| LABEL | DESCRIPTION |
|---|---|
| *interface_name* | The name of the Ethernet interface. This depends on the ZyWALL / USG model.<br>For the ZyWALL / USG USG 300 and above, use ge*x*, *x* = 1~N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model.<br>The ZyWALL / USG USG 200 and below models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. |

## 8.3.1 MAC Address Setting Commands

This table lists the commands you can use to set the MAC address of an interface. On some ZyWALL / USG models, these commands only apply to a WAN or OPT interface.

**Table 34** interface Commands: MAC Setting

| COMMAND | DESCRIPTION |
|---|---|
| `interface` *interface_name* | Enters sub-command mode. |
| `no mac` | Has the interface use its default MAC address. |
| `mac` *mac* | Specifies the MAC address the interface is to use. |

**Table 34** interface Commands: MAC Setting (continued)

| COMMAND | DESCRIPTION |
|---|---|
| type {internal \| external \| general} | Sets which type of network you will connect this interface. The ZyWALL / USG automatically adds default route and SNAT settings for traffic it routes from internal interfaces to external interfaces; for example LAN to WAN traffic.<br>internal: Set this to connect to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The ZyWALL / USG automatically adds default SNAT settings for traffic flowing from this interface to an external interface.<br>external: Set this to connect to an external network (like the Internet). The ~~ZyWALL~~ZyWALL / USG automatically adds this interface to the default WAN trunk.<br>general: Set this if you want to manually configure a policy route to add routing and SNAT settings for the interface. |
| no use-defined-mac | Has the interface use its default MAC address. |
| use-defined-mac | Has the interface use a MAC address that you specify. |

## 8.3.2 Port Grouping Commands

This section covers commands that are specific to port grouping.

Note: In CLI, representative interfaces are also called representative ports.

**Table 35** Basic Interface Setting Commands

| COMMAND | DESCRIPTION |
|---|---|
| show port-grouping | Displays which physical ports are assigned to each representative interface. |
| port-grouping *representative_interface* port <1..*x*> | Adds the specified physical port to the specified representative interface.<br>*representative_interface*: ge*x* in a ZyWALL / USG USG 300 or above.<br>A dmz, ext-wlan, or lan1 interface in a ZyWALL / USG USG 100 or 200.<br><1..*x*> where *x* equals the highest numbered port for your ZyWALL / USG model. |
| no port <1..*x*> | Removes the specified physical port from its current representative interface and adds it to its default representative interface (for example, port *x* --> ge*x*). |
| port status Port<1..*x*> | Enters a sub-command mode to configure the specified port's settings. |
| [no] duplex <full \| half> | Sets the port's duplex mode. The no command returns the default setting. |
| exit | Leaves the sub-command mode. |
| [no] negotiation auto | Sets the port to use auto-negotiation to determine the port speed and duplex. The no command turns off auto-negotiation. |
| [no] speed <100,10> | Sets the Ethernet port's connection speed in Mbps. The no command returns the default setting. |
| show port setting | Displays the Ethernet port negotiation, duplex, and speed settings. |
| show port status | Displays statistics for the Ethernet ports. |

### 8.3.2.1 Port Grouping Command Examples

The following commands add physical port ~~5~~7 to representative interface ~~ge1~~lan2.

```
Router# configure terminal
Router(config)# show port-grouping
No. Representative Name  Port1 Port2 Port3 Port4 Port5
============================================================
1   ge1                  yes   no    no    no    no
2   ge2                  no    yes   no    no    no
3   ge3                  no    no    yes   no    no
4   ge4                  no    no    no    yes   no
5   ge5                  no    no    no    no    yesRouter(config)# show port-grouping
No. Representative Name  Port1 Port2 Port3 Port4 Port5 Port6 Port7
================================================================================
1   wan1                 yes   no    no    no    no    no    no
2   wan2                 no    yes   no    no    no    no    no
3   opt                  no    no    yes   no    no    no    no
4   lan1                 no    no    no    yes   yes   yes   no
5   lan2                 no    no    no    no    no    no    no
6   reserved             no    no    no    no    no    no    no
7   dmz                  no    no    no    no    no    no    yes
Router(config)#
Router(config)# port-grouping ge1
Router(config-port-grouping)# port 5
Router(config-port-grouping)# exit
Router(config)# show port-grouping
No. Representative Name  Port1 Port2 Port3 Port4 Port5
============================================================
1   ge1                  yes   no    no    no    yes
2   ge2                  no    yes   no    no    no
3   ge3                  no    no    yes   no    no
4   ge4                  no    no    no    yes   no
5   ge5                  no    no    no    no    noRouter(config)# port-grouping lan2
Router(config-port-grouping)# port 7
Router(config-port-grouping)# exit
Router(config)# show port-grouping
No. Representative Name  Port1 Port2 Port3 Port4 Port5 Port6 Port7
================================================================================
1   wan1                 yes   no    no    no    no    no    no
2   wan2                 no    yes   no    no    no    no    no
3   opt                  no    no    yes   no    no    no    no
4   lan1                 no    no    no    yes   yes   yes   no
5   lan2                 no    no    no    no    no    no    yes
6   reserved             no    no    no    no    no    no    no
7   dmz                  no    no    no    no    no    no    no
Router(config)#
```

The following commands set port 1 to use auto-negotiation auto and port 2 to use a 10 Mbps connection speed and half duplex.

```
Router(config)# port status Port1
Router(config-port-status)# negotiation auto
Router(config-port-status)# exit
Router(config)# port status Port2
Router(config-port-status)# duplex half
Router(config-port-status)# speed 10
Router(config-port-status)# exit
Router(config)# exit
```

# 8.4 Virtual Interface Specific Commands

Virtual interfaces use many of the general interface commands discussed at the beginning of Section 8.2 on page 73. There are no additional commands for virtual interfaces.

## 8.4.1 Virtual Interface Command Examples

The following commands set up a virtual interface on top of Ethernet interface ge1. The virtual interface is named ge1:1 with the following parameters: IP 1.2.3.4, subnet 255.255.255.0, gateway 4.6.7.8, upstream bandwidth 345, downstream bandwidth 123, and description “I am vir interface”.

```
Router# configure terminal
Router(config)# interface ge1:1
Router(config-if-vir)# ip address 1.2.3.4 255.255.255.0
Router(config-if-vir)# ip gateway 4.6.7.8
Router(config-if-vir)# upstream 345
Router(config-if-vir)# downstream 123
Router(config-if-vir)# description I am vir interface
Router(config-if-vir)# exit
```

# 8.5 PPPoE/PPTP Specific Commands

This section covers commands that are specific to PPPoE/PPTP interfaces. PPPoE/PPTP interfaces also use many of the general interface commands discussed at the beginning of Section 8.2 on page 73.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 36** Input Values for PPPoE/PPTP Interface Commands

| LABEL | DESCRIPTION |
|---|---|
| *interface_name* | PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL / USG model supports. |
| *profile_name* | The name of the ISP account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |

This table lists the PPPoE/PPTP interface commands.

**Table 37** interface Commands: PPPoE/PPTP Interfaces

| COMMAND | DESCRIPTION |
|---|---|
| `interface dial` *interface_name* | Connects the specified PPPoE/PPTP interface. |
| `interface disconnect` *interface_name* | Disconnects the specified PPPoE/PPTP interface. |
| `interface` *interface_name* | Creates the specified interface if necessary and enters sub-command mode. |
| `[no] account` *profile_name* | Specifies the ISP account for the specified PPPoE/PPTP interface. The `no` command clears the ISP account field. |
| `[no] bind` *interface_name* | Specifies the base interface for the PPPoE/PPTP interface. The `no` command removes the base interface. |

**Table 37** interface Commands: PPPoE/PPTP Interfaces (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] connectivity {nail-up \| dial-on-demand} | Specifies whether the specified PPPoE/PPTP interface is always connected (nail-up) or connected only when used (dial-on-demand). The no command sets it to dial-on-demand. |
| [no] local-address *ip* | Specifies a static IP address for the specified PPPoE/PPTP interface. The no command makes the PPPoE/PPTP interface a DHCP client; the other computer assigns the IP address. |
| [no] remote-address *ip* | Specifies the IP address of the PPPoE/PPTP server. If the PPPoE/PPTP server is not available at this IP address, no connection is made. The no command lets the ZyWALL / USG get the IP address of the PPPoE/PPTP server automatically when it establishes the connection. |
| [no] mss <536..1452> | Specifies the maximum segment size (MSS) the interface can use. MSS is the largest amount of data, specified in bytes, that the interface can handle in a single, unfragmented piece. The no command has the ZyWALL / USG use its default MSS setting. |
| mtu <576..1492> | Sets the Maximum Transmission Unit in bytes. |
| [no] ipv6 enable | Turns on the IPv6 interface. The no command turns it off. |
| [no] ipv6 nd ra accept | Sets the IPv6 interface to accept IPv6 neighbor discovery router advertisement messages. The no command sets the IPv6 interface to discard IPv6 neighbor discovery router advertisement messages. |
| [no] ipv6 metric <0..15> | Sets the interface's metric for IPv6 traffic. The no command clears it. |
| [no] ipv6 address *dhcp6_profile dhcp6_suffix_128* | Has the ZyWALL / USG obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. The no command removes the specified setting for using a delegated prefix as the beginning part of the network prefix.<br>*dhcp6_profile*: Specify the DHCPv6 request object to use.<br>*dhcp6_suffix_128*: Specify the ending part of the IPv6 address, a slash (/), and the prefix length. The ZyWALL / USG appends it to the delegated prefix.<br>For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 for the *dhcp6_suffix_128*. |
| ipv6 dhcp6 [client] | Sets the IPv6 interface to be a DHCPv6 client. |
| [no] ipv6 dhcp6 rapid-commit | Shortens the DHCPv6 message exchange process from four to two steps to help reduce network traffic. The no command sets the full four-step DHCPv6 message exchange process. |
| [no] ipv6 dhcp6 address-request | Get this interface's IPv6 address from the DHCPv6 server. The no command has the ZyWALL / USG not get this interface's IPv6 address from the DHCPv6 server. |
| ipv6 dhcp6 duid { *duid* \| mac } | Specify the DHCP Unique IDentifier (DUID) of the interface or have it generated from the interface's default MAC address. |
| [no] ipv6 dhcp6-request-object *dhcp6_profile* | For a DHCPv6 client interface, specify the profile of DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. The no command removes the DHCPv6 request settings profile. |
| show interface ppp system-default | Displays system default PPP interfaces (non-deletable) that come with the ZyWALL / USG. |
| show interface ppp user-define | Displays all PPP interfaces that were manually configured on the ZyWALL / USG. |

### 8.5.1 PPPoE/PPTP Interface Command Examples

The following commands show you how to configure PPPoE/PPTP interface ppp0 with the following characteristics: base interface ge1, ISP account **Hinet**, local address 1.1.1.1, remote address 2.2.2.2, MTU 1200, upstream bandwidth 345, downstream bandwidth 123, description “I am ppp0”, and dialed only when used.

```
Router# configure terminal
Router(config)# interface ppp0
Router(config-if-ppp)# account Hinet
Router(config-if-ppp)# bind ge1
Router(config-if-ppp)# local-address 1.1.1.1
Router(config-if-ppp)# remote-address 2.2.2.2
Router(config-if-ppp)# mtu 1200
Router(config-if-ppp)# upstream 345
Router(config-if-ppp)# downstream 123
Router(config-if-ppp)# connectivity dial-on-demand
Router(config-if-ppp)# description I am ppp0
Router(config-if-ppp)# exit
```

The following commands show you how to connect and disconnect ppp0.

```
Router# interface dial ppp0
Router# interface disconnect ppp0
```

## 8.6 Cellular Interface Specific Commands

Use a 3G (Third Generation) cellular device with the ZyWALL / USG for wireless broadband Internet access.

Use these commands to add, edit, dial, disconnect, or delete cellular interfaces. When you add a new cellular interface, make sure you enter the account. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 38** Cellular Interface Commands

| COMMAND | DESCRIPTION |
|---|---|
| `[no] interface` *interface_name* | Creates the specified interface if necessary and enters sub-command mode. The `no` command deletes the specified interface. |
| `[no] account` *profile_name* | Specifies the ISP account for the specified cellular interface. The `no` command clears the ISP account field. |
| `[no] band {auto\|wcdma\|gsm}` | Sets (or clears) the cellular band that the cellular interface uses.<br>`auto` has the ZyWALL / USG always use the fastest network that is in range.<br>`gsm` has this interface only use a 2.5G or 2.75G network (respectively). If you only have a GSM network available to you, you may want to use this so the ZyWALL / USG does not spend time looking for a WCDMA network.<br>`wcdma` has this interface only use a 3G or 3.5G network (respectively). You may want to use this if you want to make sure the interface does not use the GSM network. |

**Table 38** Cellular Interface Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] network-selection {auto\|home} | Home network is the network to which you are originally subscribed.<br><br>Home has the 3G device connect only to the home network. If the home network is down, the ~~ZyWALL~~ZyWALL / USG's 3G Internet connection is also unavailable.<br><br>Auto is the default setting and allows the 3G device to connect to a network to which you are not subscribed when necessary, for example when the home network is down or another 3G base station's signal is stronger. This is recommended if you need continuous Internet connectivity. If you select this, you may be charged using the rate of a different network. |
| [no] budget active | Sets a monthly limit for the user account of the installed 3G card. You can set a limit on the total traffic and/or call time. The ZyWALL / USG takes the actions you specified when a limit is exceeded during the month. Use the no command to disable budget control. |
| [no] budget time active <1..672> | Sets the amount of time (in hours) that the 3G connection can be used within one month. If you change the value, the ZyWALL / USG resets the statistics. Use the no command to disable time budget control. |
| [no] budget data active {download-upload\|download\|upload} <1..100000> | Sets how much downstream and/or upstream data (in Mega bytes) can be transmitted via the 3G connection within one month.<br><br>download: set a limit on the downstream traffic (from the ISP to the ZyWALL / USG).<br><br>upload: set a limit on the upstream traffic (from the ZyWALL / USG to the ISP).<br><br>download-upload: set a limit on the total traffic in both directions.<br><br>If you change the value, the ZyWALL / USG resets the statistics.<br><br>Use the no command to disable data budget control. |
| budget reset-day <0..31> | Sets the date on which the ZyWALL / USG resets the budget every month. If the date you selected is not available in a month, such as 30th or 31st, the ZyWALL / USG resets the budget on the last day of the month. |
| budget reset-counters | Resets the time and data budgets immediately. The count starts over with the 3G connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart. |
| budget {log\|log-alert}[recursive <1..65535>] | Sets the ZyWALL / USG to create a log (log) or an alert log (log-alert) when the time or data limit is exceeded. You can also specify how often (from 1 to 65535 minutes) to generate a log or an alert. |
| no budget log [recursive] | Sets the ZyWALL / USG to not create a log when the time or data limit is exceeded. Specify recursive to have the ZyWALL / USG only create a log one time when the time or data limit is exceeded. |
| budget new-connection {allow\|disallow} | Sets to permit (allow) or drop/block (disallow) new 3G connections when the time or data limit is exceeded. |
| budget current-connection {keep\|drop} | Sets to maintain the existing 3G connection (keep) or disconnect it (drop) when the time or data limit is exceeded. You cannot set budget new-connection to allow and budget current-connection to drop at the same time.<br><br>If you set budget new-connection to disallow and budget current-connection to keep, the ZyWALL / USG allows you to transmit data using the current connection, but you cannot build a new connection if the existing connection is disconnected. |

**Table 38** Cellular Interface Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] network-selection {auto\|home} | Home network is the network to which you are originally subscribed.<br><br>Home has the 3G device connect only to the home network. If the home network is down, the ~~ZyWALL~~ZyWALL / USG's 3G Internet connection is also unavailable.<br><br>Auto is the default setting and allows the 3G device to connect to a network to which you are not subscribed when necessary, for example when the home network is down or another 3G base station's signal is stronger. This is recommended if you need continuous Internet connectivity. If you select this, you may be charged using the rate of a different network. |
| [no] budget active | Sets a monthly limit for the user account of the installed 3G card. You can set a limit on the total traffic and/or call time. The ZyWALL / USG takes the actions you specified when a limit is exceeded during the month. Use the no command to disable budget control. |
| [no] budget time active <1..672> | Sets the amount of time (in hours) that the 3G connection can be used within one month. If you change the value, the ZyWALL / USG resets the statistics. Use the no command to disable time budget control. |
| [no] budget data active {download-upload\|download\|upload} <1..100000> | Sets how much downstream and/or upstream data (in Mega bytes) can be transmitted via the 3G connection within one month.<br><br>download: set a limit on the downstream traffic (from the ISP to the ZyWALL / USG).<br><br>upload: set a limit on the upstream traffic (from the ZyWALL / USG to the ISP).<br><br>download-upload: set a limit on the total traffic in both directions.<br><br>If you change the value, the ZyWALL / USG resets the statistics.<br><br>Use the no command to disable data budget control. |
| budget reset-day <0..31> | Sets the date on which the ZyWALL / USG resets the budget every month. If the date you selected is not available in a month, such as 30th or 31st, the ZyWALL / USG resets the budget on the last day of the month. |
| budget reset-counters | Resets the time and data budgets immediately. The count starts over with the 3G connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart. |
| budget {log\|log-alert}[recursive <1..65535>] | Sets the ZyWALL / USG to create a log (log) or an alert log (log-alert) when the time or data limit is exceeded. You can also specify how often (from 1 to 65535 minutes) to generate a log or an alert. |
| no budget log [recursive] | Sets the ZyWALL / USG to not create a log when the time or data limit is exceeded. Specify recursive to have the ZyWALL / USG only create a log one time when the time or data limit is exceeded. |
| budget new-connection {allow\|disallow} | Sets to permit (allow) or drop/block (disallow) new 3G connections when the time or data limit is exceeded. |
| budget current-connection {keep\|drop} | Sets to maintain the existing 3G connection (keep) or disconnect it (drop) when the time or data limit is exceeded. You cannot set budget new-connection to allow and budget current-connection to drop at the same time.<br><br>If you set budget new-connection to disallow and budget current-connection to keep, the ZyWALL / USG allows you to transmit data using the current connection, but you cannot build a new connection if the existing connection is disconnected. |

**Table 38** Cellular Interface Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| budget percentage {ptime\|pdata} <0..99> | Sets a percentage (0~99) of time budget (ptime) or data (pdata) limit. When the specified limit is exceeded, the ZyWALL / USG takes the action configured using the budget {log-percentage\|log-percentage-alert} command. |
| budget {log-percentage\|log-percentage-alert} [recursive <1..65535>] | Sets to have the ZyWALL / USG create a log (log-percentage) or an alert log (log-percentage-alert) when the set percentage of time budget or data limit is exceeded. You can configure the percentage using the budget percentage command.<br>You can also set how often (from 1 to 65535 minutes) to send the log or alert. |
| no budget log-percentage | Sets the ZyWALL / USG to not create a log when the set percentage of time budget or data limit is exceeded. You can configure the percentage using the budget percentage command. |
| connectivity {nail-up \| dial-on-demand} | Sets the connection to be always on or only when there is traffic. |
| [no] local-address <*ip*> | Sets (or clears) the cellular interface's local (own) IP address. |
| mtu <576..1492> | Sets the Maximum Transmission Unit in bytes. |
| [no] pin <*pin code*> | Sets (or clears) the PIN code for the cellular device's 3G card. Use 1-4 alphanumeric characters, underscores(_), or dashes (-). |
| [no] remote-address <*ip*> | Sets (or clears) the IP address of the cellular interface's peer (like a gateway or PPPoE server). |
| interface cellular budget-auto-save <5..1440> | Sets how often (in minutes) the ZyWALL / USG saves time and data usage records for a connection using the 3G card. |
| show interface cellular [corresponding-slot\|device-status\|support-device] | Shows the status of the specified cellular interface. |
| show interface cellular corresponding-slot | Shows which cellular interface is on which slot and whether which cellular interface has been configured. |
| show interface cellular device-status | Displays the installed SIM card and 3G card status. |
| show interface cellular support-device | Displays all 3G card models the ZyWALL / USG can support. |
| show interface cellular budget-auto-save | Displays how often (in minutes) the ZyWALL / USG records time and data usage of your 3G budgets. |
| show interface cellular status | Displays the traffic statistics and connection status for your cellular interfaces. See Section 8.6.1 on page 97 for all possible cellular status descriptions. |
| show interface *interface_name* [budget] | Displays the budget control settings for the specified cellular interface. |
| show interface *interface_name* device status | Displays the 3G card and SIM card information for the specified cellular interface. |
| show interface *interface_name* device profile | Displays the 3G connection profile settings of the specified cellular interface. |

## 8.6.1 Cellular Status

The following table describes the different kinds of cellular connection status on the ZyWALL / USG.

**Table 39** Cellular Status

| STATUS | DESCRIPTION |
|---|---|
| No device | no 3G device is connected to the ZyWALL / USG. |
| No service | no 3G network is available in the area; you cannot connect to the Internet. |

**Table 39** Cellular Status

| STATUS | DESCRIPTION |
|---|---|
| Limited service | returned by the service provider in cases where the SIM card is expired, the user failed to pay for the service and so on; you cannot connect to the Internet. |
| Device detected | displays when you connect a 3G device. |
| Device error | a 3G device is connected but there is an error. |
| Probe device fail | the ZyWALL / USG's test of the 3G device failed. |
| Probe device ok | the ZyWALL / USG's test of the 3G device failed. |
| Init device fail | the ZyWALL / USG was not able to initialize the 3G device. |
| Init device ok | the ZyWALL / USG initialized the 3G card. |
| Check lock fail | the ZyWALL / USG's check of whether or not the 3G device is locked failed. |
| Device locked | the 3G device is locked. |
| SIM error | there is a SIM card error on the 3G device. |
| SIM locked-PUK | the PUK is locked on the 3G device's SIM card. |
| SIM locked-PIN | the PIN is locked on the 3G device's SIM card. |
| Unlock PUK fail | Your attempt to unlock a WCDMA 3G device's PUK failed because you entered an incorrect PUK. |
| Unlock PIN fail | Your attempt to unlock a WCDMA 3G device's PIN failed because you entered an incorrect PIN. |
| Unlock device fail | Your attempt to unlock a CDMA2000 3G device failed because you entered an incorrect device code. |
| Device unlocked | You entered the correct device code and unlocked a CDMA2000 3G device. |
| Get dev-info fail | The ZyWALL / USG cannot get cellular device information. |
| Get dev-info ok | The ZyWALL / USG succeeded in retrieving 3G device information. |
| Searching network | The 3G device is searching for a network. |
| Get signal fail | The 3G device cannot get a signal from a network. |
| Network found | The 3G device found a network. |
| Apply config | The ZyWALL / USG is applying your configuration to the 3G device. |
| Device unready | The 3G interface is disabled. |
| Active | The 3G interface is enabled. |
| Incorrect device | The connected 3G device is not compatible with the ZyWALL / USG. |
| Correct device | The ZyWALL / USG detected a compatible 3G device. |
| Set band fail | Applying your band selection was not successful. |
| Set band ok | The ZyWALL / USG successfully applied your band selection. |
| Set profile fail | Applying your ISP settings was not successful. |
| Set profile ok | The ZyWALL / USG successfully applied your ISP settings. |
| PPP fail | The ZyWALL / USG failed to create a PPP connection for the cellular interface. |
| Need auth-password | You need to enter the password for the 3G card in the cellular edit screen. |
| Device ready | The ZyWALL / USG successfully applied all of your configuration and you can use the 3G connection. |

## 8.6.2 Cellular Interface Command Examples

This example shows the configuration of a cellular interface named cellular2 for use with a Sierra Wireless AC850 3G card. It uses only a 3G (or 3.5G) connection, PIN code 1234, an MTU of 1200 bytes, a description of "This is cellular2" and sets the connection to be nailed-up.

```
Router(config)# interface cellular2
Router(config-if-cellular)# device AC850
Router(config-if-cellular)# band wcdma
Router(config-if-cellular)# pin 1234
Router(config-if-cellular)# connectivity nail-up
Router(config-if-cellular)# description This is cellular2
Router(config-if-cellular)# mtu 1200
Router(config-if-cellular)# exit
```

This second example shows specifying a new PIN code of 4567.

```
Router(config)# interface cellular2
Router(config-if-cellular)# pin 4567
Router(config-if-cellular)# exit
```

This example shows the 3G and SIM card information for interface cellular2 on the ZyWALL / USG.

```
Router(config)# show interface cellular2 device status
interface name: cellular2
extension slot: USB 1
service provider: Chunghwa Telecom
cellular system: WCDMA
signal strength: -95 dBm
signal quality: Poor
device type: WCDMA
device manufacturer: Huawei
device model: E220/E270/E800A
device firmware: 076.11.07.106
device IMEI/ESN: 351827019784694
SIM card IMSI: 466923100565274
```

This example shows the 3G connection profile settings for interface cellular2 on the ZyWALL / USG. You have to dial *99***1# to use profile 1, but authentication is not required. Dial *99***2# to use profile 2 and authentication is required.

```
Router(config)# show interface cellular2 device profile
profile: 1
apn: internet
dial-string: *99***1#
authentication: none
user: n/a
password: n/a
profile: 2
apn: internet
dial-string: *99***2#
authentication: chap
user:
password: ***
----------------------SNIP!-----------------------------------------------
```

# 8.7 Tunnel Interface Specific Commands

The ZyWALL / USG uses tunnel interfaces in Generic Routing Encapsulation (GRE), IPv6 in IPv4, and 6to4 tunnels. This section covers commands specific to tunnel interfaces. Tunnel interfaces also use many of the general interface commands discussed at the beginning of Section 8.2 on page 73.

Use these commands to add, edit, activate, deactivate, or delete tunnel interfaces. You must use the `configure terminal` command to enter the configuration mode before you can use these commands. GRE mode tunnels support ping check. See Section 8.2.7 on page 88 for more on ping check.

**Table 40** Tunnel Interface Commands

| COMMAND | DESCRIPTION |
|---|---|
| `[no] interface tunnel_iface` | Creates the specified interface if necessary and enters sub-command mode. The `no` command deletes the specified interface.<br>*tunnel_iface*: Name of tunnel interface. tunnel([0-3]). |
| `[no] shutdown` | Deactivates the specified interface. The `no` command activates it. |
| `tunnel source [ipv4\|tunnel_bind_interface\|_any]` | Configures the outer source IP address of the tunneled packets. Specify an IPv4 address or use the IP address of an interface.<br>`_any`: Have automatically select the outer source IP. Not available for ipv6ip mode tunnels. |
| `tunnel destination ipv4` | Configures the outer destination IP address of the tunneled IPv4 packets. |
| `ip address ipv4 ipv4` | Sets the inner source IP of packets sent through the tunnel interface. |
| `tunnel mode ip gre` | Sets this interface to use GRE tunnel mode. |
| `[no] mtu <576..1480>` | Specifies the Maximum Transmission Unit, which is the maximum number of bytes in each packet moving through this interface. The ZyWALL / USG divides larger packets into smaller fragments. The `no` command resets the MTU to 1480. |
| `[no] downstream <0..1048576>` | Specifies the downstream bandwidth for the specified interface. The `no` command sets the downstream bandwidth to 1048576. |
| `tunnel mode [ ipv6ip [ manual \| 6to4 ] ] ]` | Sets the interface to be an IPv6 over IPv4 tunnel.<br>`manual`: Use for a point-to-point manual tunnel for IPv6 transition. You must also configure a policy route for the tunnel.<br>6to4: Use for a 6to4/6RD automatic tunnel. |
| `ipv6 address ipv6_addr_prefix` | Sets an IPv6 address with prefix for the interface. |
| `ipv6 6to4 [ prefix ipv6_addr_prefix \| destination-prefix ipv4_cidr \| relay ipv4 ]` | For a 6to4 tunnel, sets the IPv6 address with prefix, remote gateway prefix, or relay router IPv4 address. |
| `traffic-prioritize {tcp-ack\|content-filter\|dns} bandwidth <0..1048576> priority <1..7> [maximize-bandwidth-usage];` | Applies traffic priority when the interface sends TCP-ACK traffic, traffic for querying the content filter, or traffic for resolving domain names. It also sets how much bandwidth the traffic can use and can turn on maximize bandwidth usage. |
| `traffic-prioritize {tcp-ack\|content-filter\|dns} deactivate` | Turns off traffic priority settings for when the interface sends the specified type of traffic. |
| `exit` | Leaves the sub-command mode. |
| `show interface tunnel_iface` | Displays the the specified tunnel's settings. |
| `show interface tunnel status` | Displays the status of the tunnel interfaces. |

### 8.7.1 Tunnel Interface Command Examples

This example creates a tunnel interface called tunnel0 that uses wan1 as the source, 168.168.168.168 as the destination, and 10.0.0.100 and 255.255.0.0 as the inner source IP.

```
Router> configure terminal
Router(config)# interface tunnel0
Router(config-if-tunnel)# tunnel source wan1
Router(config-if-tunnel)# tunnel destination 168.168.168.168
Router(config-if-tunnel)# ip address 10.0.0.100 255.255.0.0
Router(config-if-tunnel)# exit

Router(config)# show interface tunnel
tunnel interface: 1
  interface name: tunnel0
  local address: ge2
  local address type: bind
  remote address: 168.168.168.168
  mode: gre
  IP address: 10.0.0.100
  netmask: 255.255.0.0
  status: Inactive
  active: no
```

## 8.8 USB Storage Specific Commands

Use these commands to configure settings that apply to the USB storage device connected to the ZyWALL / USG.

Note: For the ZyWALL / USG which supports more than one USB ports, these commands only apply to the USB storage device that is first attached to the ZyWALL / USG.

**Table 41** USB Storage General Commands

| COMMAND | DESCRIPTION |
|---|---|
| `show usb-storage` | Displays the status of the connected USB storage device. |
| `[no] usb-storage activate` | Enables or disables the connected USB storage service. |
| `usb-storage warn` *number* `<`*percentage*`\|megabyte>` | Sets a number and the unit (`percentage` or `megabyte`) to have the ~~ZyWALL~~ZyWALL / USG send a warning message when the remaining USB storage space is less than the set value. |
| `usb-storage mount` | Mounts the connected USB storage device. |
| `usb-storage umount` | Unmounts the connected USB storage device. |
| `[no] logging usb-storage` | Sets to have the ZyWALL / USG log or not log any information about the connected USB storage device(s) for the system log. |
| `show logging status usb-storage` | Displays the logging settings for the connected USB storage device. |
| `logging usb-storage category` *category* `level <all\|normal>` | Configures the logging settings for the specified category for the connected USB storage device. |
| `logging usb-storage category` *category* `disable` | Stops logging for the specified category to the connected USB storage device. |
| `logging usb-storage flushThreshold <1..100>` | Configures the maximum storage space (in percentage) for storing system logs on the connected USB storage device. |

**Table 41** USB Storage General Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| `[no] diag-info copy usb-storage` | Sets to have the ZyWALL / USG save or stop saving the current system diagnostics information to the connected USB storage device. You may need to send this file to customer support for troubleshooting. |
| `show diag-info copy usb-storage` | Displays whether (enable or disable) the ZyWALL / USG saves the current system diagnostics information to the connected USB storage device. |
| `[no] corefile copy usb-storage` | Sets to have the ZyWALL / USG save or not save a process's core dump to the connected USB storage device if the process terminates abnormally (crashes). You may need to send this file to customer support for troubleshooting. |
| `show corefile copy usb-storage` | Displays whether (enable or disable) the ZyWALL / USG saves core dump files to the connected USB storage device. |

### 8.8.1 USB Storage General Commands Example

This example shows how to display the status of the connected USB storage device.

```
Router> show usb-storage
USBStorage Configuration:
Activation: enable
Criterion Number: 100
Criterion Unit: megabyte
USB Storage Status:
Device description: N/A
Usage: N/A
Filesystem: N/A
Speed: N/A
Status: none
Detail: none
```

## 8.9 WLAN Specific Commands

You can install a compatible WLAN card to use the ZyWALL / USG as an access point (AP) for a wireless network.

The following table identifies the values required for several WLAN commands. Other input values are discussed with the corresponding commands.

**Table 42** Input Values for WLAN Interface Commands

| LABEL | DESCRIPTION |
|---|---|
| *psk-key* | Use 8 to 63 case-sensitive alphanumeric characters or 64 hexadecimal characters. This is used for WLAN interface commands. See Table 44 on page 104 |

## 8.9.1 WLAN General Commands

Use these commands to configure global settings that apply to all of the wireless LAN interfaces you create on the WLAN card.

**Table 43** WLAN General Commands

| COMMAND | DESCRIPTION |
|---|---|
| wlan *slot_name* | Specifies the slot the WLAN card is installed in and enters sub-command mode.<br>*slot_name*: The name of the slot where the WLAN card is installed in the ZyWALL / USG. Use slot*x* where *x* equals the number of the card slot. |
| [no] activate | Turns the wireless device on. The no command turns it off. |
| band <b \| g \| bg\| bgn \| gn> | Sets which IEEE 802.11 wireless standard wireless clients can use to connect to the wireless interface.<br>• b<br>• g<br>• b or g<br>• b, g, or n<br>• g or n. |
| channel <*wireless_channel* \| auto> | Sets the wireless operating channel of an IEEE 802.11n interface.<br>*wireless_channel*: Specify the channel number. The numbers available vary by region. |
| channel-width <auto \| 20m \| 40m> | Sets how wide a channel the IEEE 802.11n interface uses. |
| guard-interval <short \| long> | Sets the IEEE 802.11n interface's gap between data transmissions from users to reduce interference.<br>short: increases data throughput but may make data transfer more prone to errors.<br>long: prioritizes data integrity but reduces data transfer rates. |
| [no] ampdu | For an IEEE 802.11n interface, enables or disables grouping of several A-MPDUs (Aggregate MAC Protocol Data Unit) into one larger frame for faster data transfer rates. |
| [no] amsdu | For an IEEE 802.11n interface, enables or disables grouping of several A-MSDUs (Aggregate MAC Service Data Units) into one large A-MPDU (Aggregate MAC Protocol Data Unit) for faster data transfer rates. |
| [no] block-ack | Turns the IEEE 802.11n interface's block ACK (BA) mechanism on or off. Block ACK lets multiple frames be streamed out and acknowledged by a single frame. This cuts the wait time between frames and increases data throughput. |
| qos <none \| wmm> | Select the WLAN Quality of Service priority for an IEEE 802.11n interface.<br>none: Apply no priority to traffic.<br>wmm: Wi-Fi Multimedia has the priority of a data packet depend on the packet's IEEE 802.1q or DSCP header. If a packet has no WMM value assigned to it, it is assigned the default priority. |
| [no] ctsrts <256..2346> | Sets the Clear To Send/Request To Send threshold. CTS/RTS reduces data collisions caused by wireless clients that are associated with the same AP but out of range of one another. The no command turns off CTS/RTS. |
| [no] frag <256..2346> | Sets the threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. |
| [no] super | Enables super mode (fast frame and packet bursting). |
| role ap | Sets the ZyWALL / USG to act as an AP (only the AP role is supported at the time of writing. |
| output-power [100% \| 50% \| 25% \| 12.5%] | Sets the wireless output power. Reducing output power can help reduce interference with other nearby APs. |

**Table 43** WLAN General Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| qos [none \| wmm} | Applies Wi-Fi Multimedia Quality of Service (QoS) or no wireless QoS. |
| guard-interval [short \| long] | Sets Guard Interval to Short (increases data throughput) or Long (prioritize data integrity). |
| [no] amsdu | Enables Aggregated Mac Service Data Unit (AMSDU) for faster data transfer rates. |
| [no] ampdu | Enables Aggregated Mac Protocol Data Unit (AMPDU) for faster data transfer rates. |
| [no] block-ack | Adds the block ACK (BA) mechanism to increase data output. |
| exit | Leaves the sub-command mode. |

#### 8.9.1.1 WLAN General Commands Example

This example sets wireless slot 1 to use the IEEE 802.11b and IEEE 802.11g bands, channel 5, super mode, 50 % output power, and enables it.

```
Router(config)# wlan slot1
Router(config-wlan-slot)# band bg
Router(config-wlan-slot)# channel 5
Router(config-wlan-slot)# super
Router(config-wlan-slot)# output-power 50%
Router(config-wlan-slot)# activate
Router(config-wlan-slot)# exit
Router(config)#
```

### 8.9.2 WLAN Interface Commands

Use these commands to configure global settings that apply to all of the wireless LAN interfaces you create on the WLAN card.

**Table 44** WLAN Interface Commands

| COMMAND | DESCRIPTION |
|---|---|
| [no] interface *ap_interface* | Creates the specified interface if necessary and enters sub-command mode. The no command deletes the specified interface.<br><br>*ap_interface*: The name of the WLAN Access Point interface. Use wlan-*x*-*y* where *x* equals the number of the card slot and *y* equals the number of the individual WLAN interface. For example, wlan-1-1. |
| [no] block-intra | Enables intra-BSS blocking (prevents) wireless clients in this profile's BSS from communicating with one another. |
| group-key <30..30000> | Sets the WPA2 group key update timer. This is the interval in seconds for how often the AP sends a new group key out to all clients. |
| [no] hide | Obscures the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning. |
| idle <30..30000> | Sets the WPA2 idle timeout. The ZyWALL / USG automatically disconnects a wireless station that has been inactive for this number of seconds. The wireless station needs to enter the username and password again before access to the wired network is allowed. |
| [no] ip address *ip subnet_mask* | Assigns the specified IP address and subnet mask to the specified interface. The no command clears the IP address and the subnet mask. |
| [no] ip gateway *ip* [metric <0..15>] | Adds the specified gateway for the interface. Sets the priority (relative to every gateway on every interface) for the specified gateway. The lower the number, the higher the priority. The no command removes the gateway. |

**Table 44** WLAN Interface Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] mtu <576..2304> | Specifies the Maximum Transmission Unit, which is the maximum number of bytes in each packet moving through this interface. The ZyWALL / USG divides larger packets into smaller fragments. The no command resets the MTU to 1500. |
| reauth <30..30000> | Sets the WPA2 reauthentication timer. This is at what interval wireless stations have to resend usernames and passwords in order to stay connected. If a RADIUS server authenticates wireless stations, the reauthentication timer on the RADIUS server has priority. |
| security mode {none \| wep \| wpa \| wpa-wpa2 \| wpa2} | Sets what type of security the wireless interface uses.<br>none: applies no security.<br>wep: WEP security (extremely weak).<br>wpa: WPA security.<br>wpa-wpa2: WPA/WPA2-Enterprise or WPA/WPA2-PSK security.<br>wpa2: WPA2 security (strongest option). |
| security wep <64 \| 128> default-key <1..4> | Sets WEP encryption to use a 64 or 128 bit key and selects the default key. |
| security wep mode <open \| share> | Sets the WEP encryption to use open or shared key authentication. |
| security wpa <tkip \| aes> eap internal *profile-name* tls-cert *certificate name* | Configures WPA enterprise security using TKIP or AES and an existing AAA authentication method object (*profile-name*). Set the certificate the ZyWALL / USG uses to authenticate itself to the wireless clients. The wireless clients must use TTLS authentication protocol and PAP inside the TTLS secure tunnel. |
| security wpa <tkip \| aes> eap external | Configures WPA enterprise security using TKIP or AES and an external server. Use the security external command to specify the server's address. |
| security wpa <tkip \| aes> psk key *psk-key* | Configures WPA security using TKIP or AES and a Pre-Shared Key (PSK). |
| security wpa-wpa2 <tkip \| aes> eap internal *profile-name* tls-cert *certificate name* | This allows users to either use WPA or WPA2 enterprise security to connect to the wireless interface. You have to also configure to use either TKIP or AES and an existing AAA authentication method object (*profile-name*). Set the certificate the ZyWALL / USG uses to authenticate itself to the wireless clients. The wireless clients must use TTLS authentication protocol and PAP inside the TTLS secure tunnel. |
| security wpa-wpa2 <tkip \| aes> eap external | Configures WPA or WPA2 enterprise security using TKIP or AES and an external server. Use the security external command to specify the server's address. |
| security wpa-wpa2 <tkip \| aes> psk key *psk-key* | Configures WPA or WPA2 security using TKIP or AES and a Pre-Shared Key (PSK). |
| security wpa2 <tkip \| aes> eap internal *profile-name* tls-cert *certificate name* | Configures WPA2 enterprise security using TKIP or AES and an existing AAA authentication method object (*profile-name*). Select the certificate the ZyWALL / USG uses to authenticate itself to the wireless clients. The wireless clients must use TTLS authentication protocol and PAP inside the TTLS secure tunnel. |
| security wpa2 <tkip \| aes> eap external | Configures WPA2 enterprise security using TKIP or AES and an external server. Use the security external command to specify the server's address. |
| security wpa2 <tkip \| aes> psk key *psk-key* | Configures WPA2 security using TKIP or AES and a Pre-Shared Key (PSK). |
| [no] security dot1x acct *ip* port <1..65535> | Sets the IP address and port number of an external accounting server. |
| [no] security dot1x auth *ip* port <1..65535> | Sets the IP address and port number of an external authentication (RADIUS) server. |
| [no] security dot1x activate | Enables IEEE 802.1x accounting and authentication. |

**Table 44** WLAN Interface Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] security external acct *ip* port <1..65535> | Sets the IP address and port number of an external accounting server. |
| [no] security external auth *ip* port <1..65535> | Sets the IP address and port number of an external authentication (RADIUS) server. |
| no security {none \| wep \| wpa \| wpa-wpa2 \| wpa2} | Disables the specified security mode for the wireless interface. |
| ssid *ssid* | Sets the (Service Set IDentity). This identifies the Service Set with which a wireless station is associated. Wireless stations associating to the ZyWALL / USG must have the same SSID.<br>*ssid*: Use up to 32 printable 7-bit ASCII characters as a name for the wireless LAN. |
| station-limit <1..255> | Sets the highest number of wireless clients that are allowed to connect to the wireless interface at the same time. |
| wep-key <1..4> *key* | There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations.<br>If you set WEP encryption to use a 64 bit key using the security mode and security wep 64 commands, type any 5 characters (ASCII string) or 5 pairs of hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>If you set WEP encryption to use a 128 bit key using the security mode and security wep 128 commands, type 13 characters (ASCII string) or 13 pairs of hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. |

### 8.9.2.1 WLAN Interface Commands Example

This example configures WLAN AP interface 2 for slot 1 to use SSID WLAN_test, WPA security modes with a pre-shared key of 12345678, IP address 1.1.1.1, netmask 255.255.255.0, and a gateway IP address of 1.2.3.4 with a priority of 10.

```
Router(config)# interface wlan-1-2
Router(config-if-wlan)# ssid WLAN_test
Router(config-if-wlan)# security wpa tkip psk key 12345678
Router(config-if-wlan)# security mode wpa
Router(config-if-wlan)# ip address 1.1.1.1 255.255.255.0
Router(config-if-wlan)# ip gateway 1.2.3.4 metric 10
Router(config-if-wlan)# exit
```

### 8.9.3 WLAN MAC Filter Commands

Use these commands to give specific wireless clients exclusive access to the ZyWALL / USG (allow association) or block specific devices from accessing the ZyWALL / USG (deny association) based on the devices' MAC addresses.

**Table 45** WLAN General Commands

| COMMAND | DESCRIPTION |
|---|---|
| `[no] wlan mac-filter` *mac_address* `[description` *description*`]` | Specifies the MAC address (in XX:XX:XX:XX:XX:XX format) of the wireless station that is to be allowed or denied access to the ZyWALL / USG. The `no` command removes the entry.<br>*description*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long. |
| `[no] wlan mac-filter activate` | Turns the MAC address filter on or off. |
| `wlan mac-filter associate <allow \| deny>` | Defines the filter action for the list of MAC addresses in the MAC address filter table. Allow permits them to access to the ZyWALL / USG, MAC addresses not listed will be blocked.<br>Deny blocks the listed addresses from accessing the router, MAC addresses not listed will be allowed to access the router. |
| `show wlan mac-filter status` | Displays the MAC filter's activation and association settings. |
| `show wlan mac-filter` | Displays the WLAN MAC filter entries. |

#### 8.9.3.1 WLAN MAC Filter Commands Example

This example creates a MAC filter entry for MAC address 01:02:03:04:05:06 and sets the ZyWALL / USG to allow wireless access from that entry's MAC address only.

```
Router(config)# wlan mac-filter 01:02:03:04:05:06 description example
Router(config)# wlan mac-filter associate allow
Router(config)# wlan mac-filter activate
Router(config)# show wlan mac-filter status
Enable: yes
Association: allow
Router(config)# show wlan mac-filter
No. MAC                 Description
================================================================================
1   01:02:03:04:05:06    example
```

## 8.10 VLAN Interface Specific Commands

This section covers commands that are specific to VLAN interfaces. VLAN interfaces also use many of the general interface commands discussed at the beginning of Section 8.2 on page 73.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 46** Input Values for VLAN Interface Commands

| LABEL | DESCRIPTION |
|---|---|
| *interface_name* | VLAN interface: vlan*x*, *x* = 0 - 4094<br><br>Ethernet interface: For the ZyWALL / USG USG 300 and above, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model.<br><br>The ZyWALL / USG USG 200 and below models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. |

This table lists the VLAN interface commands.

**Table 47** interface Commands: VLAN Interfaces

| COMMAND | DESCRIPTION |
|---|---|
| `interface` *interface_name* | Creates the specified interface if necessary and enters sub-command mode. |
| `[no] port` *interface_name* | Specifies the Ethernet interface on which the VLAN interface runs. The `no` command clears the port. |
| `[no] vlan-id <1..4094>` | Specifies the VLAN ID used to identify the VLAN. The `no` command clears the VLAN ID. |
| `show port vlan-id` | Displays the Ethernet interface VLAN settings. |

## 8.10.1 VLAN Interface Command Examples

The following commands show you how to set up VLAN vlan100 with the following parameters: VLAN ID 100, interface ge1, IP 1.2.3.4, subnet 255.255.255.0, MTU 598, gateway 2.2.2.2, description "I am vlan100", upstream bandwidth 345, and downstream bandwidth 123.

```
Router# configure terminal
Router(config)# interface vlan100
Router(config-if-vlan)# vlan-id 100
Router(config-if-vlan)# port ge1
Router(config-if-vlan)# ip address 1.2.3.4 255.255.255.0
Router(config-if-vlan)# ip gateway 2.2.2.2
Router(config-if-vlan)# mtu 598
Router(config-if-vlan)# upstream 345
Router(config-if-vlan)# downstream 123
Router(config-if-vlan)# description I am vlan100
Router(config-if-vlan)# exit
```

# 8.11 Bridge Specific Commands

This section covers commands that are specific to bridge interfaces. Bridge interfaces also use many of the general interface commands discussed at the beginning of Section 8.2 on page 73.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 48** Input Values for Bridge Interface Commands

| LABEL | DESCRIPTION |
|---|---|
| *interface_name* | The name of the interface.<br>Ethernet interface: For the ZyWALL / USG USG 300 and above, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model.<br>The ZyWALL / USG USG 200 and below models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.<br>VLAN interface: vlan*x*, *x* = 0 - 4094<br>bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ZyWALL / USG model supports. |

This table lists the bridge interface commands.

**Table 49** interface Commands: Bridge Interfaces

| COMMAND | DESCRIPTION |
|---|---|
| `interface` *interface_name* | Creates the specified interface if necessary and enters sub-command mode. |
| `[no] join` *interface_name* | Adds the specified Ethernet interface or VLAN interface to the specified bridge. The `no` command removes the specified interface from the specified bridge. |
| `show bridge available member` | Displays the available interfaces that could be added to a bridge. |

## 8.11.1 Bridge Interface Command Examples

The following commands show you how to set up a bridge interface named br0 with the following parameters: member ge1, IP 1.2.3.4, subnet 255.255.255.0, MTU 598, gateway 2.2.2.2, upstream bandwidth 345, downstream bandwidth 123, and description “I am br0”.

```
Router# configure terminal
Router(config)# interface br0
Router(config-if-brg)# join ge1
Router(config-if-brg)# ip address 1.2.3.4 255.255.255.0
Router(config-if-brg)# ip gateway 2.2.2.2
Router(config-if-brg)# mtu 598
Router(config-if-brg)# upstream 345
Router(config-if-brg)# downstream 123
Router(config-if-brg)# description I am br0
Router(config-if-brg)# exit
```

# 8.12 Auxiliary Interface Specific Commands

The first table below lists the auxiliary `interface` commands, and the second table explains the values you can input with these commands.

**Table 50** interface Commands: Auxiliary Interface

| COMMAND | DESCRIPTION |
|---|---|
| `interface dial aux`<br>`interface disconnect aux` | Dials or disconnects the auxiliary interface. |
| `interface aux` | Enters sub-command mode. |
| `[no] authentication {chap-pap \| chap \| pap \| mschap \| mschap-v2}` | Specifies the authentication type of the auxiliary interface. The `no` command sets the authentication to chap-pap. |
| `[no] dial timeout <30..120>` | Specifies the number of seconds the auxiliary interface waits for an answer each time it tries to connect. The `no` command disables the timeout. |
| `[no] dialing type {tone \| pulse}` | Specifies the dial type of the auxiliary interface. The `no` command sets the dial type to tone. |
| `[no] idle <0..360>` | Specifies the number of seconds the auxiliary interface waits for activity before it automatically disconnects. The `no` command disables the idle timeout. |
| `[no] initial-string` *`initial_string`* | Specifies the initial string of the auxiliary interface. The `no` command sets the initial string to "ATZ".<br><br>*`initial_string`*: You can use up to 64 characters. Semicolons (;) and backslashes (\) are not allowed. |
| `[no] password` *`password`* | Specifies the password of the auxiliary interface. The `no` command clears the password.<br><br>*`password`*: You can use up to 63 printable ASCII characters. Spaces are not allowed. |
| `[no] phone-number` *`phone`* | Specifies the phone number of the auxiliary interface. You can use 1-20 numbers, commas (,), or plus signs (+). Use a comma to pause during dialing. Use a plus sign to tell the external modem to make an international call. The `no` command clears the phone number. |
| `[no] port-speed {9600 \| 19200 \| 38400 \| 57600 \| 115200}` | Specifies the baud rate of the auxiliary interface. The `no` command sets the baud rate to 115200. |
| `[no] username` *`username`* | Specifies the username of the auxiliary interface. The `no` command clears the username.<br><br>*`username`*: You can use alphanumeric, underscores (_), dashes (-), periods (.), and /@$ characters, and it can be up to 64 characters long. |

## 8.12.1 Auxiliary Interface Command Examples

The following commands show you how to set up the auxiliary interface aux with the following parameters: phone-number 0340508888, tone dialing, port speed 115200, initial-string ATZ,

timeout 30 seconds, username **kk**, password kk@u2online, chap-pap authentication, and description "I am aux interface".

```
Router# configure terminal
Router(config)# interface aux
Router(config-if-aux)# phone-number 0340508888
Router(config-if-aux)# dialing-type tone
Router(config-if-aux)# port-speed 115200
Router(config-if-aux)# initial-string ATZ
Router(config-if-aux)# timeout 30
Router(config-if-aux)# username kk
Router(config-if-aux)# password kk@u2online
Router(config-if-aux)# authentication chap-pap
Router(config-if-aux)# description I am aux interface
Router(config-if-aux)# exit
```

The following commands show how to dial, disconnect, and stop the auxiliary interface.

```
Router# interface dial aux
Router# interface disconnect aux
```

# 9

# Trunks

This chapter shows you how to configure trunks on your ZyWALL / USG.

## 9.1 Trunks Overview

You can group multiple interfaces together into trunks to have multiple connections share the traffic load to increase overall network throughput and enhance network reliability. If one interface's connection goes down, the ZyWALL / USG sends traffic through another member of the trunk. For example, you can use two interfaces for WAN connections. You can connect one interface to one ISP (or network) and connect the another to a second ISP (or network). The ZyWALL / USG can balance the load between multiple connections. If one interface's connection goes down, the ZyWALL / USG can automatically send its traffic through another interface.

You can use policy routing to specify through which interface to send specific traffic types. You can use trunks in combination with policy routing. You can also define multiple trunks for the same physical interfaces. This allows you to send specific traffic types through the interface that works best for that type of traffic, and if that interface's connection goes down, the ZyWALL / USG can still send its traffic through another interface.

## 9.2 Trunk Scenario Examples

Suppose one of the ZyWALL / USG's interfaces is connected to an ISP that is also your Voice over IP (VoIP) service provider. You may want to set that interface as active and set another interface (connected to another ISP) to passive. This way VoIP traffic goes through the interface connected to the VoIP service provider whenever the interface's connection is up.

Another example would be if you use multiple ISPs that provide different levels of service to different places. Suppose ISP A has better connections to Europe while ISP B has better connections to Australia. You could use policy routing and trunks to send traffic for your European branch offices primarily through ISP A and traffic for your Australian branch offices primarily through ISP B.

# 9.3 Trunk Commands Input Values

The following table explains the values you can input with the `interface-group` commands.

**Table 51** interface-group Command Input Values

| LABEL | DESCRIPTION |
|---|---|
| *group-name* | A descriptive name for the trunk.<br><br>For the ZyWALL / USG USG 300 and above, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.<br><br>~~The ZyWALL / USG USG 200 and lower models use WAN_TRUNK or WAN_TRUNK2-5.~~ |
| *interface-name* | The name of an interface, it could be an Ethernet, PPP, VLAN or bridge interface. The possible number of each interface type and the abbreviation to use are as follows.<br><br>Ethernet interface: For the ZyWALL / USG USG 300 and above, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model.<br><br>~~The~~Some ZyWALL / USG ~~USG 200 and lower~~ models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.<br><br>PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL / USG model supports.<br><br>VLAN interface: vlan*x*, *x* = 0 - 4094<br><br>bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ZyWALL / USG model supports. |
| *num* | The interface's position in the trunk's list of members `<1..8>`. |
| `<CR>` | Carriage Return (the "enter" key). |

# 9.4 Trunk Commands Summary

The following table lists the `interface-group` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands. See Table 51 on page 114 for details about the values you can input with these commands.

**Table 52** interface-group Commands Summary

| COMMAND | DESCRIPTION |
|---|---|
| `show interface-group {system-default\|user-define\|`*group-name*`}` | Displays pre-configured system default trunks, your own user configuration trunks or a specified trunk's settings. |
| `[no] interface-group` *group-name* | Creates a trunk name and enters the trunk sub-command mode where you can configure the trunk. The `no` command removes the trunk. |
| `algorithm {wrr\|llf\|spill-over}` | Sets the trunk's load balancing algorithm. |
| `exit` | Leaves the trunk sub-command mode. |
| `flush` | Deletes a trunk's interface settings. |
| `interface {`*num*`\|append\|insert` *num*`}` *interface-name* `[weight <1..10>\|limit <1..2097152>\|passive]` | This subcommand adds an interface to a trunk. Sets the interface's number. It also sets the interface's weight and spillover limit or sets it to be passive. |

**Table 52** interface-group Commands Summary (continued)

| COMMAND | DESCRIPTION |
|---|---|
| loadbalancing-index <inbound\|outbound\|total> | Use this command only if you use least load first or spill-over as the trunk's load balancing algorithm.<br>Set either inbound, outbound, or total (outbound and inbound) traffic to which the ZyWALL / USG will apply the specified algorithm. Outbound traffic means the traffic travelling from an internal interface (ex. LAN) to an external interface (ex. WAN). Inbound traffic means the opposite. |
| mode {normal\|trunk} | Sets the mode for a trunk. Do this first in the trunk's sub-command mode. |
| move <1..8> to <1..8> | Changes a the interface order in a trunk. |
| [no] interface {*num*\|*interface-name*} | Removes an interface from the trunk. |
| system default-interface-group *group-name* | Sets the ZyWALL / USG to first attempt to use the the specified WAN trunk. |
| [no] system default-snat | Enables or disables Source NAT (SNAT). When SNAT is enabled, the ZyWALL / USG uses the IP address of the outgoing interface as the source IP address of the packets it sends out through the WAN interfaces. |
| show system default-snat | Displays whether the ZyWALL / USG enable SNAT or not. The ZyWALL / USG performs SNAT by default for traffic going to or from the WAN interfaces. |
| show system default-interface-group | Displays the WAN trunk the ZyWALL / USG first attempts to use. |

# 9.5 Trunk Command Examples

The following example creates a weighted round robin trunk for Ethernet interfaces ge1 and ge2. The ZyWALL / USG sends twice as much traffic through ge1.

```
Router# configure terminal
Router(config)# interface-group wrr-example
Router(if-group)# mode trunk
Router(if-group)# algorithm wrr
Router(if-group)# interface 1 ge1 weight 2
Router(if-group)# interface 2 ge2 weight 1
Router(if-group)# exit
Router(config)#
```

The following example creates a least load first trunk for Ethernet interface ge3 and VLAN 5, which will only apply to outgoing traffic through the trunk. The ZyWALL / USG sends new session traffic through the least utilized of these interfaces.

```
Router# configure terminal
Router(config)# interface-group llf-example
Router(if-group)# mode trunk
Router(if-group)# algorithm llf
Router(if-group)# interface 1 ge3
Router(if-group)# interface 2 vlan5
Router(if-group)# loadbalancing-index outbound
Router(if-group)# exit
Router(config)#
```

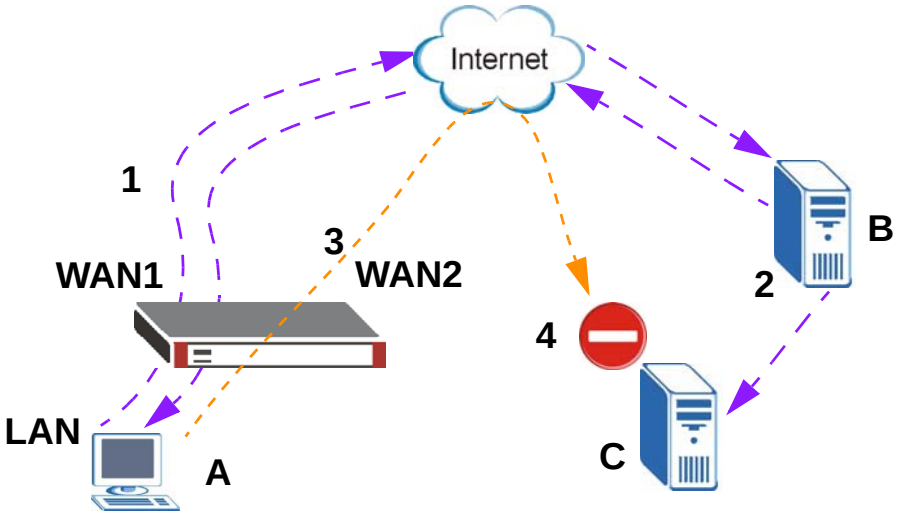
The following example creates a spill-over trunk for Ethernet interfaces ge1 and ge3, which will apply to both incoming and outgoing traffic through the trunk.. The ZyWALL / USG sends traffic through ge1 until it hits the limit of 1000 kbps. The ZyWALL / USG sends anything over 1000 kbps through ge3.

```
Router# configure terminal
Router(config)# interface-group spill-example
Router(if-group)# mode trunk
Router(if-group)# algorithm spill-over
Router(if-group)# interface 1 ge1 limit 1000
Router(if-group)# interface 2 ge3 limit 1000
Router(if-group)# loadbalancing-index total
Router(if-group)# exit
Router(config)#
```

# 9.6 Link Sticking

You can have the ZyWALL / USG send each local computer's traffic through a single WAN interface for a specified period of time. This is useful when a redirect server forwards a user request for a file and informs the file server that a particular WAN IP address is requesting the file. If the user's subsequent sessions came from a different WAN IP address, the file server would deny the request. Here is an example.

**Figure 14** Link Sticking




1 LAN user **A** tries to download a file from server **B** on the Internet. The ZyWALL / USG uses WAN1 to send the request to server **B**.

2 However remote server **B** is actually a redirect server. So server **B** sends a file list to LAN user **A**. The file list lets LAN user **A**'s computer know that the desired file is actually on file server (**C**). At the same time, register server **B** informs file server **C** that a computer located at the WAN1's IP address will download a file.

3 The ZyWALL / USG is using active/active load balancing. So when LAN user **A** tries to retrieve the file from file server **C**, the request goes out through WAN2.

4 File server **C** finds that the request comes from WAN2's IP address instead of WAN1's IP address and rejects the request.

5 If link sticking had been configured, the ZyWALL / USG would have still used WAN1 to send LAN user **A**'s request to file server **C** and the file server would have given the file to **A**.

# 9.7 Link Sticking Commands Summary

The following table lists the `ip load-balancing link-sticking` commands for link sticking. (The link sticking commands have the prefix `ip load-balancing` because they affect the ZyWALL / USG's load balancing behavior.) You must use the `configure terminal` command to enter the configuration mode before you can use these commands. See Table 51 on page 114 for details about the values you can input with these commands.

**Table 53** ip load-balancing link-sticking Commands Summary

| COMMAND | DESCRIPTION |
|---|---|
| `[no] ip load-balancing link-sticking activate` | Turns link sticking on or off. |
| `[no] ip load-balancing link-sticking timeout` *timeout* | Sets for how many seconds (30-3600) the ZyWALL / USG sends all of each local computer's traffic through one WAN interface. |
| `show ip load-balancing link-sticking status` | Displays the current link sticking settings. |

# 9.8 Link Sticking Command Example

This example shows how to activate link sticking and set the timeout to 600 seconds (ten minutes).

```
Router(config)# ip load-balancing link-sticking activate
Router(config)# ip load-balancing link-sticking timeout 600
Router(config)# show ip load-balancing link-sticking status
active     : yes
timeout    : 300
```

# 10

# Route

This chapter shows you how to configure policies for IP routing and static routes on your ZyWALL / USG.

## 10.1 Policy Route

Traditionally, routing is based on the destination address only and the ZyWALL / USG takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

## 10.2 Policy Route Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 54** Input Values for General Policy Route Commands

| LABEL | DESCRIPTION |
|---|---|
| *address_object* | The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *address6_object* | The name of the IPv6 address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |

**Table 54** Input Values for General Policy Route Commands (continued)

| LABEL | DESCRIPTION |
|---|---|
| *interface_name* | The name of the interface.<br>Ethernet interface: For the ZyWALL / USG USG 300 and above, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model.<br>~~The~~Some ZyWALL / USG ~~USG 200 and lower~~ models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.<br>virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4<br>VLAN interface: vlan*x*, *x* = 0 - 4094<br>virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 12<br>bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ZyWALL / USG model supports.<br>virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4<br>PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL / USG model supports. |
| *policy_number* | The number of a policy route. 1 - *X* where *X* is the highest number of policy routes the ZyWALL / USG model supports. See the ZyWALL / USG's User's Guide for details. |
| *schedule_object* | The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *service_name* | The name of the service (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *user_name* | The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *destv6* | The IPv6 route prefix (subnet address) for the destination. |
| *prefix* | The IPv6 prefix length, 0 - 128. |
| *gatewayv6* | The IPv6 address of the specified gateway. |
| *ipv6_addr* | An IPv6 address. |
| *ipv6_global_address* | An IPv6 address excluding the link-local address (fe80::). |
| *ipv6_link_local* | An fe80:: IPv6 address. |

The following table describes the commands available for policy route. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 55** Command Summary: Policy Route

| COMMAND | DESCRIPTION |
|---|---|
| `[no] bwm activate` | Globally enables bandwidth management. You must globally activate bandwidth management to have individual policy routes or application patrol policies apply bandwidth management. The `no` command globally disables bandwidth management. |
| `policy {`*`policy_number`*` \| append \| insert `*`policy_number`*`}` | Enters the policy-route sub-command mode to configure, add or insert a policy. |

**Table 55** Command Summary: Policy Route (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] auto-destination | When you set tunnel as the next-hop type (using the next-hop tunnel command) for this route, you can use this command to have the ZyWALL / USG use the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy instead of what you configure by using the destination command. The no command disables the setting. |
| [no] auto-disable | When you set interface or trunk as the next-hop type (using the next-hop interface or next-hop trunk command) for this route, you can use this command to have the ZyWALL / USG automatically disable this policy route when the next-hop's connection is down. The no command disables the setting. |
| [no] bandwidth <1..1048576> priority <1..1024> [maximize-bandwidth-usage] | Sets the maximum bandwidth and priority for the policy. The no command removes bandwidth settings from the rule. You can also turn maximize bandwidth usage on or off. |
| [no] deactivate | Disables the specified policy. The no command enables the specified policy. |
| [no] description *description* | Sets a descriptive name for the policy. The no command removes the name for the policy. |
| [no] destination {*address_object*\|any} | Sets the destination IP address the matched packets must have. The no command resets the destination IP address to the default (any). any means all IP addresses. |
| [no] dscp {any \| <0..63>} | Sets a custom DSCP code point (0~63). This is the DSCP value of incoming packets to which this policy route applies. any means all DSCP value or no DSCP marker. |
| [no] dscp class {default \| *dscp_class*} | Sets a DSCP class. Use default to apply this policy route to incoming packets that are marked with DSCP value 0. Use one of the pre-defined AF classes (including af11~af13, af21~af23, af31~af33, and af41~af43) to apply this policy route to incoming packets that are marked with the DSCP AF class.<br><br>The "af" entries stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 124 for more details. |
| dscp-marking <0..63> | Sets a DSCP value to have the ZyWALL / USG apply that DSCP value to the route's outgoing packets. |
| dscp-marking class {default \| *dscp_class*} | Sets how the ZyWALL / USG handles the DSCP value of the outgoing packets that match this route. Set this to default to have the ZyWALL / USG set the DSCP value of the packets to 0. Set this to an "af" class (including af11~af13, af21~af23, af31~af33, and af41~af43) which stands for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 124 for more details. |
| no dscp-marking | Use this command to have the ZyWALL / USG not modify the DSCP value of the route's outgoing packets. |
| exit | Leaves the sub-command mode. |
| [no] interface *interface_name* | Sets the interface on which the incoming packets are received. The no command resets the incoming interface to the default (any). any means all interfaces. |
| [no] next-hop {auto\|gateway *address object* \|interface *interface_name* \|trunk *trunk_name*\|tunnel *tunnel_name*} | Sets the next-hop to which the matched packets are routed. The no command resets next-hop settings to the default (auto). |

**Table 55** Command Summary: Policy Route (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] schedule *schedule_object* | Sets the schedule. The no command removes the schedule setting to the default (none). none means any time. |
| [no] service {*service_name*\|any} | Sets the IP protocol. The no command resets service settings to the default (any). any means all services. |
| [no] snat {outgoing-interface\|pool {*address_object*}} | Sets the source IP address of the matched packets that use SNAT. The no command removes source NAT settings from the rule. |
| [no] source {*address_object*\|any} | Sets the source IP address that the matched packets must have. The no command resets the source IP address to the default (any). any means all IP addresses. |
| [no] sslvpn *tunnel_name* | Sets the incoming interface to an SSL VPN tunnel. The no command removes the SSL VPN tunnel through which the incoming packets are received. |
| ~~[no] trigger <1..8> incoming *service_name* trigger *service_name*~~ | ~~Sets a port triggering rule. The no command removes port trigger settings from the rule.~~ |
| ~~trigger append incoming *service_name* trigger *service_name*~~ | ~~Adds a new port triggering rule to the end of the list.~~ |
| ~~trigger delete <1..8>~~ | ~~Removes a port triggering rule.~~ |
| ~~trigger insert <1..8> incoming *service_name* trigger *service_name*~~ | ~~Adds a new port triggering rule before the specified number.~~ |
| ~~trigger move <1..8> to <1..8>~~ | ~~Moves a port triggering rule to the number that you specified.~~ |
| [no] tunnel *tunnel_name* | Sets the incoming interface to an IPSec VPN tunnel. The no command removes the IPSec VPN tunnel through which the incoming packets are received. |
| [no] user *user_name* | Sets the user name. The no command resets the user name to the default (any). any means all users. |
| policy6 {*policy_number* \| append \| insert *policy_number*} | Enters the IPv6 policy-route sub-command mode to configure, add or insert a policy. |
| [no] bandwidth <1..1048576> priority <1..1024> [maximize-bandwidth-usage] | Sets the maximum bandwidth and priority for the policy. The no command removes bandwidth settings from the rule. You can also turn maximize bandwidth usage on or off. |
| [no] deactivate | Disables the specified policy. The no command enables the specified policy. |
| [no] description *description* | Sets a descriptive name for the IPv6 policy. The no command removes the name for the policy. |
| [no] destination {*address6_object*\|any} | Sets the destination IPv6 IP address the matched packets must have. The no command resets the destination IP address to the default (any). any means all IP addresses. |
| [no] dscp {any \| <0..63>} | Sets a custom DSCP code point (0~63). This is the DSCP value of incoming packets to which this policy route applies. any means all DSCP value or no DSCP marker. |
| [no] dscp class {default \| *dscp_class*} | Sets a DSCP class. Use default to apply this policy route to incoming packets that are marked with DSCP value 0. Use one of the pre-defined AF classes (including af11~af13, af21~af23, af31~af33, and af41~af43) to apply this policy route to incoming packets that are marked with the DSCP AF class.<br><br>The "af" entries stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 124 for more details. |
| dscp-marking <0..63> | Sets a DSCP value to have the ZyWALL / USG apply that DSCP value to the route's outgoing packets. |

**Table 55** Command Summary: Policy Route (continued)

| COMMAND | DESCRIPTION |
|---|---|
| dscp-marking class {default \| *dscp_class*} | Sets how the ZyWALL / USG handles the DSCP value of the outgoing packets that match this route. Set this to default to have the ZyWALL / USG set the DSCP value of the packets to 0. Set this to an "af" class (including af11~af13, af21~af23, af31~af33, and af41~af43) which stands for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 124 for more details. |
| no dscp-marking | Use this command to have the ZyWALL / USG not modify the DSCP value of the route's outgoing packets. |
| exit | Leaves the sub-command mode. |
| [no] interface *interface_name* | Sets the interface on which the matched packets are received. The no command resets the incoming interface to the default (any). any means all interfaces. |
| [no] next-hop {auto\|gateway *gatewayv6* \|interface *interface_name* \|trunk *trunk_name*\|tunnel *tunnel_name*} | Sets the next-hop to which the matched packets are routed. The no command resets next-hop settings to the default (auto). |
| [no] schedule *schedule_object* | Sets the schedule. The no command removes the schedule setting to the default (none). none means any time. |
| [no] service {*service_name*\|any} | Sets the IP protocol. The no command resets service settings to the default (any). any means all services. |
| [no] source {*address6_object*\|any} | Sets the source IPv6 IP address that the matched packets must have. The no command resets the source IP address to the default (any). any means all IP addresses. |
| [no] user *user_name* | Sets the user name. The no command resets the user name to the default (any). any means all users. |
| [no] policy controll-ipsec-dynamic-rules activate | Enables the ZyWALL / USG to use policy routes to manually specify the destination addresses of dynamic IPSec rules. You must manually create these policy routes. The ZyWALL / USG automatically obtains source and destination addresses for dynamic IPSec rules that do not match any of the policy routes.<br>The no command has the ZyWALL / USG automatically obtain source and destination addresses for all dynamic IPSec rules. |
| policy default-route | Enters the policy-route sub-command mode to set a route with the name "default-route". |
| policy delete *policy_number* | Removes a routing policy. |
| policy flush | Clears the policy routing table. |
| policy list table | Displays all policy route settings. |
| policy move *policy_number* to *policy_number* | Moves a routing policy to the number that you specified. |
| [no] policy override-direct-route activate | Has the ZyWALL / USG forward packets that match a policy route according to the policy route instead of sending the packets to a directly connected network. Use the no command to disable it. |
| [no] policy controll-virtual-server-rules activate | Gives policy routes priority over NAT virtual server rules (1-1 SNAT). Use the no command to give NAT virtual server rules priority over policy routes. |
| [no] policy6 override-direct-route activate | Has the ZyWALL / USG forward IPv6 packets that match a policy route according to the policy route instead of sending the packets to a directly connected network. Use the no command to disable it. |
| show bwm activation | Displays whether or not the global setting for bandwidth management on the ZyWALL / USG is enabled. |

**Table 55** Command Summary: Policy Route (continued)

| COMMAND | DESCRIPTION |
|---|---|
| `show bwm-usage < [policy-route` *`policy_number`*`] \| [interface` *`interface_name`*`]` | Displays the specified policy route or interface's bandwidth allotment, current bandwidth usage, and bandwidth usage statistics. |
| `show policy-route [`*`policy_number`*`]` | Displays all or specified policy route settings. |
| `show policy-route begin <1..200> end <1..200>` | Displays the specified range of policy route settings. |
| `show policy-route controll-ipsec-dynamic-rules` | Displays whether the ZyWALL / USG checks policy routes first before IPSec dynamic rules. |
| `show policy-route override-direct-route` | Displays whether or not the ZyWALL / USG forwards packets that match a policy route according to the policy route instead of sending the packets to a directly connected network. |
| `show policy-route controll-virtual-server-rules` | Displays whether or not policy routes have priority over NAT virtual server rules (1-1 SNAT). |
| `show policy-route6 override-direct-route` | Displays whether or not the ZyWALL / USG forwards IPv6 packets that match a policy route according to the policy route instead of sending the packets to a directly connected network. |
| `show policy-route rule_count` | Displays the number of policy routes that have been configured on the ZyWALL / USG. |
| `show policy-route underlayer-rules` | Displays all policy route rule details for advanced debugging. |

## 10.2.1 Assured Forwarding (AF) PHB for DiffServ

Assured Forwarding (AF) behavior is defined in RFC 2597. The AF behavior group defines four AF classes. Inside each class, packets are given a high, medium or low drop precedence. The drop precedence determines the probability that routers in the network will drop packets when congestion occurs. If congestion occurs between classes, the traffic in the higher class (smaller numbered class) is generally given priority. Combining the classes and drop precedence produces the following twelve DSCP encodings from AF11 through AF43. The decimal equivalent is listed in brackets.

**Table 56** Assured Forwarding (AF) Behavior Group

| | CLASS 1 | CLASS 2 | CLASS 3 | CLASS 4 |
|---|---|---|---|---|
| Low Drop Precedence | AF11 (10) | AF21 (18) | AF31 (26) | AF41 (34) |
| Medium Drop Precedence | AF12 (12) | AF22 (20) | AF32 (28) | AF42 (36) |
| High Drop Precedence | AF13 (14) | AF23 (22) | AF33 (30) | AF43 (38) |

## 10.2.2 Policy Route Command Example

The following commands create two address objects (TW_SUBNET and GW_1) and insert a policy that routes the packets (with the source IP address TW_SUBNET and any destination IP address)

through the interface ge1 to the next-hop router GW_1. This route uses the IP address of the outgoing interface as the matched packets' source IP address.

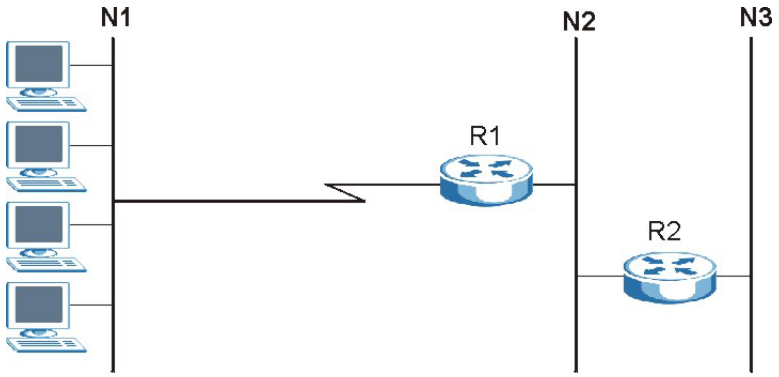
```
Router(config)# address-object TW_SUBNET 192.168.2.0 255.255.255.0
Router(config)# address-object GW_1 192.168.2.250
Router(config)# policy insert 1
Router(policy-route)# description example
Router(policy-route)# destination any
Router(policy-route)# interface ge1
Router(policy-route)# next-hop gateway GW_1
Router(policy-route)# snat outgoing-interface
Router(policy-route)# source TW_SUBNET
Router(policy-route)# exit
Router(config)# show policy-route 1
index: 1
  active: yes
  description: example
  user: any
  schedule: none
  interface: ge1
  tunnel: none
  sslvpn: none
  source: TW_SUBNET
  destination: any
  DSCP code: any
  service: any
  nexthop type: Gateway
  nexthop: GW_1
  nexthop state: Not support
  auto destination: no
  bandwidth: 0
  bandwidth priority: 0
  maximize bandwidth usage: no
  SNAT: outgoing-interface
  DSCP marking: preserve
  amount of port trigger: 0
Router(config)#
```

# 10.3 IP Static Route

The ZyWALL / USG has no knowledge of the networks beyond the network that is directly connected to the ZyWALL / USG. For instance, the ZyWALL / USG knows about network **N2** in the following figure through gateway **R1**. However, the ZyWALL / USG is unable to route a packet to network **N3** because it doesn't know that there is a route through the same gateway **R1** (via

gateway **R2**). The static routes are for you to tell the ZyWALL / USG about the networks beyond the network connected to the ZyWALL / USG directly.

**Figure 15** Example of Static Routing Topology




# 10.4 Static Route Commands

The following table describes the commands available for static route. You must use the `configure terminal` command to enter the configuration mode before you can use these commands. See Section Table 54 on page 119 for information on input values.

**Table 57** Command Summary: Static Route

| COMMAND | DESCRIPTION |
|---|---|
| `[no] ip route {w.x.y.z} {w.x.y.z} {interface\|w.x.y.z} <0..127>` | Sets a static route. The `no` command deletes a static route. |
| `ip route replace {w.x.y.z} {w.x.y.z} {interface\|w.x.y.z} <0..127> with {w.x.y.z} {w.x.y.z} {interface\|w.x.y.z} <0..127>` | Changes an existing route's settings. |
| `show ip route-settings` | Displays static route information. Use `show ip route` to see learned route information. See Section 11.2.5 on page 132. |
| `ip6 route destv6/prefix { ipv6_global_address \| ipv6_link_local \| interface} [<0..127>]` | Sets an IPv6 static route. |
| `ip6 route destv6/prefix { ipv6_link_local interface} [<0..127>]` | Sets an IPv6 link local static route. |
| `no ip6 route destv6/prefix { gatewayv6 \| interface} [<0..127>]` | Deletes the specified IPv6 static route. |
| `ip6 route replace destv6/prefix { gatewayv6 \| interface} [<0..127>] with destv6/prefix { gatewayv6 \| interface} [<0..127>]` | Changes an existing IPv6 route's settings. |
| `[no] ip route control-virtual-server-rules activate` | Gives static routes priority over NAT virtual server rules (1-1 SNAT). It also automatically gives policy routes priority over NAT virtual server rules. Use the `no` command to give NAT virtual server rules priority over static routes. |
| `show ip route control-virtual-server-rules` | Displays whether or not static routes have priority over NAT virtual server rules (1-1 SNAT). |

## 10.4.1 Static Route Commands Examples

The following command sets a static route with IP address 10.10.10.0 and subnet mask 255.255.255.0 and with the next-hop interface ge1. Then use the `show` command to display the setting.

```
Router(config)# ip route 10.10.10.0 255.255.255.0 ge1
Router(config)#
Router(config)# show ip route-settings
Route           Netmask         Nexthop         Metric
================================================================================
10.10.10.0      255.255.255.0   ge1             0
```

The following commands set and show three examples of static IPv6 routes for traffic destined for IPv6 addresses with prefix 2002:22:22:34::. The first route sends the traffic out through interface ge2 and uses metric 1. The second sends the traffic to gateway 2001:12::12 and uses metric 2. The third sends the traffic to the fe80::1:2 link local gateway on interface ge2 and uses metric 2.

```
Router(config)# ip6 route 2002:22:22:34::/64 ge2 1
Router(config)# ip6 route 2002:22:22:34::/64 2001:12::12 2
/* link-local gateway bind on interface */
Router(config)# ip6 route 2002:22:22:34::/64 fe80::1:2 ge2 2
Router(config)# show ip6 route-settings
No.  Route                                          Prefix Length
     Nexthop                                        Metric
================================================================================
1    2002:22:22:34::                                64
     2001:12::12                                    2
2    2002:22:22:34::                                64
     ge2                                            1
```

The following command deletes a specific static IPv6 route.

```
Router(config)# no ip6 route 2002:22:22:34::/64 2001:12::12
```

The following command deletes all static IPv6 routes with the same prefix.

```
Router(config)# no ip6 route 2002:22:22:34::/64
```

# 11

# Routing Protocol

This chapter describes how to set up RIP and OSPF routing protocols for the ZyWALL / USG.

## 11.1 Routing Protocol Overview

Routing protocols give the ZyWALL / USG routing information about the network from other routers. The ZyWALL / USG then stores this routing information in the routing table, which it uses when it makes routing decisions. In turn, the ZyWALL / USG can also provide routing information via routing protocols to other routers.

The ZyWALL / USG supports two standards, RIP and OSPF, for routing protocols. RIP and OSPF are compared in Table 58 on page 129, and they are discussed further in the next two sections.

**Table 58** OSPF vs. RIP

| | OSPF | RIP |
|---|---|---|
| Network Size | Large | Small (with up to 15 routers) |
| Metric | Bandwidth, hop count, throughput, round trip time and reliability. | Hop count |
| Convergence | Fast | Slow |

## 11.2 Routing Protocol Commands Summary

The following table describes the values required for many routing protocol commands. Other values are discussed with the corresponding commands.

**Table 59** Input Values for Routing Protocol Commands

| LABEL | DESCRIPTION |
|---|---|
| *ip* | The 32-bit name of the area or virtual link in IP address format. |
| *authkey* | The password for text or MD5 authentication. You may use alphanumeric characters or underscores(_).<br>text password: 1-8 characters long<br>MD5 password: 1-16 characters long |

The following sections list the routing protocol commands.

## 11.2.1 RIP Commands

This table lists the commands for RIP.

**Table 60** router Commands: RIP

| COMMAND | DESCRIPTION |
|---|---|
| router rip | Enters sub-command mode. |
| [no] network *interface_name* | Enables RIP on the specified Ethernet interface. The no command disables RIP on the specified interface. |
| [no] redistribute {static \| ospf} | Enables redistribution of routing information learned from the specified source. The no command disables redistribution from the specified source. |
| redistribute {static \| ospf} metric <0..16> | Sets the metric when redistributing routing information learned from the specified source. |
| [no] version <1..2> | Sets the default RIP version for all interfaces with RIP enabled. If the interface RIP version is blank, the interface uses the default version. This is not available in the GUI. The no command sets the default RIP version to 2. |
| [no] passive-interface *interface_name* | Sets the direction to "In-Only" for the specified interface. The no command sets the direction to bi-directional. |
| [no] authentication mode {md5 \| text} | Sets the authentication mode for RIP. The no command sets the authentication mode to "none". |
| [no] authentication string *authkey* | Sets the password for text authentication. The no command clears the password. |
| authentication key <1..255> key-string *authkey* | Sets the MD5 ID and password for MD5 authentication. |
| no authentication key | Clears the MD5 ID and password. |
| [no] outonly-interface *interface_name* | Sets the direction to "Out-Only" for the specified interface. The no command sets the direction to "BiDir". |

## 11.2.2 General OSPF Commands

This table lists the commands for general OSPF configuration.

**Table 61** router Commands: General OSPF Configuration

| COMMAND | DESCRIPTION |
|---|---|
| router ospf | Enters sub-command mode. |
| [no] redistribute {static \| rip} | Enables redistribution of routing information learned from the specified non-OSPF source. The no command disables redistribution from the specified non-OSPF source. |
| [no] redistribute {static \| rip} metric-type <1..2> metric <0..16777214> | Sets the metric for routing information learned from the specified non-OSPF source. The no command clears the metric. |
| [no] passive-interface *interface_name* | Sets the direction to "In-Only" for the specified interface. The no command sets the direction to "BiDir". |
| [no] router-id IP | Sets the 32-bit ID (in IP address format) of the ZyWALL / USG. The no command resets it to "default", or the highest available IP address. |

## 11.2.3 OSPF Area Commands

This table lists the commands for OSPF areas.

**Table 62** router Commands: OSPF Areas

| COMMAND | DESCRIPTION |
|---|---|
| router ospf | Enters sub-command mode. |
| [no] network *interface* area IP | Adds the specified interface to the specified area. The no command removes the specified interface from the specified area. |
| [no] area IP [{stub \| nssa}] | Creates the specified area and sets it to the indicated type. The no command removes the area. |
| [no] area IP authentication | Enables text authentication in the specified area. The no command disables authentication in the specified area. |
| [no] area IP authentication message-digest | Enables MD5 authentication in the specified area. The no command disables authentication in the specified area. |
| [no] area IP authentication authentication-key *authkey* | Sets the password for text authentication in the specified area. The no command clears the password. |
| [no] area IP authentication message-digest-key <1..255> md5 *authkey* | Sets the MD5 ID and password for MD5 authentication in the specified area. The no command clears the MD5 ID and password. |

## 11.2.4 Virtual Link Commands

This table lists the commands for virtual links in OSPF areas.

**Table 63** router Commands: Virtual Links in OSPF Areas

| COMMAND | DESCRIPTION |
|---|---|
| show ospf area IP virtual-link | Displays information about virtual links for the specified area. |
| router ospf | |
| [no] area IP virtual-link IP | Creates the specified virtual link in the specified area. The no command removes the specified virtual link. |
| [no] area IP virtual-link IP authentication | Enables text authentication in the specified virtual link. The no command disables authentication in the specified virtual link. |
| [no] area IP virtual-link IP authentication message-digest | Enables MD5 authentication in the specified virtual link. The no command disables authentication in the specified virtual link. |
| [no] area IP virtual-link IP authentication authentication-key *authkey* | Sets the password for text authentication in the specified virtual link. The no command clears the password in the specified virtual link. |
| [no] area IP virtual-link IP authentication message-digest-key <1..255> md5 *authkey* | Sets the MD5 ID and password for MD5 authentication in the specified virtual link. The no command clears the MD5 ID and password in the specified virtual link. |
| [no] area IP virtual-link IP authentication same-as-area | Sets the virtual link's authentication method to the area's default authentication. |
| [no] area IP virtual-link IP authentication-key *authkey* | Sets the password for text authentication in the specified virtual link. The no command clears the password. |
| area IP virtual-link IP message-digest-key <1..255> md5 *authkey* | Sets the MD5 ID and password for MD5 authentication in the specified virtual link. |
| no area IP virtual-link IP message-digest-key <1..255> | Clears the MD5 ID in the specified virtual link. |

## 11.2.5 Learned Routing Information Commands

This table lists the commands to look at learned routing information.

**Table 64** ip route Commands: Learned Routing Information

| COMMAND | DESCRIPTION |
|---|---|
| `show ip route [kernel \| connected \| static \| ospf \| rip \| bgp]` | Displays learned routing and other routing information. |

## 11.2.6 show ip route Command Example

The following example shows learned routing information on the ZyWALL / USG.

```
Router> show ip route
Flags: A - Activated route, S - Static route, C - directly Connected
       O - OSPF derived, R - RIP derived, G - selected Gateway
       ! - reject, B - Black hole, L - Loop

IP Address/Netmask    Gateway          IFace           Metric    Flags    Persist
=============================================================================
0.0.0.0/0             172.16.1.254     wan1            0         ASG      -
10.59.0.0/24          0.0.0.0          ext-wlan        0         ACG      -
127.0.0.0/8           0.0.0.0          lo              0         ACG      -
172.16.1.0/24         0.0.0.0          wan1            0         ACG      -
192.168.1.0/24        0.0.0.0          lan1            0         ACG      -
192.168.2.0/24        0.0.0.0          lan2            0         ACG      -
192.168.3.0/24        0.0.0.0          dmz             0         ACG      -
```

# 12

# Zones

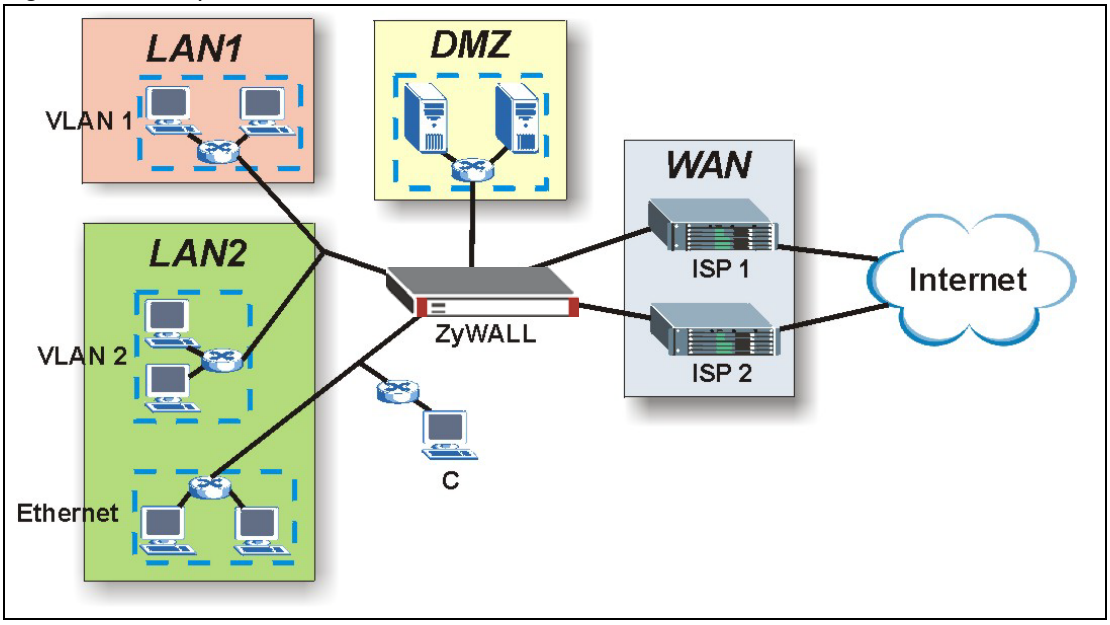
Set up zones to configure network security and network policies in the ZyWALL / USG.

## 12.1 Zones Overview

A zone is a group of interfaces and VPN tunnels. The ZyWALL / USG uses zones, not interfaces, in many security and policy settings, such as firewall rules and remote management.

Zones cannot overlap. Each Ethernet interface, VLAN interface, bridge interface, PPPoE/PPTP interface, auxiliary interface, and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

**Figure 16** Example: Zones



# 12.2 Zone Commands Summary

The following table describes the values required for many zone commands. Other values are discussed with the corresponding commands.s

**Table 65** Input Values for Zone Commands

| LABEL | DESCRIPTION |
|---|---|
| *profile_name* | The name of a zone, or the name of a VPN tunnel.<br><br>For ~~the~~some ZyWALL / USG models ~~USG 300 and above,~~ use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.<br><br>~~About the pre-defined zones in the~~ For other ZyWALL / USG ~~USG 200 and below~~ models:<br><br>• The lan1 interface always belongs to the LAN1 zone.<br>• The lan2 interface always belongs to the LAN2 zone.<br>• The dmz interface always belongs to the DMZ zone.<br>• The wan1, wan2, wan1_ppp, or wan2_ppp interfaces always belong to the WAN zone.<br>• An opt_ppp interface can be added to the WAN or OPT zone. |

This table lists the zone commands.

**Table 66** zone Commands

| COMMAND | DESCRIPTION |
|---|---|
| `show zone [`*`profile_name`*`]` | Displays information about the specified zone or about all zones. |
| `show zone binding-iface` | Displays each interface and zone mappings. |
| `show zone default-binding` | Displays the pre-configured interface and zone mappings that come with the ZyWALL / USG. |
| `show zone none-binding` | Displays the interfaces, tunnels and SSL VPNs that are not associated with a zone yet. |
| `show zone system-default` | Displays the pre-configured default zones that you cannot delete from the ZyWALL / USG. |
| `show zone user-define` | Displays all customized zones. |
| `[no] zone` *`profile_name`* | Creates the zone if necessary and enters sub-command mode. The `no` command deletes the zone. |
| `zone` *`profile_name`* | Enter the sub-command mode. |
| `[no] block` | Blocks intra-zone traffic. The `no` command allows intra-zone traffic. |
| `[no] interface` *`interface_name`* | Adds the specified interface to the specified zone. The `no` command removes the specified interface from the specified zone. See Section 8.2 on page 73 for information about interface names. |
| `[no] crypto` *`profile_name`* | Adds the specified IPSec VPN tunnel to the specified zone. The `no` command removes the specified IPSec VPN tunnel from the specified zone. |
| `[no] sslvpn` *`profile_name`* | Adds the specified SSL VPN tunnel to the specified zone. The `no` command removes the specified SSL VPN tunnel from the specified zone. |

## 12.2.1 Zone Command Examples

The following commands add Ethernet interfaces ge1 and ge2 to zone A and block intra-zone traffic.

```
Router# configure terminal
Router(config)# zone A
Router(zone)# interface ge1
Router(zone)# interface ge2
Router(zone)# block
Router(zone)# exit
Router(config)# show zone
No. Name                            Block  Member
================================================================================
1   A                               yes    ge1,ge2
Router(config)# show zone A
blocking intra-zone traffic: yes
No. Type                            Member
================================================================================
1   interface                       ge1
2   interface                       ge2
```

# 13

# DDNS

This chapter describes how to configure dynamic DNS (DDNS) services for the ZyWALL / USG.

## 13.1 DDNS Overview

DNS maps a domain name to a corresponding IP address and vice versa. Similarly, dynamic DNS maps a domain name to a dynamic IP address. As a result, anyone can use the domain name to contact you (in NetMeeting, CU-SeeMe, etc.) or to access your FTP server or Web site, regardless of the current IP address.

Note: You must have a public WAN IP address to use Dynamic DNS.

Set up a dynamic DNS account with a supported DNS service provider to be able to use Dynamic DNS services with the ZyWALL / USG. When registration is complete, the DNS service provider gives you a password or key. At the time of writing, the ZyWALL / USG supports the following DNS service providers. See the listed websites for details about the DNS services offered by each.

**Table 67** Network > DDNS

| DDNS SERVICE PROVIDER | SERVICE TYPES SUPPORTED | WEBSITE | NOTES |
|---|---|---|---|
| DynDNS | Dynamic DNS, Static DNS, and Custom DNS | www.dyndns.com) | |
| Dynu | Basic, Premium | www.dynu.com | |
| No-IP | No-IP | www.no-ip.com | |
| Peanut Hull | Peanut Hull | www.oray.cn | Chinese website |
| 3322 | DynamicDNS, StaticDNS | www.3322.org | Chinese website |
| Selfhost | Selfhost | selfhoost.de | German website |

Note: Record your DDNS account's user name, password, and domain name to use to configure the ZyWALL / USG.

After, you configure the ZyWALL / USG, it automatically sends updated IP addresses to the DDNS service provider, which helps redirect traffic accordingly.

# 13.2 DDNS Commands Summary

The following table describes the values required for many DDNS commands. Other values are discussed with the corresponding commands.

**Table 68** Input Values for DDNS Commands

| LABEL | DESCRIPTION |
|---|---|
| *profile_name* | The name of the DDNS profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |

The following table lists the DDNS commands.

**Table 69** ip ddns Commands

| COMMAND | DESCRIPTION |
|---|---|
| show ddns [*profile_name*] | Displays information about the specified DDNS profile or about all DDNS profiles. |
| show ddns-status | Shows which DDNS profiles are active, inactive or have failed. |
| [no] ip ddns profile *profile_name* | Creates or edits the specified DDNS profile ~~if necessary~~ and enters sub-command mode if necessary. The no command deletes ~~it~~this profile. |
| [no]https activate | Encrypts traffic using SSL (port 443) to the DDNS server. Not all DDNS providers support this option. The no command disables HTTPS. |
| [no] service-type {dyndns \| dyndns_static \| dyndns_custom \| dynu-basic \| dynu-premium \| no-ip \| peanut-hull \| 3322-dyn \| 3322-static \| Selfhost \| User custom} | Sets the service type in the specified DDNS profile. The no command clears it. |
| [no] username *username* password *password* | Sets the username and password in the specified DDNS profile. The no command clears these fields.<br>*username*: You can use up to 31 alphanumeric characters and the underscore (_).<br>*password*: You can use up to 64 alphanumeric characters and the underscore (_). |
| [no] host *hostname* | Sets the domain name in the specified DDNS profile. The no command clears the domain name.<br>*hostname*: You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character must be alphanumeric. |
| [no] ip-select {iface \| auto \| custom} | Sets the IP address update policy in the specified DDNS profile. The no command clears the policy. |
| [no] ip-select-backup {iface \| auto \| custom} | Sets the alternate IP address update policy in the specified DDNS profile. The no command clears the policy. |
| [no] custom *ip* | Sets the static IP address in the specified DDNS profile. The no command clears it. |
| [no] backup-custom *ip* | Sets the static IP address for the backup interface in the specified DDNS profile. The no command clears it. |

**Table 69** ip ddns Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] mx {*ip* \| *domain_name*} | Enables the mail exchanger and sets the fully-qualified domain name of the mail server to which mail from this domain name is forwarded. The no command disables the mail exchanger.<br>*domain_name*: You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character must be alphanumeric. |
| [no] wan-iface *interface_name* | Sets the WAN interface in the specified DDNS profile. The no command clears it. |
| [no] backup-iface *interface_name* | Sets the backup WAN interface in the specified DDNS profile. The no command clears it. |
| [no] ha-iface *interface_name* | Sets the HA interface in the specified DDNS profile. The no command clears it. |
| [no] backmx | Enables the backup mail exchanger. The no command disables it. |
| [no] wildcard | Enables the wildcard feature. The no command disables it. |
| [no] additional-ddns-options | Avaialable for User custom. Enter one ofg the following.<br>• --ip server name which should be the URL to get the server's public IP address - for example, http://myip.easylife.tw/<br>• --dyndns system to specify the DYNDNS Server type - for example, dyndns@dyndns.org |

## 13.3 DDNS Commands Example

The following example sets up a DDNS profile where the interface is wan1 and uses HTTP..

```
Router# configure terminal
Router(config)# ip ddns profile bbb
# activate
# service-type user-custom
# username yjyeh001 password xxxxxx
# host yjye007.dyndns.org
# wan-iface wan1
# url /nic/update?
# ddns-server members.dyndns.org
# additional-ddns-options --dyndns_system dyndns@dyndns.org
```

# 14

# Virtual Servers

This chapter describes how to set up, manage, and remove virtual servers. Virtual server commands configure NAT.

## 14.1 Virtual Server Overview

Virtual server is also known as port forwarding or port translation.

Virtual servers are computers on a private network behind the ZyWALL / USG that you want to make available outside the private network. If the ZyWALL / USG has only one public IP address, you can make the computers in the private network available by using ports to forward packets to the appropriate private IP address.

### 14.1.1 1:1 NAT and Many 1:1 NAT

1:1 NAT - If the private network server will initiate sessions to the outside clients, use 1:1 NAT to have the ZyWALL / USG translate the source IP address of the server's outgoing traffic to the same public IP address that the outside clients use to access the server.

Many 1:1 NAT - If you have a range of private network servers that will initiate sessions to the outside clients and a range of public IP addresses, use many 1:1 NAT to have the ZyWALL / USG translate the source IP address of each server's outgoing traffic to the same one of the public IP addresses that the outside clients use to access the server. The private and public ranges must have the same number of IP addresses.

One many 1:1 NAT rule works like multiple 1:1 NAT rules, but it eases the configuration effort since you only create one rule.

## 14.2 Virtual Server Commands Summary

The following table describes the values required for many virtual server commands. Other values are discussed with the corresponding commands.

**Table 70** Input Values for Virtual Server Commands

| LABEL | DESCRIPTION |
|---|---|
| *service_object* | The name of a service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *profile_name* | The name of the virtual server. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |

The following table lists the virtual server commands.

**Table 71** ip virtual-server Commands

| COMMAND | DESCRIPTION |
|---|---|
| `show ip virtual-server [profile_name]` | Displays information about the specified virtual server or about all the virtual servers. |
| `no ip virtual-server profile_name` | Deletes the specified virtual server. |
| `ip virtual-server profile_name interface interface_name original-ip {any \| ip \| address_object} map-to {address_object \| ip} map-type any [nat-loopback [nat-1-1-map] [deactivate] \| nat-1-1-map [deactivate] \| deactivate]` | Creates or modifies the specified virtual server and maps the specified destination IP address (for all destination ports) to the specified destination address object or IP address. The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (*address-object*). NAT loopback allows local users to use a domain name to access this virtual server.<br><br>Select what kind of NAT this rule is to perform.<br><br>`nat-1-1-map`: means the NAT type is either 1:1 NAT or many 1:1 NAT. See Section 14.1.1 on page 141 for more information.<br><br>Using this command without `nat-1-1-map` means the NAT type is Virtual Server. This makes computers on a private network behind the ZyWALL / USG available to a public network outside the ZyWALL / USG (like the Internet).<br><br>The `deactivate` command disables the virtual server rule. |
| `ip virtual-server profile_name interface interface_name original-ip {any \| IP \| address_object} map-to {address_object \| ip} map-type port protocol {any \| tcp \| udp} original-port <1..65535> mapped-port <1..65535> [nat-loopback [nat-1-1-map] [deactivate] \| nat-1-1-map [deactivate] \| deactivate]` | Creates or modifies the specified virtual server and maps the specified (destination IP address, protocol, and destination port) to the specified (destination IP address and destination port). The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (*address-object*). NAT loopback allows local users to use a domain name to access this virtual server.<br><br>`nat-1-1-map`: means the NAT type is either 1:1 NAT or many 1:1 NAT. See Section 14.1.1 on page 141 for more information.<br><br>Using this command without `nat-1-1-map` means the NAT type is Virtual Server. This makes computers on a private network behind the ZyWALL / USG available to a public network outside the ZyWALL / USG (like the Internet).<br><br>The `deactivate` command disables the virtual server rule. |
| `ip virtual-server profile_name interface interface_name original-ip {any \| IP \| address_object} map-to {address_object \| ip} map-type ports protocol {any \| tcp \| udp} original-port-begin <1..65535> original-port-end <1..65535> mapped-port-begin <1..65535> [nat-loopback [nat-1-1-map] [deactivate] \| nat-1-1-map [deactivate] \| deactivate]` | Creates or modifies the specified virtual server and maps the specified (destination IP address, protocol, and range of destination ports) to the specified (destination IP address and range of destination ports). The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (*address-object*). NAT loopback allows local users to use a domain name to access this virtual server.<br><br>`nat-1-1-map`: means the NAT type is either 1:1 NAT or many 1:1 NAT. See Section 14.1.1 on page 141 for more information.<br><br>Using this command without `nat-1-1-map` means the NAT type is Virtual Server. This makes computers on a private network behind the ZyWALL / USG available to a public network outside the ZyWALL / USG (like the Internet).<br><br>The `deactivate` command disables the virtual server rule. |

**Table 71** ip virtual-server Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| ip virtual-server *profile_name* interface *interface_name* original-ip {any \| IP \| *address_object*} map-to {*address_object* \| *ip*} map-type original-service *service_object* mapped-service *service_object* [nat-loopback [nat-1-1-map] [deactivate] \| nat-1-1-map [deactivate] \| deactivate] | Creates or modifies the specified virtual server and maps the specified (destination IP address, protocol, and service object) to the specified (destination IP address and service object). The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (*address-object*). NAT loopback allows local users to use a domain name to access this virtual server.<br><br>nat-1-1-map: means the NAT type is either 1:1 NAT or many 1:1 NAT. See Section 14.1.1 on page 141 for more information.<br><br>Using this command without nat-1-1-map means the NAT type is Virtual Server. This makes computers on a private network behind the ZyWALL / USG available to a public network outside the ZyWALL / USG (like the Internet).<br><br>The deactivate command disables the virtual server rule. |
| ip virtual-server {activate \| deactivate} *profile_name* | Activates or deactivates the specified virtual server. |
| ip virtual-server delete *profile_name* | Deletes the specified virtual server. |
| ip virtual-server flush | Deletes all virtual servers. |
| ip virtual-server rename *profile_name* *profile_name* | Renames the specified virtual server from the first *profile_name* to the second *profile_name*. |

## 14.2.1 Virtual Server Command Examples

The following command creates virtual server WAN-LAN_H323 on the wan1 interface that maps IP addresses 10.0.0.8 to 192.168.1.56. for TCP protocol traffic on port 1720. It also adds a NAT loopback entry.

```
Router# configure terminal
Router(config)# ip virtual-server WAN-LAN_H323 interface wan1 original-ip 10.0.0.8
map-to 192.168.1.56 map-type port protocol tcp original-port 1720 mapped-port 1720
nat-loopback
Router(config)#
```

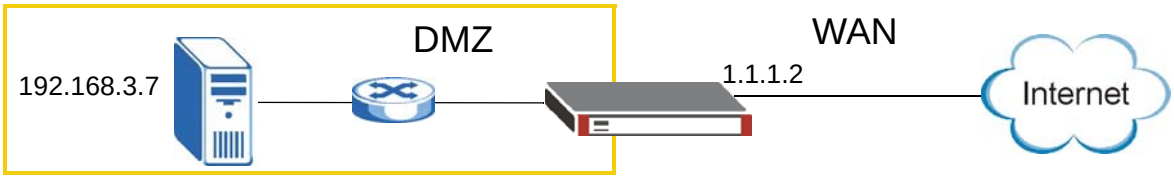
The following command shows information about all the virtual servers in the ZyWALL / USG.

```
Router(config)# show ip virtual-server
virtual server: WAN-LAN_H323
  active: yes
  interface: wan1
  NAT-loopback active: yes
  NAT 1-1: no
  original IP: 10.0.0.8
  mapped IP: 192.168.1.56
  mapping type: port
  protocol type: tcp
  original service:
  mapped service:
  original start port: 1720
  original end port:
  mapped start port: 1720
  mapped end port:
Router(config)#
```

## 14.2.2 Tutorial - How to Allow Public Access to a Server

This is an example of making an HTTP (web) server in the DMZ zone accessible from the Internet (the WAN zone). You will use a public IP address of 1.1.1.2 on the ge2 (or wan1 on ~~USG 200 and lower~~some models) interface and map it to the HTTP server's private IP address of 192.168.3.7.

**Figure 17** Public Server Example Network Topology




Follow the following steps for the setting.

**1** Configure Address object

Create two address objects. One is named DMZ_HTTP for the HTTP server's private IP address of 192.168.3.7. The other one is named ge2_HTTP for the ge2 (wan1) public IP address of 1.1.1.2.

```
Router# configure terminal
Router(config)# address-object DMZ_HTTP 192.168.3.7
Router(config)# address-object ge2_HTTP 1.1.1.2
Router(config)#
```

**2** Configure NAT

You need a NAT rule to send HTTP traffic coming to IP address 1.1.1.2 on ge2 (wan1) to the HTTP server's private IP address of 192.168.3.7. Use the following settings:

- This NAT rule is for any HTTP traffic coming in on ge2 (wan1) to IP address 1.1.1.2.
- The NAT rule sends this traffic to the HTTP server's private IP address of 192.168.3.7 (defined in the DMZ_HTTP object).
- HTTP traffic and the HTTP server in this example both use TCP port 80. So you set the port mapping type to "port", the protocol type to "TCP", and the original and mapped ports to "80".

```
Router(config)# ip virtual-server To-VirtualServer-WWW interface ge2 original-ip
ge2_HTTP map-to DMZ_HTTP map-type port protocol tcp original-port 80 mapped-port 80
Router(config)#
```

**3** Configure firewall

Create a firewall rule to allow HTTP traffic from the WAN zone to the DMZ web server.

```
Router(config)# firewall insert 1
Router(firewall)# description To-VirtualServer-WWW
Router(firewall)# from WAN
Router(firewall)# to DMZ
Router(firewall)# destinationip DMZ_HTTP
Router(firewall)# service HTTP
Router(firewall)# exit
Router(config)# write
Router(config)#
```

Now the public can go to IP address 1.1.1.2 to access the HTTP server.

# 15

# HTTP Redirect

This chapter shows you how to configure HTTP redirection on your ZyWALL / USG.

## 15.1 HTTP Redirect Overview

HTTP redirect forwards the client's HTTP request (except HTTP traffic destined for the ZyWALL / USG) to a web proxy server.

### 15.1.1 Web Proxy Server

A proxy server helps client devices make indirect requests to access the Internet or outside network resources/services. A proxy server can act as a firewall or an ALG (application layer gateway) between the private network and the Internet or other networks. It also keeps hackers from knowing internal IP addresses.

# 15.2 HTTP Redirect Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 72** Input Values for HTTP Redirect Commands

| LABEL | DESCRIPTION |
|---|---|
| *description* | The name to identify the rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *interface_name* | The name of the interface.<br><br>Ethernet interface: For ~~the~~some ZyWALL / USG ~~USG 300 and above,~~models use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model.<br><br>~~The~~For other ZyWALL / USG ~~USG 200 and lower~~ models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.<br><br>virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4<br><br>VLAN interface: vlan*x*, *x* = 0 - 4094<br><br>virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 4<br><br>bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ZyWALL / USG model supports.<br><br>virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4<br><br>PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL / USG model supports. |

The following table describes the commands available for HTTP redirection. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 73** Command Summary: HTTP Redirect

| COMMAND | DESCRIPTION |
|---|---|
| `ip http-redirect` *description* `interface` *interface_name* `redirect-to` *w.x.y.z* `<1..65535>` | Sets a HTTP redirect rule. |
| `ip http-redirect` *description* `interface` *interface_name* `redirect-to` *w.x.y.z* `<1..65535> deactivate` | Disables a HTTP redirect rule. |
| `ip http-redirect activate` *description* | Enables a rule with the specified rule name. |
| `ip http-redirect deactivate` *description* | Disables a rule with the specified rule name. |
| `no ip http-redirect` *description* | Removes a rule with the specified rule name. |
| `ip http-redirect flush` | Clears all HTTP redirect rules. |
| `show ip http-redirect [`*description*`]` | Displays HTTP redirect settings. |

## 15.2.1 HTTP Redirect Command Examples

The following commands create a HTTP redirect rule, disable it and display the settings.

```
Router# configure terminal
Router(config)# ip http-redirect example1 interface ge1 redirect-to 10.10.2.3 80
Router(config)# ip http-redirect example1 interface ge1 redirect-to 10.10.2.3 80
deactivate
Router(config)# show ip http-redirect
Name                            Interface    Proxy Server    Port    Active
================================================================================
example1                         ge1          10.10.2.3       80      no
```

# 16

# ALG

This chapter covers how to use the ZyWALL / USG's ALG feature to allow certain applications to pass through the ZyWALL / USG.

## 16.1 ALG Introduction

The ZyWALL / USG can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as SIP) to operate properly through the ZyWALL / USG's NAT.

Some applications cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload. The ZyWALL / USG examines and uses IP address and port number information embedded in the VoIP traffic's data stream. When a device behind the ZyWALL / USG uses an application for which the ZyWALL / USG has VoIP pass through enabled, the ZyWALL / USG translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and allows the related sessions to go through the firewall so the application's traffic can come in from the WAN to the LAN.

The ZyWALL / USG only needs to use the ALG feature for traffic that goes through the ZyWALL / USG's NAT. The firewall allows related sessions for VoIP applications that register with a server. The firewall allows or blocks peer to peer VoIP traffic based on the firewall rules.

You do not need to use a TURN (Traversal Using Relay NAT) server for VoIP devices behind the ZyWALL / USG when you enable the SIP ALG.

# 16.2 ALG Commands

The following table lists the `alg` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 74** alg Commands

| COMMAND | DESCRIPTION |
|---|---|
| [no] alg sip [default port <1..65535> \| direct-media \| direct-signalling \| inactivity-timeout ~~\| signal-port <1025..65535> \| signal-extra port <1025..65535>~~ \| media-timeout <1..86400> \| signal-timeout <1..86400> \| transformation] | Turns on or configures the ALG.<br>Use default port to add a custom UDP port number for SIP traffic.<br>Use direct-media to to set the ZyWALL / USG to allow SIP audio session.<br>Use direct-signalling to set the ZyWALL / USG to allow SIP signaling sessions.<br>Use inactivity-timeout to have the ZyWALL / USG apply SIP media and signaling inactivity time out limits.<br>~~Use signal port with a listening port number (1025 to 65535) if you are using SIP on a port other than UDP 5060.~~<br>~~Use signal extra port with a listening port number (1025 to 65535) if you are also using SIP on an additional UDP port number, enter it here.~~<br>Use media-timeout and a number of seconds (1~86400) for how long to allow a voice session to remain idle (without voice traffic) before dropping it.<br>Use signal-timeout and a number of seconds (1~86400) for how long to allow a SIP signaling session to remain idle (without SIP packets) before dropping it.<br>Use transformation to have the ZyWALL / USG modify IP addresses and port numbers embedded in the SIP data payload. You do not need to use this if you have a SIP device or server that will modify IP addresses and port numbers embedded in the SIP data payload.<br>The no command turns off the SIP ALG or removes the settings that you specify. |
| Router(SIP Signaling Port)# [no] port <1025..65535> | Enter the custom UDP port number for SIP traffic. The no command removes the custom UDP port number for SIP traffic. |
| [no] alg <h323 \| ftp> [signal-port <1025..65535> \| signal-extra-port <1025..65535> \| transformation] | Turns on or configures the H.323 or FTP ALG.<br>Use signal-port with a listening port number (1025 to 65535) if you are using H.323 on a TCP port other than 1720 or FTP on a TCP port other than 21.<br>Use signal-extra-port with a listening port number (1025 to 65535) if you are also using H.323 or FTP on an additional TCP port number, enter it here.<br>Use transformation to have the ZyWALL / USG modify IP addresses and port numbers embedded in the H.323 or FTP data payload. You do not need to use this if you have an H.323 or FTP device or server that will modify IP addresses and port numbers embedded in the H.323 or FTP data payload.<br>The no command turns off the H.323 or FTP ALG or removes the settings that you specify. |
| show alg <sip \| h323 \| ftp> | Displays the specified ALG's configuration. |

# 16.3 ALG Commands Example

The following example turns on pass through for SIP and turns it off for H.323.

```
Router# configure terminal
Router(config)# alg sip
Router(config)# no alg h323
```

# 17

# UPnP

## 17.1 UPnP and NAT-PMP Overview

The ZyWALL / USG supports both UPnP and NAT-PMP to permit networking devices to discover each other and connect seamlessly.

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. A gateway that supports UPnP is called Internet Gateway Device (IGD). The standardized Device Control Protocol (DCP) is defined by the UPnP Forum for IGDs to configure port mapping automatically.

NAT Port Mapping Protocol (NAT-PMP), introduced by Apple and implemented in current Apple products, is used as an alternative NAT traversal solution to the UPnP IGD protocol. NAT-PMP runs over UDP port 5351. NAT-PMP is much simpler than UPnP IGD and mainly designed for small home networks. It allows a client behind a NAT router to retrieve the router's public IP address and port number and make them known to the peer device with which it wants to communicate. The client can automatically configure the NAT router to create a port mapping to allow the peer to contact it.

## 17.2 UPnP and NAT-PMP Commands

The following table lists the `ip upnp` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 75** ip upnp Commands

| COMMAND | DESCRIPTION |
|---|---|
| `ip upnp` | Enters the `config-upnp` sub-command mode to configure the UPnP or NAT-PMP settings. |
| `[no] bypass-firewall activate` | Allows traffic from UPnP-enabled or NAT-PMP-enabled applications to bypass the firewall.<br>The `no` command has the firewall block all UPnP or NAT-PMP application packets (for example, MSN packets). |
| `link-sticking outgoing interface {`*`interface_name`*` \| all}` | Specifies through which WAN interface(s) you want to send out traffic from UPnP-enabled or NAT-PMP-enabled applications.<br>If the WAN interface you specified loses its connection, the ZyWALL / USG attempts to use the other WAN interface. If the other WAN interface also does not work, the ZyWALL / USG drops outgoing packets from UPnP-enabled or NAT-PMP-enabled applications. |
| `[no] listen-interface` *`interface_name`* | Enables UPnP and/or NAT-PMP on an internal interface.<br>The `no` command disables UPnP and/or NAT-PMP on the interface. |

**Table 75** ip upnp Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] nat-pmp activate | Enables NAT-PMP on the ZyWALL / USG.<br>The no command disables NAT-PMP on the ZyWALL / USG. |
| [no] upnp-igd activate | Enables UPnP on the ZyWALL / USG.<br>The no command disables UPnP on the ZyWALL / USG. |
| no ip upnp port-mapping port {<1..65535> type <tcp\|udp> \| all} | Removes all or a specific port mapping rule. |
| show ip upnp listen-interface | Displays the name(s) of the internal interface(s) on which the ZyWALL / USG supports UPnP and/or NAT-PMP. |
| show ip upnp port-mapping | Displays the UPnP and/or NAT-PMP port mapping rules on the ZyWALL / USG. |
| show ip upnp status | Displays the UPnP and/or NAT-PMP configuration. |

# 17.3 UPnP & NAT-PMP Commands Example

The following example turns on UPnP and NAT-PMP on the ZyWALL / USG and it's two LAN interfaces. It also shows the UPnP and NAT-PMP settings.

```
Router# configure terminal
Router(config)# ip upnp
Router(config-upnp)# nat-pmp activate
Router(config-upnp)# upnp-igd activate
Router(config-upnp)# listen-interface lan1
Router(config-upnp)# listen-interface lan2
Router(config-upnp)# exit
Router(config)# show ip upnp status
upnp active: yes
nat-pmp active: yes
bypass-firewall active: no
link-sticking outgoing: all
Router(config)# show ip upnp listen-interface
interface
================================================================================
lan1
lan2
Router(config)#
```

The following example displays the ZyWALL / USG's port mapping entries and removes the entry with the specified port number and protocol type.

```
Router# configure terminal
Router(config) # show ip upnp port-mapping
No: 0
  Remote Host: (null)
  Client Type: upnp
  External Port: 1122
  Protocol: tcp
  Internal Port: 1122
  Internal Client: 172.16.1.2
  Description: test1
No: 1
  Remote Host: (null)
  Client Type: upnp
  External Port: 5566
  Protocol: tcp
  Internal Port: 5566
  Internal Client: 172.16.1.2
  Description: test2
Router(config)# no ip upnp port-mapping port 5566 type tcp
Router(config)# show ip upnp port-mapping
No: 0
  Remote Host: (null)
  Client Type: upnp
  External Port: 1122
  Protocol: tcp
  Internal Port: 1122
  Internal Client: 172.16.1.2
  Description: test1
Router(config)#
```

# 18

# IP/MAC Binding

## 18.1 IP/MAC Binding Overview

IP address to MAC address binding helps ensure that only the intended devices get to use privileged IP addresses. The ZyWALL / USG uses DHCP to assign IP addresses and records to MAC address it assigned each IP address. The ZyWALL / USG then checks incoming connection attempts against this list. A user cannot manually assign another IP to his computer and use it to connect to the ZyWALL / USG.

Suppose you configure access privileges for IP address 192.168.1.27 and use static DHCP to assign it to Tim's computer's MAC address of 12:34:56:78:90:AB. IP/MAC binding drops traffic from any computer with another MAC address that tries to use IP address 192.168.1.27.

## 18.2 IP/MAC Binding Commands

The following table lists the `ip-mac-binding` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 76** ip-mac-binding Commands

| COMMAND | DESCRIPTION |
|---|---|
| `[no] ip ip-mac-binding` *`interface_name`* `activate` | Turns on IP/MAC binding for the specified interface. The `no` command turns IP/MAC binding off for the specified interface. |
| `[no] ip ip-mac-binding` *`interface_name`* `log` | Turns on the IP/MAC binding logs for the specified interface. The `no` command turns IP/MAC binding logs off for the specified interface. |
| `ip ip-mac-binding exempt` *`name start-ip end-ip`* | Adds a named IP range as being exempt from IP/MAC binding. |
| `no ip ip-mac-binding exempt` *`name`* | Deletes the named IP range from the list of addresses that are exempt from IP/MAC binding. |
| `show ip ip-mac-binding` *`interface_name`* | Shows whether IP/MAC binding is enabled or disabled for the specified interface. |
| `show ip ip-mac-binding all` | Shows whether IP/MAC binding is enabled or disabled for all interfaces. |
| `show ip ip-mac-binding status` *`interface_name`* | Displays the current IP/MAC bindings for the specified interface. |
| `show ip ip-mac-binding status all` | Displays the current IP/MAC bindings for all interfaces. |
| `show ip ip-mac-binding exempt` | Shows the current IP/MAC binding exempt list. |
| `ip ip-mac-binding clear-drop-count` *`interface_name`* | Resets the packet drop counter for the specified interface. |
| `debug ip ip-mac-binding activate` | Turns on the IP/MAC binding debug logs. |
| `no debug ip ip-mac-binding activate` | Turns off the IP/MAC binding debug logs. |

# 18.3 IP/MAC Binding Commands Example

The following example enables IP/MAC binding on the LAN1 interface and displays the interface's IP/MAC binding status.

```
Router# configure terminal
Router(config)# ip ip-mac-binding lan1 activate
Router(config)# show ip ip-mac-binding lan1
Name: lan1
Status: Enable
Log: No
Binding Count: 0
Drop Count: 0
Router(config)#
```

# 19

# ~~Firewall~~Secure Policy

This chapter introduces the ZyWALL / USG's ~~firewall~~secure policies ~~your ZyWALL / USG's firewall.~~them.

## 19.1 ~~Firewall~~Secure Policy Overview

~~The ZyWALL / USG's firewall is a stateful inspection firewall. The ZyWALL / USG restricts access by screening data packets against defined access rules. It can also inspect sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.~~

~~A zone is a group of interfaces or VPN tunnels. Group the ZyWALL / USG's interfaces into different zones based on your needs. You can configure firewall rules for data passing between zones or even between interfaces and/or VPN tunnels in a zone.~~

~~This example shows the ZyWALL / USG's default firewall behavior for WAN to LAN traffic and how stateful inspection works. A LAN user can initiate a Telnet session from within the LAN zone and the firewall allows the response. However, the firewall blocks Telnet traffic initiated from the WAN zone and destined for the LAN zone. The firewall allows VPN traffic between any of the networks.~~

**Figure 18** ~~Default Firewall Action~~

~~Your customized rules take precedence and override the ZyWALL / USG's default settings. The ZyWALL / USG checks the schedule, user name (user's login name on the ZyWALL / USG), source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the ZyWALL / USG takes the action specified in the rule.~~

~~For example, if you want to allow a specific user from any computer to access one zone by logging in to the ZyWALL / USG, you can set up a rule based on the user name only. If you also apply a schedule to the firewall rule, the user can only access the network at the scheduled time. A user-aware firewall rule is activated whenever the user logs in to the ZyWALL / USG and will be disabled after the user logs out of the ZyWALL / USG.~~A secure policy is a template of security settings that can be applied to specific traffic at specific times. The policy can be applied:

- to a specific direction of travel of packets (from / to)
- to a specific source and destination address objects
- to a specific type of traffic (services)
- to a specific user or group of users

- at a specific schedule

The policy can be configured:

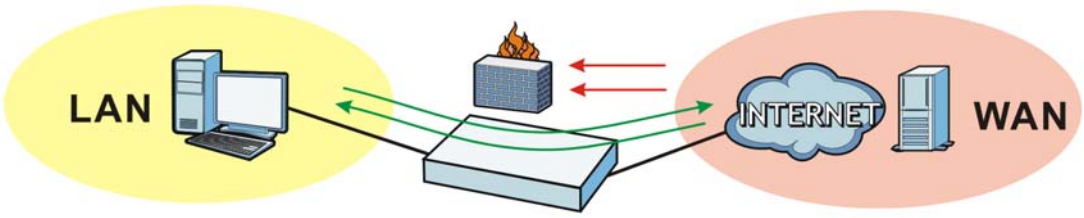
- to allow or deny traffic that matches the criteria above
- send a log or alert for traffic that matches the criteria above
- to apply the actions configured in the UTM profiles (application patrol, content filter, IDP, anti-virus, anti-spam) to traffic that matches the criteria above

Note: Security policies can be applied to both IPv4 and IPv6 traffic

The secure policies can also limit the number of user sessions.

The following example shows the ZyWALL / USG's default security policies behavior for a specific direction of travel of packets. WAN to LAN traffic and how stateful inspection works. A LAN user can initiate a Telnet session from within the LAN zone and the ZyWALL / USG allows the response. However, the ZyWALL / USG blocks incoming Telnet traffic initiated from the WAN zone and destined for the LAN zone.

**Figure 19** Default Directional Policy Example




# 19.2 ~~Firewall~~Secure Policy Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 77** Input Values for General Firewall Commands

| LABEL | DESCRIPTION |
|---|---|
| *address_object* | The name of the IP address (or address group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *address6_object* | The name of the IPv6 address (or address group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *user_name* | The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *zone_object* | The name of the zone. For ~~the~~some ZyWALL / USG ~~USG 300 and above~~models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.<br><br>~~The~~For other ZyWALL / USG ~~USG 200 and lower~~ models use pre-defined zone names like DMZ, LAN1, SSL VPN, WLAN, IPSec VPN, OPT, and WAN. |
| *rule_number* | The priority number of a firewall rule. 1 - *X* where *X* is the highest number of rules the ZyWALL / USG model supports. See the ZyWALL / USG's User's Guide for details. |

**Table 77** Input Values for General Firewall Commands (continued)

| LABEL | DESCRIPTION |
|---|---|
| *schedule_object* | The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *service_name* | The name of the service (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |

The following table describes the commands available for the firewall. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands. Commands that do not have IPv6 specified in the description are for IPv4.

**Table 78** Command Summary: Firewall

| COMMAND | DESCRIPTION |
|---|---|
| `[no] firewall asymmetrical-route activate` | Allows or disallows asymmetrical route topology. |
| `[no] connlimit max-per-host <1..8192>` | Sets the highest number of sessions that the ZyWALL / USG will permit a host to have at one time. The `no` command removes the settings. |
| `firewall rule_number` | Enters the firewall sub-command mode to set a firewall rule. See Table 79 on page 163 for the sub-commands. |
| `firewall zone_object {zone_object\|ZyWALL} rule_number` | Enters the firewall sub-command mode to set a direction specific through-ZyWALL rule or to-ZyWALL rule. See Table 79 on page 163 for the sub-commands. |
| `firewall zone_object {zone_object\|ZyWALL} append` | Enters the firewall sub-command mode to add a direction specific through-ZyWALL rule or to-ZyWALL rule to the end of the global rule list. See Table 79 on page 163 for the sub-commands. |
| `firewall zone_object {zone_object\|ZyWALL} delete <1..5000>` | Removes a direction specific through-ZyWALL rule or to-ZyWALL rule.<br>`<1..5000>`: the index number in a direction specific firewall rule list. |
| `firewall zone_object {zone_object\|ZyWALL} flush` | Removes all direction specific through-ZyWALL rule or to-ZyWALL rules. |
| `firewall zone_object {zone_object\|ZyWALL} insert rule_number` | Enters the firewall sub-command mode to add a direction specific through-ZyWALL rule or to-ZyWALL rule before the specified rule number. See Table 79 on page 163 for the sub-commands. |
| `firewall zone_object {zone_object\|ZyWALL} move rule_number to rule_number` | Moves a direction specific through-ZyWALL rule or to-ZyWALL rule to the number that you specified. |
| `[no] firewall activate` | Enables the firewall on the ZyWALL / USG. The `no` command disables the firewall. |
| `firewall append` | Enters the firewall sub-command mode to add a global firewall rule to the end of the global rule list. See Table 79 on page 163 for the sub-commands. |
| `firewall default-rule action {allow \| deny \| reject} { no log \| log [alert] }` | Sets how the firewall handles packets that do not match any other firewall rule. |
| `firewall delete rule_number` | Removes a firewall rule. |
| `firewall flush` | Removes all firewall rules. |

**Table 78** Command Summary: Firewall (continued)

| COMMAND | DESCRIPTION |
|---|---|
| `firewall insert rule_number` | Enters the firewall sub-command mode to add a firewall rule before the specified rule number. See Table 79 on page 163 for the sub-commands. |
| `firewall move rule_number to rule_number` | Moves a firewall rule to the number that you specified. |
| `show connlimit max-per-host` | Displays the highest number of sessions that the ZyWALL / USG will permit a host to have at one time. |
| `show firewallsecure-policy` | Displays all firewallSecure Policy settings. |
| `show firewallsecure-policy rule_number` | Displays a firewall rule's settings. |
| `show firewallsecure-policy zone_object {zone_object\|ZyWALL}` | Displays all firewall rules settings for the specified packet direction. |
| `show firewallsecure-policy zone_object {zone_object\|ZyWALL} rule_number` | Displays a specified firewall rule's settings for the specified packet direction. |
| `show firewallsecure-policy status` | Displays whether or not the firewall is active, whether or not asymmetrical route topology is allowed, and the default firewall rule's configuration. |
| `show firewall block_rules` | Displays all the firewall rules that deny access. |
| `show firewall any ZyWALL` | Shows all the to-ZyWALL / USG firewall rules. |
| `[no] connlimit6 max-per-host <1..8192>` | Sets the highest number of IPv6 sessions that the ZyWALL / USG will permit a host to have at one time. The no command removes the setting. |
| `firewall6 rule_number` | Enters the IPv6 firewall sub-command mode to set a firewall rule. See Table 79 on page 163 for the sub-commands. |
| `firewall6 zone_object {zone_object\|ZyWALL} rule_number` | Enters the IPv6 firewall sub-command mode to set a direction specific through-ZyWALL rule or to-ZyWALL rule. See Table 79 on page 163 for the sub-commands. |
| `firewall6 zone_object {zone_object\|ZyWALL} append` | Enters the IPv6 firewall sub-command mode to add a direction specific through-ZyWALL rule or to-ZyWALL rule to the end of the global rule list. See Table 79 on page 163 for the sub-commands. |
| `firewall6 zone_object {zone_object\|ZyWALL} delete <1..5000>` | Removes a direction specific IPv6 through-ZyWALL rule or to-ZyWALL rule.<br><br>`<1..5000>`: the index number in a direction specific firewall rule list. |
| `firewall6 zone_object {zone_object\|ZyWALL} flush` | Removes all direction specific IPv6 through-ZyWALL rule or to-ZyWALL rules. |
| `firewall6 zone_object {zone_object\|ZyWALL} insert rule_number` | Enters the IPv6 firewall sub-command mode to add a direction specific through-ZyWALL rule or to-ZyWALL rule before the specified rule number. See Table 79 on page 163 for the sub-commands. |
| `firewall6 zone_object {zone_object\|ZyWALL} move rule_number to rule_number` | Moves a direction specific IPv6 through-ZyWALL rule or to-ZyWALL rule to the number that you specified. |
| `[no] firewall activate` | Enables the IPv6 firewall on the ZyWALL / USG. The no command disables the IPv6 firewall. |
| `firewall6 append` | Enters the IPv6 firewall sub-command mode to add a global firewall rule to the end of the global rule list. See Table 79 on page 163 for the sub-commands. |
| `firewall6 default-rule action {allow \| deny \| reject} { no log \| log [alert] }` | Sets how the IPv6 firewall handles packets that do not match any other firewall rule. |

**Table 78** Command Summary: Firewall (continued)

| COMMAND | DESCRIPTION |
|---|---|
| `firewall6 delete` *rule_number* | Removes a IPv6 firewall rule. |
| `firewall6 flush` | Removes all IPv6 firewall rules. |
| `firewall6 insert` *rule_number* | Enters the IPv6 firewall sub-command mode to add a firewall rule before the specified rule number. See Table 79 on page 163 for the sub-commands. |
| `firewall6 move` *rule_number* `to` *rule_number* | Moves a IPv6 firewall rule to the number that you specified. |
| `show connlimit6 max-per-host` | Displays the highest number of IPv6 sessions that the ZyWALL / USG will permit a host to have at one time. |
| `show firewall6` | Displays all IPv6 firewall settings. |
| `show firewall6` *rule_number* | Displays a IPv6 firewall rule's settings. |
| `show firewall6` *zone_object* {*zone_object*\|ZyWALL} | Displays all IPv6 firewall rules settings for the specified packet direction. |
| `show firewall6` *zone_object* {*zone_object*\|ZyWALL} *rule_number* | Displays a specified IPv6 firewall rule's settings for the specified packet direction. |
| `show firewall6 status` | Displays whether or not the IPv6 firewall is active, whether or not IPv6 asymmetrical route topology is allowed, and the default IPv6 firewall rule's configuration. |
| `show firewall6 block_rules` | Displays all the IPv6 firewall rules that deny access. |
| `show firewall6 any ZyWALL` | Shows all the IPv6 to-ZyWALL / USG firewall rules. |
| `[no] firewall6 asymmetrical-route activate` | Allows or disallows asymmetrical route topology for IPv6 traffic. |

## 19.2.1 Firewall Sub-Commands

The following table describes the sub-commands for several `firewall` and `firewall6` commands.

**Table 79** firewall Sub-commands

| COMMAND | DESCRIPTION |
|---|---|
| `action {allow\|deny\|reject}` | Sets the action the ZyWALL / USG takes when packets match this rule. |
| `[no] activate` | Enables a firewall rule. The `no` command disables the firewall rule. |
| `[no] ctmatch {dnat \| snat}` | Use `dnat` to block packets sent from a computer on the ZyWALL / USG's WAN network from being forwarded to an internal network according to a virtual server rule.<br>Use `snat` to block packets sent from a computer on the ZyWALL / USG's internal network from being forwarded to the WAN network according to a 1:1 NAT or Many 1:1 NAT rule.<br>The `no` command forwards the matched packets. |
| `[no] description` *description* | Sets a descriptive name (up to 60 printable ASCII characters) for a firewall rule. The `no` command removes the descriptive name from the rule. |
| `[no] destinationip` *address_object* | Sets the destination IP address. The `no` command resets the destination IP address(es) to the default (`any`). `any` means all IP addresses. |

**Table 79** firewall Sub-commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] destinationip6 *address_object* | Sets the destination IPv6 address. The no command resets the destination IP address(es) to the default (any). any means all IP addresses. |
| [no] from *zone_object* | Sets the zone on which the packets are received. The no command removes the zone on which the packets are received and resets it to the default (any) meaning all interfaces or VPN tunnels. |
| [no] log [alert] | Sets the ZyWALL / USG to create a log (and optionally an alert) when packets match this rule. The no command sets the ZyWALL / USG not to create a log or alert when packets match this rule. |
| [no] schedule *schedule_object* | Sets the schedule that the rule uses. The no command removes the schedule settings from the rule. |
| [no] service *service_name* | Sets the service to which the rule applies. The no command resets the service settings to the default (any). any means all services. |
| [no] sourceip *address_object* | Sets the source IP address(es). The no command resets the source IP address(es) to the default (any). any means all IP addresses. |
| [no] sourceip6 *address_object* | Sets the source IP address(es). The no command resets the source IP address(es) to the default (any). any means all IP addresses. |
| [no] sourceport {tcp\|udp} {eq <1..65535>\|range <1..65535> <1..65535>} | Sets the source port for a firewall rule. The no command removes the source port from the rule. |
| [no] to {*zone_object*\|ZyWALL} | Sets the zone to which the packets are sent. The no command removes the zone to which the packets are sent and resets it to the default (any). any means all interfaces or VPN tunnels. |
| [no] user *user_name* | Sets a user-aware firewall rule. The rule is activated only when the specified user logs into the system. The no command resets the user name to the default (any). any means all users. |

## 19.2.2 Firewall Command Examples

These are IPv4 firewall configuration examples. The IPv6 firewall commands are similar.

The following example shows you how to add an IPv4 firewall rule to allow a MyService connection from the WAN zone to the IP addresses Dest_1 in the LAN zone.

- Enter configuration command mode.
- Create an IP address object.
- Create a service object.
- Enter the firewall sub-command mode to add a firewall rule.
- Set the direction of travel of packets to which the rule applies.
- Set the destination IP address(es).
- Set the service to which this rule applies.

- Set the action the ZyWALL / USG is to take on packets which match this rule.

```
Router# configure terminal
Router(config)# service-object MyService tcp eq 1234
Router(config)# address-object Dest_1 10.0.0.10-10.0.0.15
Router(config)# firewall insert 3
Router(firewall)# from WAN
Router(firewall)# to LAN
Router(firewall)# destinationip Dest_1
Router(firewall)# service MyService
Router(firewall)# action allow
```

The following command displays the default IPv4 firewall rule that applies to the WAN to ZyWALL / USG packet direction. The firewall rule number is in the rule's priority number in the global rule list.

```
Router(config)# show firewall WAN ZyWALL
firewall rule: 13
  description:
  user: any, schedule: none
  from: WAN, to: ZyWALL
  source IP: any, source port: any
  destination IP: any, service: Default_Allow_WAN_To_ZyWALL
  log: no, action: allow, status: yes
  connection match: no
```

The following command displays the default IPv6 firewall rule that applies to the WAN to ZyWALL / USG packet direction. The firewall rule number is in the rule's priority number in the global rule list.

```
Router(config)# show firewall6 WAN ZyWALL
firewall rule: 13
  description:
  user: any, schedule: none
  from: WAN, to: ZyWALL
  source IP: any, source port: any
  destination IP: any, service: Default_Allow_v6_WAN_To_ZyWALL
  log: no, action: allow, status: yes
```

# 19.3 Session Limit Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 80** Input Values for General Session Limit Commands

| LABEL | DESCRIPTION |
|---|---|
| *rule_number* | The priority number of a session limit rule, 1 - 1000. |
| *address_object* | The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |

**Table 80** Input Values for General Session Limit Commands (continued)

| LABEL | DESCRIPTION |
|---|---|
| *address6_object* | The name of the IPv6 address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *user_name* | The name of a user (group). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |

The following table describes the session-limit commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 81** Command Summary: Session Limit

| COMMAND | DESCRIPTION |
|---|---|
| `[no] session-limit activate` | Turns the session-limit feature on or off. |
| `session-limit limit <0..8192>` | Sets the default number of concurrent NAT/firewall sessions per host. |
| `session-limit` *rule_number* | Enters the session-limit sub-command mode to set a session-limit rule. |
| `[no] activate` | Enables the session-limit rule. The `no` command disables the session limit rule. |
| `[no] address` *address_object* | Sets the source IP address. The `no` command sets this to `any`, which means all IP addresses. |
| `[no] description` *description* | Sets a descriptive name (up to 64 printable ASCII characters) for a session-limit rule. The `no` command removes the descriptive name from the rule. |
| `exit` | Quits the sub-command mode. |
| `[no] limit <0..8192>` | Sets the limit for the number of concurrent NAT/firewall sessions this rule's users or addresses can have. 0 means any. |
| `[no] user` *user_name* | Sets a session-limit rule for the specified user. The `no` command resets the user name to the default (`any`). `any` means all users. |
| `session-limit append` | Enters the session-limit sub-command mode to add a session-limit rule to the end of the session-limit rule list. |
| `session-limit delete` *rule_number* | Removes a session-limit rule. |
| `session-limit flush` | Removes all session-limit rules. |
| `session-limit insert` *rule_number* | Enters the session-limit sub-command mode to add a session-limit rule before the specified rule number. |
| `session-limit move` *rule_number* `to` *rule_number* | Moves a session-limit to the number that you specified. |
| `show session-limit` | Shows the session-limit configuration. |
| `show session-limit begin` *rule_number* `end` *rule_number* | Shows the settings for a range of session-limit rules. |
| `show session-limit` *rule_number* | Shows the session-limit rule's settings. |
| `show session-limit status` | Shows the general session-limit settings. |
| `[no] session-limit6 activate` | Turns the IPv6 session-limit feature on or off. |
| `session-limit6 limit <0..8192>` | Sets the default number of concurrent NAT/firewall IPv6 sessions per host. |
| `session-limit6` *rule_number* | Enters the IPv6 session-limit sub-command mode to set a session-limit rule. |
| `[no] activate` | Enables the IPv6 session-limit rule. The `no` command disables the session limit rule. |

**Table 81** Command Summary: Session Limit (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] address *address6_object* | Sets the IPv6 source IP address. The no command sets this to any, which means all IP addresses. |
| [no] description *description* | Sets a descriptive name (up to 64 printable ASCII characters) for a session-limit rule. The no command removes the descriptive name from the rule. |
| exit | Quits the sub-command mode. |
| [no] limit <0..8192> | Sets the limit for the number of concurrent NAT/firewall IPv6 sessions this rule's users or addresses can have. 0 means any. |
| [no] user *user_name* | Sets an IPv6 session-limit rule for the specified user. The no command resets the user name to the default (any). any means all users. |
| session-limit6 append | Enters the IPv6 session-limit sub-command mode to add a session-limit rule to the end of the session-limit rule list. |
| session-limit6 delete *rule_number* | Removes an IPv6 session-limit rule. |
| session-limit6 flush | Removes all IPv6 session-limit rules. |
| session-limit6 insert *rule_number* | Enters the IPv6 session-limit sub-command mode to add a session-limit rule before the specified rule number. |
| session-limit6 move *rule_number* to *rule_number* | Moves an IPv6 session-limit to the number that you specified. |
| show session-limit6 | Shows the IPv6 session-limit configuration. |
| show session-limit6 begin *rule_number* end *rule_number* | Shows the settings for a range of IPv6 session-limit rules. |
| show session-limit6 *rule_number* | Shows the IPv6 session-limit rule's settings. |
| show session-limit6 status | Shows the general IPv6 session-limit settings. |

# 20

# Web Authentication

## 20.1 Web Authentication Overview

Web authentication can intercepts network traffic, according to the authentication policies, until the user authenticates his or her connection, usually through a specifically designated login web page. This means all web page requests can initially be redirected to a special web page that requires users to authenticate their sessions. Once authentication is successful, they can then connect to the rest of the network or Internet.

As soon as a user attempt to open a web page, the ZyWALL / USG reroutes his/her browser to a web portal page that prompts he/she to log in.

## 20.2 Web Authentication Commands

This table lists the commands for forcing user authentication. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 82** web-auth Commands

| COMMAND | DESCRIPTION |
|---|---|
| `[no] web-auth activate` | Enables force user authentication that force users to log in to the ZyWALL / USG before the ZyWALL / USG routes traffic for them. The no command means the user authentication is not required. |
| `web-auth default-rule authentication {required \| unnecessary} {no log \| log [alert]}` | Sets the default authentication policy that the ZyWALL / USG uses on traffic that does not match any exceptional service or other authentication policy.<br>`required`: Users need to be authenticated. They must manually go to the ZyWALL / USG's login screen. The ZyWALL / USG will not redirect them to the login screen.<br>`unnecessary`: Users do not need to be authenticated.<br>`no log \| log [alert]`: Select whether to have the ZyWALL / USG generate a log (`log`), log and alert (`log alert`) or not (`no log`) for packets that match this default policy. |
| `web-auth [no] exceptional-service` *`service_name`* | Sets a service which you want users to be able to access without user authentication. The `no` command removes the specified service from the exceptional list. |
| `web-auth login setting` | Sets the login web page through which the user authenticates his or her connection before he or she can then connect to the rest of the network or Internet. See Table 83 on page 170 for the sub-commands. |
| `web-auth method {portal \| user-agreement}` | Sets a client to authenticate with the ZyWALL / USG through the specifically designated web portal or user agreement page. |
| `web-auth policy <1..1024>` | Creates the specified condition for forcing user authentication, if necessary, and enters sub-command mode. The conditions are checked in sequence, starting at 1. See Table 84 on page 172 for the sub-commands. |

**Table 82** web-auth Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| `web-auth policy append` | Creates a new condition for forcing user authentication at the end of the current list and enters sub-command mode. See Table 84 on page 172 for the sub-commands. |
| `web-auth policy insert <1..1024>` | Creates a new condition for forcing user authentication at the specified location, renumbers the other conditions accordingly, and enters sub-command mode. See Table 84 on page 172 for the sub-commands. |
| `web-auth policy delete <1..1024>` | Deletes the specified condition.<br>To modify a condition, you can insert a new condition (N) and then delete the one (N+1) that you want to modify. |
| `web-auth policy flush` | Deletes every condition. |
| `web-auth policy move <1..1024> to <1..1024>` | Moves the specified condition to the specified location and renumbers the other conditions accordingly. |
| `web-auth user-agreement` | Enters sub-command mode to configure user agreement pages and related settings. See Table 85 on page 173 for the sub-commands. |
| `show web-auth activation` | Displays whether forcing user authentication is enabled or not. |
| `show web-auth default-rule` | Displays settings of the default web authentication policy. |
| `show web-auth exceptional-service` | Displays services that users can access without user authentication. |
| `show web-auth method` | Displays whether a client is to authenticate with the ZyWALL / USG through the specifically designated web portal or user agreement page when web authentication is enabled. |
| `show web-auth policy {<1..1024> \| all}` | Displays details about the policies for forcing user authentication. |
| `show web-auth portal status` | Displays the web portal page settings. |
| `show web-auth status` | Displays the web portal page or user agreement page settings. |
| `show web-auth user-agreement status` | Displays the user agreement page settings. |

## 20.2.1 web-auth login setting Sub-commands

The following table describes the sub-commands for the web-auth login setting command.

**Table 83** web-auth login setting Sub-commands

| COMMAND | DESCRIPTION |
|---|---|
| `exit` | Leaves the sub-command mode. |
| `type {external \| internal}` | Sets the login page appears whenever the web portal intercepts network traffic, preventing unauthorized users from gaining access to the network.<br>`internal`: Use the default login page built into the ZyWALL / USG.<br>`external`: Use a custom login page from an external web portal instead of the default one built into the ZyWALL / USG. You can configure the look and feel of the web portal page.<br>Note: If you select the external option, you cannot use endpoint security to make sure that users' computers meet specific security requirements before they can access the network. |
| `[no] error-url` *url* | Sets the error page's URL; for example, http://IIS server IP Address/error.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%) in quotes.<br>The `no` command removes the URL.<br>The Internet Information Server (IIS) is the web server on which the web portal files are installed. |

**Table 83** web-auth login setting Sub-commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] internal-welcome-url *url* | Sets the welcome page's URL when you select to use the default login page built into the ZyWALL / USG; for example, http://IIS server IP Address/welcome.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%) in quotes.<br>The no command removes the URL.<br>The Internet Information Server (IIS) is the web server on which the web portal files are installed. |
| [no] login-url *url* | Sets the login page's URL; for example, http://IIS server IP Address/login.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%) in quotes.<br>The no command removes the URL.<br>The Internet Information Server (IIS) is the web server on which the web portal files are installed. |
| [no] logout-ip *ipv4_address* | Sets an IP address that users can use to terminate their sessions manually by entering the IP address in the address bar of the web browser.<br>The no command removes the IP address. |
| [no] logout-url *url* | Sets the logout page's URL; for example, http://IIS server IP Address/ logout.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%) in quotes.<br>The no command removes the URL.<br>The Internet Information Server (IIS) is the web server on which the web portal files are installed. |
| [no] session-url *url* | Sets the session page's URL; for example, http://IIS server IP Address/ session.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%) in quotes.<br>The no command removes the URL.<br>The Internet Information Server (IIS) is the web server on which the web portal files are installed. |
| [no] terms-of-service | Forces users to agree to the terms before they can use the service. An agreement checkbox will display in the login page.<br>The no command allows users to use the service without agreeing to the terms. |
| [no] welcome-url *url* | Sets the welcome page's URL; for example, http://IIS server IP Address/ welcome.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%) in quotes.<br>The no command removes the URL.<br>The Internet Information Server (IIS) is the web server on which the web portal files are installed. |

## 20.2.2 web-auth policy Sub-commands

The following table describes the sub-commands for several web-auth policy commands. Note that not all rule commands use all the sub-commands listed here.

**Table 84** web-auth policy Sub-commands

| COMMAND | DESCRIPTION |
|---|---|
| [no] activate | Activates the specified condition. The no command deactivates the specified condition. |
| [no] authentication {force \| required} | Selects the authentication requirement for users when their traffic matches this policy. The no command means user authentication is not required.<br>force: Users need to be authenticated and the ZyWALL / USG automatically display the login screen when users who have not logged in yet try to send HTTP traffic.<br>required: Users need to be authenticated. They must manually go to the login screen. The ZyWALL / USG will not redirect them to the login screen. |
| [no] description *description* | Sets the description for the specified condition. The no command clears the description.<br>*description*: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 printable ASCII characters long. |
| [no] destination {*address_object* \| *group_name*} | Sets the destination criteria for the specified condition. The no command removes the destination criteria, making the condition effective for all destinations. |
| [no] eps <1..8> *eps_object_name* | Associates the specified End Point Security (EPS) object with the specified condition. The ZyWALL / USG checks authenticated users' computers against the condition's endpoint security objects in the order of 1 to 8. You have to configure order 1 and then the others if any. The no command removes the specified EPS object's association with the condition.<br>To apply EPS for this condition, you have to also make sure you enable EPS and set authentication to either required or force for this condition. |
| [no] eps activate | Enables EPS for the specified condition. The no command means to disable EPS for the condition. |
| [no] eps periodical-check <1..1440> | Sets a number of minutes the ZyWALL / USG has to repeat the endpoint security check. The no command means that the ZyWALL / USG only perform the endpoint security check when users log in to the ZyWALL / USG. |
| [no] force | Forces users to log in to the ZyWALL / USG if the specified condition is satisfied. The no command means that users do not log in to the ZyWALL / USG. |
| interface *interface_name* | Sets an interface on which packets for the policy must be received. |
| [no] schedule *schedule_name* | Sets the time criteria for the specified condition. The no command removes the time criteria, making the condition effective all the time. |
| [no] source {*address_object* \| *group_name*} | Sets the source criteria for the specified condition. The no command removes the source criteria, making the condition effective for all sources. |
| eps insert <1..8> *eps_object_name* | Inserts the specified EPS object for the condition. The number determines the order that this EPS rule is executed in the condition. |
| eps move <1..8> to <1..8> | Changes an endpoint object's position in the execution order of the condition. |
| show | Displays information about the specified condition. |

## 20.2.3 web-auth user-agreement Sub-commands

The following table describes the sub-commands for several web-auth user-agreement commands. Note that not all rule commands use all the sub-commands listed here.

**Table 85** web-auth user-agreement Sub-commands

| COMMAND | DESCRIPTION |
|---|---|
| [no] agreement-url *url* | Sets the user agreement page's URL; for example, http://IIS server IP Address/logout.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%) in quotes.<br>The no command removes the URL.<br>The Internet Information Server (IIS) is the web server on which the user agreement files are installed. |
| [no] idle-detection [timeout <1..60>] | Sets the ZyWALL / USG to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The ZyWALL / USG automatically logs out the access user once the specified idle timeout has been reached. |
| [no] internal-page-customization | Sets the ZyWALL / USG to use the custom user agreement pages that are uploaded to the ZyWALL / USG through the web configurator. |
| logon-re-auth-time <0..1440> | Sets the number of minutes the user can be logged into the UAG in one session before having to log in again. |
| type {external \| internal} | Sets the user agreement page appears whenever the web portal intercepts network traffic, preventing unauthorized users from gaining access to the network.<br>internal: Use the default user agreement page built into the ZyWALL / USG.<br>external: Use a custom user agreement page from an external web portal instead of the default one built into the ZyWALL / USG. You can configure the look and feel of the user agreement page. |
| [no] welcome-url <*url*> | Sets the welcome page's URL; for example, http://IIS server IP Address/logout.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%) in quotes.<br>The no command removes the URL and sets the ZyWALL / USG to use the welcome page of internal user agreement file.<br>The Internet Information Server (IIS) is the web server on which the user agreement files are installed. |

## 20.2.4 ~~Web Authentication Policy Insert Command Example~~

~~The following commands show how to insert a web authentication policy at position 1 of the checking order. This policy applies endpoint security policies and uses the following settings:~~

- ~~Activate: yes~~
- ~~Description: EPS-on-LAN~~
- ~~Source: use address object "LAN1_SUBNET"~~
- ~~Destination: use address object "DMZ_Servers"~~
- ~~User Authentication: required~~
- ~~Schedule: no specified~~
- ~~Endpoint security: Activate~~

- endpoint security object: use “EPS-WinXP” and “EPS-WinVista” for the first and second checking EPS objects

```
Router# configure terminal
Router(config)# web-auth policy insert 1
Router(config-web-auth-1)# activate
Router(config-web-auth-1)# description EPS-on-LAN
Router(config-web-auth-1)# source LAN1_SUBNET
Router(config-web-auth-1)# destination DMZ_Servers
Router(config-web-auth-1)# authentication force
Router(config-web-auth-1)# no schedule
Router(config-web-auth-1)# eps activate
Router(config-web-auth-1)# eps 1 EPS-WinXP
Router(config-web-auth-1)# eps 2 EPS-WinVista
Router(config-web-auth-1)# exit
```

# 20.3 SSO Overview

SSO (Single Sign-On) integrates Domain Controller and ZyWALL / USG authentication mechanisms, so that users just need to log in once (single login) to get access to permitted resources.

- The ZyWALL / USG, the DC, the SSO agent and the LDAP or AD server must all be in the same domain and be able to communicate with each other.
- SSO does not support IPv6 or RADIUS; you must use it in an IPv4 network environment with Windows AD (Active Directory) or LDAP (Lightweight Directory Access Protocol) authentication databases.
- You must enable Web Authentication to use SSO.

## 20.3.1 SSO Configuration Commands

Use these commands to configure the ZyWALL / USG to communicate with SSO.

**Table 86** SSO Commands and Subcommnds

| COMMAND | DESCRIPTION |
|---|---|
| sso agent primary | Enters SSO primary agent subcommand mode. |
| sso agent secondary | Enters secondary agent subcommand mode. A secondary agent is an optional backup SSO agent. |
| [no] Router(config-sso-primary)# ip <*w.x.y.z*> | Sets the primary or ssecondary SSO agent *ipv4 address*. Use *[no]* to disable the IPv4 address.<br>Type the IPv4 address of the SSO agent. The ZyWALL / USG and the SSO agent must be in the same domain and be able to communicate with each other. |
| Router(config-sso-secondary)#[no] [no] port <*1025..65535*> | Sets the primary or ssecondary agent port <*1025..65535*>. Use *[no]* to disable the port. Type the same port number here as in the **Agent Listening Port** field on the SSO agent. Type a number ranging from 1025 to 65535. |
| *sso presharekey <preshared key>* | Sets the SSO preshared key. Type 8-32 printable ASCII characters or exactly 32 hex characters (0-9; a-f). The Agent PreShareKey is used to encrypt communications between the ZyWALL / USG and the SSO agent |
| *sso encrypted-presharekey <ciphertext>* | Sets the SSO encrypted preshared key. |

## 20.3.2 SSO Show Commands

You don't need to enter the configuration mode before you can use these commands. Use them to see SSO configurations done.

**Table 87** SSO Show Commands

| COMMAND | DESCRIPTION |
|---|---|
| show sso agent | Displays primary and secondary agent IP and Port configurations |
| show sso port | Displays the ZySSO port configured |
| show sso presharekey | Shows the configured ZySSO presharekey. |

## 20.3.3 Command Setup Sequence Example

The following commands show how to configure the ZyWALL / USG to communicate with an an SSO agent at IP address '1.1.1.1', using port '2158' and preshared key '12345678'.

```
Router(config)# sso agent primary
Router(config-sso-primary)# ip 1.1.1.1
Router(config-sso-primary)# port 2158
Router(config-sso-primary)# exit
Router(config)# sso presharekey 12345678
Router(config)# exit
Router# show sso agent
Agent: primary
  IP Address: 1.1.1.1
  Port: 2158
Agent: secondary
  IP Address:
  Port: 0
Router# show sso port
ZySSO port: 2158
Router# show sso presharekey
ZySSO presharekey: 12345678
Router#
```

# 21

# IPSec VPN

This chapter explains how to set up and maintain IPSec VPNs in the ZyWALL / USG.

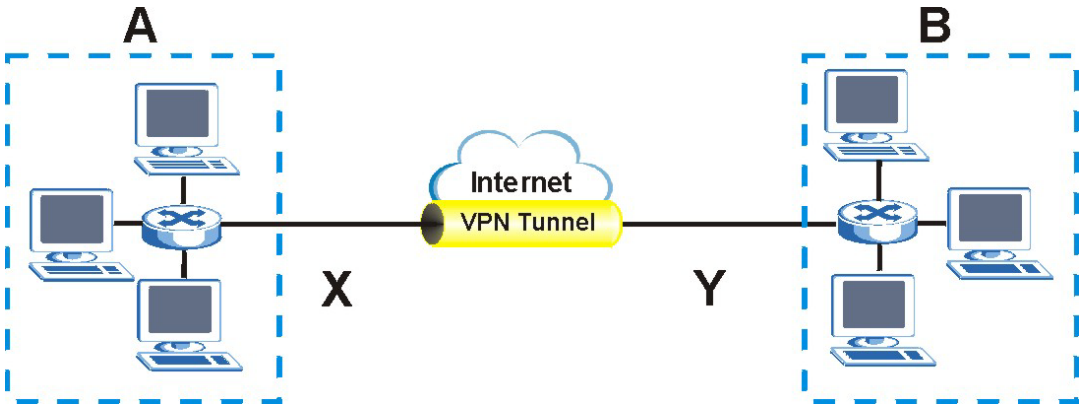
## 21.1 IPSec VPN Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

The following figure is one example of a VPN tunnel.

**Figure 20** VPN: Example

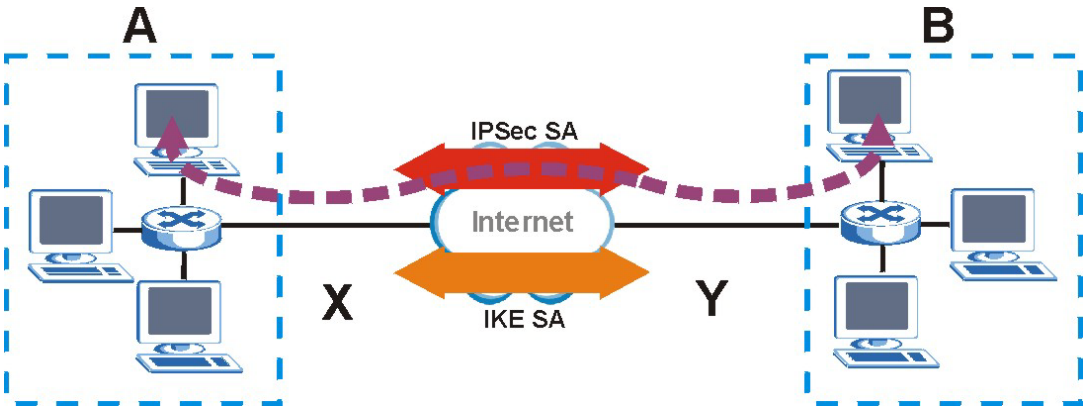



The VPN tunnel connects the ZyWALL / USG (**X**) and the remote IPSec router (**Y**). These routers then connect the local network (**A**) and remote network (**B**).

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the ZyWALL / USG and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the ZyWALL / USG and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec

SA through which the ZyWALL / USG and remote IPSec router can send data between computers on the local network and remote network. This is illustrated in the following figure.

**Figure 21** VPN: IKE SA and IPSec SA




In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is secure because routers **X** and **Y** established the IKE SA first.

# 21.2 IPSec VPN Commands Summary

The following table describes the values required for many IPSec VPN commands. Other values are discussed with the corresponding commands.

**Table 88** Input Values for IPSec VPN Commands

| LABEL | DESCRIPTION |
|---|---|
| *profile_name* | The name of a VPN concentrator. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *policy_name* | The name of an IKE SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *map_name* | The name of an IPSec SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *domain_name* | Fully-qualified domain name. You may use up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period. |
| *e_mail* | An e-mail address. You can use up to 63 alphanumeric characters, underscores (_), dashes (-), or @ characters. |

**Table 88** Input Values for IPSec VPN Commands (continued)

| LABEL | DESCRIPTION |
|---|---|
| *distinguished_name* | A domain name. You can use up to 511 alphanumeric, characters, spaces, or .@=,_- characters. |
| *sort_order* | Sort the list of currently connected SAs by one of the following classifications.<br>algorithm<br>encapsulation<br>inbound<br>name<br>outbound<br>policy<br>timeout<br>uptime |

The following sections list the IPSec VPN commands.

## 21.2.1 IKE SA Commands

This table lists the commands for IKE SAs (VPN gateways).

**Table 89** isakmp Commands: IKE SAs

| COMMAND | DESCRIPTION |
|---|---|
| show isakmp keepalive | Displays the Dead Peer Detection period. |
| show isakmp policy [*policy_name*] | Shows the specified IKE SA or all IKE SAs. |
| isakmp keepalive <2..60> | Sets the Dead Peer Detection period. |
| [no] isakmp policy *policy_name* | Creates the specified IKE SA if necessary and enters sub-command mode. The no command deletes the specified IKE SA. |
| activate<br>deactivate | Activates or deactivates the specified IKE SA. |
| authentication {pre-share \| rsa-sig} | Specifies whether to use a pre-shared key or a certificate for authentication. |
| certificate *certificate-name* | Sets the certificate that can be used for authentication. |
| [no] dpd | Enables Dead Peer Detection (DPD). The no command disables DPD. |
| [no] fall-back | Set this to have the ZyWALL / USG reconnect to the primary address when it becomes available again and stop using the secondary connection, if the connection to the primary address goes down and the ZyWALL / USG changes to using the secondary connection.<br>Users will lose their VPN connection briefly while the ZyWALL / USG changes back to the primary connection. To use this, the peer device at the secondary address cannot be set to use a nailed-up VPN connection. |
| fall-back-check-interval <60..86400> | Sets how often (in seconds) the ZyWALL / USG checks if the primary address is available. |
| mode {main \| aggressive} | Sets the negotiating mode. |
| transform-set isakmp-algo [isakmp_algo [*isakmp_algo*]] | Sets the encryption and authentication algorithms for each IKE SA proposal.<br>*isakmp_algo*: {des-md5 \| des-sha \| 3des-md5 \| 3des-sha \| aes128-md5 \| aes128-sha \| aes192-md5 \| aes192-sha \| aes256-md5 \| aes256-sha \| aes256-sha256 \| aes256-sha512} |

**Table 89** isakmp Commands: IKE SAs (continued)

| COMMAND | DESCRIPTION |
|---|---|
| lifetime <180..3000000> | Sets the IKE SA life time to the specified value. |
| group1<br>group2<br>group5 | Sets the DH*x* group to the specified group. |
| [no] natt | Enables NAT traversal. The no command disables NAT traversal. |
| local-ip {ip {*ip* \| *domain_name*} \| interface *interface_name*} | Sets the local gateway address to the specified IP address, domain name, or interface. |
| peer-ip {*ip* \| *domain_name*} [*ip* \| *domain_name*] | Sets the remote gateway address(es) to the specified IP address(es) or domain name(s). |
| keystring *pre_shared_key* | Sets the pre-shared key that can be used for authentication. The *pre_shared_key* can be:<br>• 8 - 32 alphanumeric characters or ,;\|`~!@#$%^&*()_+\{}':./<>=-".<br>• 16 - 64 hexadecimal (0-9, A-F) characters, preceded by "0x".<br>The pre-shared key is case-sensitive. |
| local-id type {ip *ip* \| fqdn *domain_name* \| mail *e_mail* \| dn *distinguished_name*} | Sets the local ID type and content to the specified IP address, domain name, or e-mail address. |
| peer-id type {any \| ip *ip* \| fqdn *domain_name* \| mail *e_mail* \| dn *distinguished_name*} | Sets the peer ID type and content to any value, the specified IP address, domain name, or e-mail address. |
| [no] xauth type {server *xauth_method* \| client name *username* password *password*} | Enables extended authentication and specifies whether the ZyWALL / USG is the server or client. If the ZyWALL / USG is the server, it also specifies the extended authentication method (aaa authentication *profile_name*); if the ZyWALL / USG is the client, it also specifies the username and password to provide to the remote IPSec router. The no command disables extended authentication.<br>*username*: You can use alphanumeric characters, underscores (_), and dashes (-), and it can be up to 31 characters long.<br>*password*: You can use most printable ASCII characters. You cannot use square brackets [ ], double quotation marks ("), question marks (?), tabs or spaces. It can be up to 31 characters long. |
| isakmp policy rename *policy_name policy_name* | Renames the specified IKE SA (first *policy_name*) to the specified name (second *policy_name*). |

## 21.2.2 IPSec SA Commands (except Manual Keys)

This table lists the commands for IPSec SAs, excluding manual keys (VPN connections using VPN gateways).

**Table 90** crypto Commands: IPSec SAs

| COMMAND | DESCRIPTION |
|---|---|
| [no] crypto ignore-df-bit | Fragment packets larger than the MTU (Maximum Transmission Unit) that have the "don't" fragment" bit in the header turned on. The no command has the ZyWALL / USG drop packets larger than the MTU that have the "don't" fragment" bit in the header turned on. |
| show crypto map [*map_name*] | Shows the specified IPSec SA or all IPSec SAs. |

**Table 90** crypto Commands: IPSec SAs (continued)

| COMMAND | DESCRIPTION |
|---|---|
| crypto map dial *map_name* | Dials the specified IPSec SA manually. This command does not work for IPSec SAs using manual keys or for IPSec SAs where the remote gateway address is 0.0.0.0. |
| [no] crypto map *map_name* | Creates the specified IPSec SA if necessary and enters sub-command mode. The no command deletes the specified IPSec SA. |
| crypto map rename *map_name map_name* | Renames the specified IPSec SA (first *map_name*) to the specified name (second *map_name*). |
| crypto map *map_name* | |
| activate<br>deactivate | Activates or deactivates the specified IPSec SA. |
| adjust-mss {auto \| <200..1500>} | Set a specific number of bytes for the Maximum Segment Size (MSS) meaning the largest amount of data in a single TCP segment or IP datagram for this VPN connection or use auto to have the ZyWALL automatically set it. |
| ipsec-isakmp *policy_name* | Specifies the IKE SA for this IPSec SA and disables manual key. |
| encapsulation {tunnel \| transport} | Sets the encapsulation mode. |
| transform-set *crypto_algo_esp* [*crypto_algo_esp* [*crypto_algo_esp*]] | Sets the active protocol to ESP and sets the encryption and authentication algorithms for each proposal.<br>*crypto_algo_esp*: esp-null-md5 \| esp-null-sha \| esp-null-sha256 \| esp-null-sha512 \| esp-des-md5 \| esp-des-sha \| esp-des-sha256 \| esp-des-sha512 \| esp-3des-md5 \| esp-3des-sha \| esp-3des-sha256 \| esp-3des-sha512 \| esp-aes128-md5 \| esp-aes128-sha \| esp-aes128-sha256 \| esp-aes128-sha512 \| esp-aes192-md5 \| esp-aes192-sha \| esp-aes192-sha256 \| esp-aes192-sha512 \| esp-aes256-md5 \| esp-aes256-sha \| esp-aes256-sha256 \| esp-aes256-sha512 |
| transform-set *crypto_algo_ah* [*crypto_algo_ah* [*crypto_algo_ah*]] | Sets the active protocol to AH and sets the encryption and authentication algorithms for each proposal.<br>*crypto_algo_ah*: ah-md5 \| ah-sha \| ah-sha256 \| ah-sha512 |
| scenario {site-to-site-static\|site-to-site-dynamic\|remote-access-server\|remote-access-client} | Select the scenario that best describes your intended VPN connection.<br>Site-to-site: The remote IPSec router has a static IP address or a domain name. This ZyWALL / USG can initiate the VPN tunnel.<br>site-to-site-dynamic: The remote IPSec router has a dynamic IP address. Only the remote IPSec router can initiate the VPN tunnel.<br>remote-access-server: Allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.<br>remote-access-client: Choose this to connect to an IPSec server. This ZyWALL / USG is the client (dial-in user) and can initiate the VPN tunnel. |
| set security-association lifetime seconds <180..3000000> | Sets the IPSec SA life time. |
| set pfs {group1 \| group2 \| group5 \| none} | Enables Perfect Forward Secrecy group. |
| local-policy *address_name* | Sets the address object for the local policy (local network). |
| remote-policy *address_name* | Sets the address object for the remote policy (remote network). |

**Table 90** crypto Commands: IPSec SAs (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] policy-enforcement | Drops traffic whose source and destination IP addresses do not match the local and remote policy. This makes the IPSec SA more secure. The no command allows traffic whose source and destination IP addresses do not match the local and remote policy.<br><br>Note: You must allow traffic whose source and destination IP addresses do not match the local and remote policy, if you want to use the IPSec SA in a VPN concentrator. |
| [no] nail-up | Automatically re-negotiates the SA as needed. The no command does not. |
| [no] replay-detection | Enables replay detection. The no command disables it. |
| [no] netbios-broadcast | Enables NetBIOS broadcasts through the IPSec SA. The no command disables NetBIOS broadcasts through the IPSec SA. |
| [no] out-snat activate | Enables out-bound traffic SNAT over IPSec. The no command disables out-bound traffic SNAT over IPSec. |
| out-snat source *address_name* destination *address_name* snat *address_name* | Configures out-bound traffic SNAT in the IPSec SA. |
| [no] in-snat activate | Enables in-bound traffic SNAT in the IPSec SA. The no command disables in-bound traffic SNAT in the IPSec SA. |
| in-snat source *address_name* destination *address_name* snat *address_name* | Configures in-bound traffic SNAT in the IPSec SA. |
| [no] in-dnat activate | Enables in-bound traffic DNAT in the IPSec SA. The no command disables in-bound traffic DNAT in the IPSec SA. |
| in-dnat delete <1..10> | Deletes the specified rule for in-bound traffic DNAT in the specified IPSec SA. |
| in-dnat move <1..10> to <1..10> | Moves the specified rule (first rule number) to the specified location (second rule number) for in-bound traffic DNAT. |
| in-dnat append protocol {all \| tcp \| udp} original-ip *address_name* <0..65535> <0..65535> mapped-ip *address_name* <0..65535> <0..65535> | Maps the specified IP address and port range (original-ip) to the specified IP address and port range (mapped-ip) and appends this rule to the end of the rule list for in-bound traffic DNAT. |
| in-dnat insert <1..10> protocol {all \| tcp \| udp} original-ip *address_name* <0..65535> <0..65535> mapped-ip *address_name* <0..65535> <0..65535> | Maps the specified IP address and port range (original-ip) to the specified IP address and port range (mapped-ip) and inserts this rule before the specified rule. |
| in-dnat <1..10> protocol {all \| tcp \| udp} original-ip *address_name* <0..65535> <0..65535> *mapped-ip address_name* <0..65535> <0..65535> | Creates or revises the specified rule and maps the specified IP address and port range (original-ip) to the specified IP address and port range (mapped-ip). |

## 21.2.3 IPSec SA Commands (for Manual Keys)

This table lists the additional commands for IPSec SAs using manual keys (VPN connections using manual keys).

**Table 91** crypto map Commands: IPSec SAs (Manual Keys)

| COMMAND | DESCRIPTION |
|---|---|
| `crypto map map_name` | |
| `set session-key {ah <256..4095> auth_key \| esp <256..4095> [cipher enc_key] authenticator auth_key}` | Sets the active protocol, SPI (<256..4095>), authentication key and encryption key (if any).<br>*auth_key*: You can use any alphanumeric characters or ,;\|`~!@#$%^&*()_+\{}':./<>=-". The length of the key depends on the algorithm.<br>md5 - 16-20 characters<br>sha - 20 characters<br>sha256 - 32 characters<br>sha512 - 64 characters<br>*enc_key*: You can use any alphanumeric characters or ,;\|`~!@#$%^&*()_+\{}':./<>=-". The length of the key depends on the algorithm.<br>des - 8-32 characters<br>3des - 24-32 characters<br>aes128 - 16-32 characters<br>aes192 - 24-32 characters<br>aes256 - 32 characters<br>If you want to enter the key in hexadecimal, type “0x” at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters.<br>The ZyWALL / USG automatically ignores any characters above the minimum number of characters required by the algorithm. For example, if you enter 1234567890XYZ for a DES encryption key, the ZyWALL / USG only uses 12345678. The ZyWALL / USG still stores the longer key. |
| `local-ip ip` | Sets the local gateway address to the specified IP address. |
| `peer-ip ip` | Sets the remote gateway address to the specified IP address. |

## 21.2.4 VPN Concentrator Commands

This table lists the commands for the VPN concentrator.

**Table 92** vpn-concentrator Commands: VPN Concentrator

| COMMAND | DESCRIPTION |
|---|---|
| `show vpn-concentrator [profile_name]` | Shows the specified VPN concentrator or all VPN concentrators. |
| `[no] vpn-concentrator profile_name` | Creates the specified VPN concentrator if necessary and enters sub-command mode. The no command deletes the specified VPN concentrator. |

**Table 92** vpn-concentrator Commands: VPN Concentrator (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] crypto *map_name* | Adds the specified IPSec SA to the specified VPN concentrator. The no command removes the specified IPSec SA from the specified VPN concentrator. |
| vpn-concentrator rename *profile_name profile_name* | Renames the specified VPN concentrator (first *profile_name*) to the specified name (second *profile_name*). |

## 21.2.5 VPN Configuration Provisioning Commands

This table lists the commands for VPN configuration provisioning.

**Table 93** vpn-configuration-provision Commands: VPN Configuration Provisioning

| COMMAND | DESCRIPTION |
|---|---|
| vpn-configuration-provision rule { append \| *conf_index* \| insert *conf_index* } | Enters the VPN configuration provisioning sub-command mode to add or edit a rule.<br>*conf_index*: The index number of a VPN configuration provisioning rule, 1 to the ZyWALL / USG's maximum number of VPN connection rules. |
| [no] activate | Turns the VPN configuration provisioning rule on or off. |
| crypto *map_name* | Specifies the name of the IPSec VPN connection (*map_name*) to bind to this VPN configuration provisioning rule's user or group. |
| user *username* | Specifies a user or group of users allowed to use the ZyWALL / USG IPSec VPN client to retrieve the associated VPN rule settings. A user may belong to a number of groups. If VPN configuration provisioning rules are configured for different groups, the ZyWALL / USG will allow VPN rule setting retrieval based on the first match found. Admin or limited-admin users are not allowed. |
| no user | Removes the VPN configuration provisioning rule's user or user group configuration. In other words, any users can match the rule. In the GUI "any" will display in the **Allowed User** field. |
| exit | Leaves the sub-command mode. |
| vpn-configuration-provision rule { delete *conf_index* \| move *conf_index* to *conf_index* } | Deletes or moves the specified VPN configuration provisioning rule. |
| [no] vpn-configuration-provision activate | Turns the VPN configuration provisioning service on or off. |
| vpn-configuration-provision authentication *auth_method* | Sets the authentication method the VPN configuration provisioning service uses to authenticate users. |
| show vpn-configuration-provision activation | Displays whether or not the VPN configuration provisioning service is activated. |
| show vpn-configuration-provision authentication | Displays the authentication method the VPN configuration provisioning service uses to authenticate users. |
| show vpn-configuration-provision rules | Displays the settings of the configured VPN configuration provisioning rules. |

## 21.2.6 SA Monitor Commands

This table lists the commands for the SA monitor.

**Table 94** sa Commands: SA Monitor

| COMMAND | DESCRIPTION |
|---|---|
| `show sa monitor [{begin <1..1000>} \| {end <1..1000>} \| {crypto-map` *regexp*`} \| {policy` *regexp*`} \|{rsort` *sort_order*`} \| {sort` *sort_order*`}]` | Displays the current IPSec SAs and the status of each one. You can specify a range of SA entries to display. You can also control the sort order of the display and search by VPN connection or (local or remote) policy.<br><br>*regexp*: A keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:?\|{}[]<>/ characters.<br><br>A question mark (?) lets a single character in the VPN connection or policy name vary. For example, use “a?c” (without the quotation marks) to specify abc, acc and so on.<br><br>Wildcards (*) let multiple VPN connection or policy names match the pattern. For example, use “*abc” (without the quotation marks) to specify any VPN connection or policy name that ends with “abc”. A VPN connection named “testabc” would match. There could be any number (of any type) of characters in front of the “abc” at the end and the VPN connection or policy name would still match. A VPN connection or policy name named “testacc” for example would not match.<br><br>A * in the middle of a VPN connection or policy name has the ZyWALL / USG check the beginning and end and ignore the middle. For example, with “abc*123”, any VPN connection or policy name starting with “abc” and ending in “123” matches, no matter how many characters are in between.<br><br>The whole VPN connection or policy name has to match if you do not use a question mark or asterisk.<br><br>See Table 88 on page 178 for other parameter description. |
| `show isakmp sa` | Displays current IKE SA and the status of each one. |
| `no sa spi` *spi* | Deletes the SA specified by the SPI.<br><br>*spi*: 2-8 hexadecimal (0-9, A-F) characters |
| `no sa tunnel-name` *map_name* | Deletes the specified IPSec SA. |
| `show vpn-counters` | Displays VPN traffic statistics. |

# 22

# SSL VPN

This chapter shows you how to set up secure SSL VPN access for remote user login.

## 22.1 SSL Access Policy

An SSL access policy allows the ZyWALL / USG to perform the following tasks:

- limit user access to specific applications or files on the network.
- allow user access to specific networks.
- assign private IP addresses and provide DNS/WINS server information to remote users to access internal networks.

### 22.1.1 SSL Application Objects

SSL application objects specify an application type and server that users are allowed to access through an SSL tunnel. See Chapter 38 on page 302 for how to configure SSL application objects.

### 22.1.2 SSL Access Policy Limitations

You cannot delete an object that is used by an SSL access policy. To delete the object, you must first unassociate the object from the SSL access policy.

## 22.2 SSL VPN Commands

The following table describes the values required for some SSL VPN commands. Other values are discussed with the corresponding commands.

**Table 95** Input Values for SSL VPN Commands

| LABEL | DESCRIPTION |
|---|---|
| *profile_name* | The descriptive name of an SSL VPN access policy. You may use up to 31 characters (“a-z”, A-Z”, “0-9”) with no spaces allowed. |
| *address_object* | The name of an IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *application_object* | The name of an SSL application object. You may use up to 31 characters (“0-9”, “a-z”, “A-Z”, “-” and “_”). No spaces are allowed. |

**Table 95** Input Values for SSL VPN Commands (continued)

| LABEL | DESCRIPTION |
|---|---|
| *user_name* | The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| eps_profile_name | The name of an endpoint security object. |

The following sections list the SSL VPN commands.

## 22.2.1 SSL VPN Commands

This table lists the commands for SSL VPN. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 96** SSL VPN Commands

| COMMAND | DESCRIPTION |
|---|---|
| show sslvpn policy [*profile_name*] | Displays the settings of the specified SSL VPN access policy. |
| show ssl-vpn network-extension local-ip | Displays the IP address that the ZyWALL / USG uses in setting up the SSL VPN. |
| show sslvpn monitor | Displays a list of the users who are currently logged into the VPN SSL client portal. |
| sslvpn network-extension local-ip *ip* | Sets the IP address that the ZyWALL / USG uses in setting up the SSL VPN. |
| sslvpn policy {*profile_name* \| *profile_name* append \| *profile_name* insert <1..16>} | Enters the SSL VPN sub-command mode to add or edit an SSL VPN access policy. |
| [no] activate | Turns the SSL VPN access policy on or off. |
| [no] application *application_object* | Adds the SSL application object to the SSL VPN access policy. |
| [no] cache-clean activate | Cleans the cookie, history, and temporary Internet files in the user's browser's cache when the user logs out. The ZyWALL / USG returns them to the values present before the user logged in. The `no` command disables this setting. |
| [no] description *description* | Adds information about the SSL VPN access policy. Use up to 60 characters ("0-9", "a-z", "A-Z", "-" and "_"). |
| [no] eps <1..8> *eps_profile_name* | Sets endpoint security objects to be used for the SSL VPN access policy. The ZyWALL / USG checks authenticated users' computers against the policy's selected endpoint security objects in the order from 1 to 8 you specified. When a user's computer meets an endpoint security object's requirements the ZyWALL / USG grants access and stops checking.<br>To make the endpoint security check as efficient as possible, arrange the endpoint security objects in order with the one that the most users should match first and the one that the least users should match last. |
| [no] eps activate | Sets to have the ZyWALL / USG check that users' computers meet the Operating System (OS) and security requirements of one of the SSL access policy's selected endpoint security objects before granting access. The `no` command disables this setting. |
| eps insert <1..8> *eps_profile_name* | Inserts the specified endpoint security object to the specified position for the endpoint security objects checking order. |
| eps move <1..8> to <1..8> | Moves the first specified endpoint security object to the second specified endpoint security object's position. |

**Table 96** SSL VPN Commands

| COMMAND | DESCRIPTION |
|---|---|
| [no] eps periodical-check activate | Sets whether to have the ZyWALL / USG repeat the endpoint security check at a regular interval configured using the next command. The no command disables this setting. |
| [no] eps periodical-check <1..1440> | Sets the number of minutes to have the ZyWALL / USG repeat the endpoint security check at a regular interval. The no command disables this setting. |
| [no] network-extension {activate \| ip-pool *address_object* \| 1st-dns {*address_object* \| *ip* } \| 2nd-dns {*address_object* \| *ip* } \| 1st-wins {*address_object* \| *ip* } \| 2nd-wins {*address_object* \| *ip* } \| network *address_object*} | Use this to configure for a VPN tunnel between the authenticated users and the internal network. This allows the users to access the resources on the network as if they were on the same local network.<br>ip-pool: specify the name of the pool of IP addresses to assign to the user computers for the VPN connection.<br>Specify the names of the DNS or WINS servers to assign to the remote users. This allows them to access devices on the local network using domain names instead of IP addresses.<br>network: specify a network users can access. |
| [no] network-extension traffic-enforcement | Forces all SSL VPN client traffic to be sent through the SSL VPN tunnel. The no command disables this setting. |
| [no] user *user_name* | Specifies the user or user group that can use the SSL VPN access policy. |
| sslvpn policy move <1..16> to <1..16> | Moves the specified SSL VPN access policy to the number that you specified. |
| sslvpn no connection username *user_name* | Terminates the user's SSL VPN connection and deletes corresponding session information from the ZyWALL / USG. |
| no sslvpn policy *profile_name* | Deletes the specified SSL VPN access policy. |
| sslvpn policy rename *profile_name* *profile_name* | Renames the specified SSL VPN access policy. |
| show workspace application | Displays the SSLVPN resources available to each user when logged into SSLVPN. |
| show workspace cifs | Displays the shared folders available to each user when logged into SSLVPN. |

## 22.2.2 Setting an SSL VPN Rule Tutorial

Here is an example SSL VPN configuration. The SSL VPN rule defines:

- Only users using the "tester" account can use the SSL VPN.
- The ZyWALL / USG will assign an IP address from 192.168.100.1 to 192.168.100.10 (defined in object "IP-POOL") to the computers which match the rule's criteria.
- The ZyWALL / USG will assign two DNS server settings (172.16.1.1 and 172.16.1.2 defined in objects DNS1 and DNS2) to the computers which match the rule's criteria.
- The SSL VPN users are allowed to access the ZyWALL / USG's local network, 172.16.10.0/24 (defined in object "Network1").
- Users have to access the SSL VPN using a computer that complies with all the following criteria (defined in object "EPS-1"):
  - Windows XP is installed.
  - TrendMicro PC-Cillin Internet Security 2007 is installed and activated.

1 First of all, configure 10.1.1.254/24 for the IP address of interface ge2 which is an external interface for public SSL VPN to access. Configure 172.16.10.254/24 for the IP address of interface ge3 which is an internal network.

```
Router(config)# interface ge2
Router(config-if-ge)# ip address 10.1.1.254 255.255.255.0
Router(config-if-ge)# exit
Router(config)# interface ge3
Router(config-if-ge)# ip address 172.16.10.254  255.255.255.0
Router(config-if-ge)# exit
```

2 Create four address objects for the SSL VPN DHCP pool, DNS servers and the local network for SSL VPN authenticated users to access.

```
Router(config)# address-object IP-POOL 192.168.100.1-192.168.100.10
Router(config)# address-object DNS1 172.16.5.1
Router(config)# address-object DNS2 172.16.5.2
Router(config)# address-object NETWORK1 172.16.10.0/24
```

3 Create an endpoint security profile named EPS-1. SSL VPN users' computers must install Windows XP and TrendMicro PC-Cillin Internet Security 2007. Besides, the PC-Cillin anti-virus must be activated.

```
Router(config)# eps profile EPS-1
Router(eps EPS-1)# matching-criteria all
Router(eps EPS-1)# os-type windows
Router(eps EPS-1)# windows-version windows-xp
Router(eps EPS-1)# anti-virus activate
Router(eps EPS-1)# anti-virus TrendMicro_PC-Cillin_Internet_Security_2007 detect-
auto-protection enable
Router(eps EPS-1)# exit
```

4 Create the SSL VPN user account named tester with password 1234.

```
Router(config)# username tester password 1234 user-type user
```

5 Create an SSL VPN rule named SSL_VPN_TEST. Enable it and apply objects you just created.

```
Router(config)# sslvpn policy SSL_VPN_TEST
Router(policy SSL_VPN_TEST)# activate
Router(policy SSL_VPN_TEST)# user tester
Router(policy SSL_VPN_TEST)# network-extension activate
Router(policy SSL_VPN_TEST)# network-extension ip-pool IP-POOL
Router(policy SSL_VPN_TEST)# network-extension 1st-dns DNS1
Router(policy SSL_VPN_TEST)# network-extension 2nd-dns DNS2
Router(policy SSL_VPN_TEST)# network-extension network NETWORK1
Router(policy SSL_VPN_TEST)# eps activate
Router(policy SSL_VPN_TEST)# eps 1 EPS-1
Router(policy SSL_VPN_TEST)# exit
```

**6** Displays the SSL VPN rule settings.

```
Router(config)# show sslvpn policy SSL_VPN_TEST
index: 1
  active: yes
  name: SSL_VPN_TEST
  description:
  user: tester
  ssl application: none
  network extension: yes
  ip pool: IP-POOL
  dns server 1: DNS1
  dns server 2: DNS2
  wins server 1: none
  wins server 2: none
  network: NETWORK1
  cache clean: no
  eps periodical check activation: no
  eps periodical check: 1
  eps activation: yes
  eps: EPS-1
  reference count: 0
```

# 23

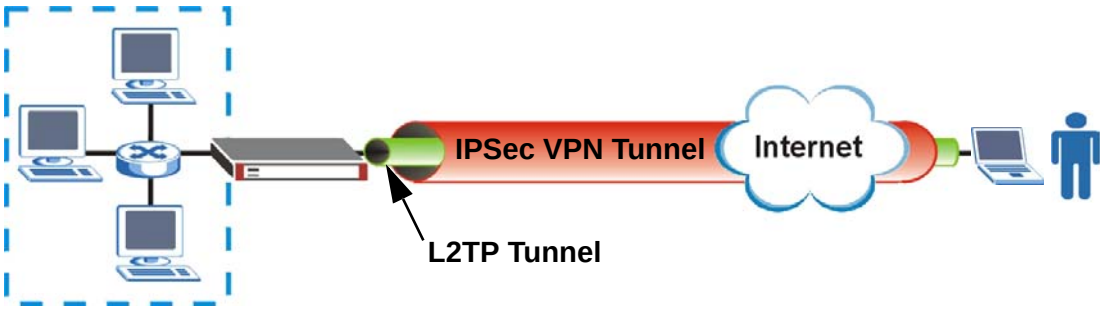
# L2TP VPN

This chapter explains how to set up and maintain L2TP VPNs in the ZyWALL / USG.

## 23.1 L2TP VPN Overview

L2TP VPN lets remote users use the L2TP and IPSec client software included with their computers' operating systems to securely connect to the network behind the ZyWALL / USG. The remote users do not need their own IPSec gateways or VPN client software.

**Figure 22** L2TP VPN Overview




The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peers over another network (like the Internet). In L2TP VPN, an IPSec VPN tunnel is established first (see Chapter 21 on page 177 for information on IPSec) and then an L2TP tunnel is built inside it.

Note: At the time of writing the L2TP remote user must have a public IP address in order for L2TP VPN to work (the remote user cannot be behind a NAT router or a firewall).

## 23.2 IPSec Configuration

You must configure an IPSec VPN connection for L2TP VPN to use (see Chapter 21 on page 177 for details). The IPSec VPN connection must:

- Be enabled.
- Use transport mode.
- Not be a manual key VPN connection.
- Use **Pre-Shared Key** authentication.
- Use a VPN gateway with the **Secure Gateway** set to **0.0.0.0** if you need to allow L2TP VPN clients to connect from more than one IP address.

### 23.2.1 Using the Default L2TP VPN Connection

**Default_L2TP_VPN_Connection** is pre-configured to be convenient to use for L2TP VPN. If you use it, edit the following.

Configure the local and remote policies as follows.

- For the **Local Policy**, create an address object that uses host type and contains the **My Address** IP address that you configured in the **Default_L2TP_VPN_GW**. Use this address object in the local policy.
- For the **Remote Policy**, create an address object that uses host type and an IP address of 0.0.0.0. Use this address object in the remote policy.

You must also edit the **Default_L2TP_VPN_GW** gateway entry.

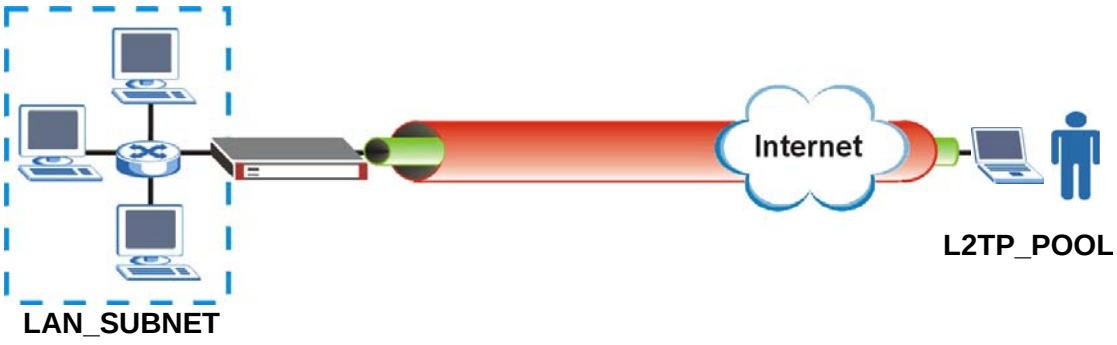
- Configure the **My Address** setting according to your requirements.
- Replace the default **Pre-Shared Key**.

## 23.3 Policy Route

You must configure a policy route to let remote users access resources on a network behind the ZyWALL / USG.

- Set the policy route's **Source Address** to the address object that you want to allow the remote users to access (**LAN_SUBNET** in the following figure).
- Set the **Destination Address** to the IP address pool that the ZyWALL / USG assigns to the remote users (**L2TP_POOL** in the following figure).

**Figure 23** Policy Route for L2TP VPN



# 23.4 L2TP VPN Commands

The following table describes the values required for some L2TP VPN commands. Other values are discussed with the corresponding commands.

**Table 97** Input Values for L2TP VPN Commands

| LABEL | DESCRIPTION |
|---|---|
| *address_object* | The name of an IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *interface_name* | The name of the interface.<br><br>Ethernet interface: For ~~the~~some ZyWALL / USG ~~USG 300 and above~~models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model.<br><br>~~The~~For other ZyWALL / USG ~~USG 200 and lower~~ models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.<br><br>VLAN interface: vlan*x*, *x* = 0 - 4094<br><br>bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ZyWALL / USG model supports. |
| *ppp_interface* | PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL / USG model supports. |
| *map_name* | The name of an IPSec SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *user_name* | The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |

The following sections list the L2TP VPN commands.

## 23.4.1 L2TP VPN Commands

This table lists the commands for L2TP VPN. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 98** L2TP VPN Commands

| COMMAND | DESCRIPTION |
|---|---|
| `l2tp-over-ipsec recover default-ipsec-policy` | If the default L2TP IPSec policy has been deleted, use this command to recreate it (with the default settings). |
| `[no] l2tp-over-ipsec activate;` | Turns L2TP VPN on. The `no` command turns it off. |
| `l2tp-over-ipsec crypto` *map_name* | Specifies the IPSec VPN connection the ZyWALL / USG uses for L2TP VPN. It must meet the requirements listed in Section 23.2 on page 193.<br><br>Note: Modifying this VPN connection (or the VPN gateway that it uses) disconnects any existing L2TP VPN sessions. |
| `l2tp-over-ipsec pool` *address-object* | Specifies the address object that defines the pool of IP addresses that the ZyWALL / USG uses to assign to the L2TP VPN clients. |
| `l2tp-over-ipsec authentication` *aaa authentication profile_name* | Specifies how the ZyWALL / USG authenticates a remote user before allowing access to the L2TP VPN tunnel.<br><br>The authentication method has the ZyWALL / USG check a user's user name and password against the ZyWALL / USG's local database, a remote LDAP, RADIUS, a Active Directory server, or more than one of these. |

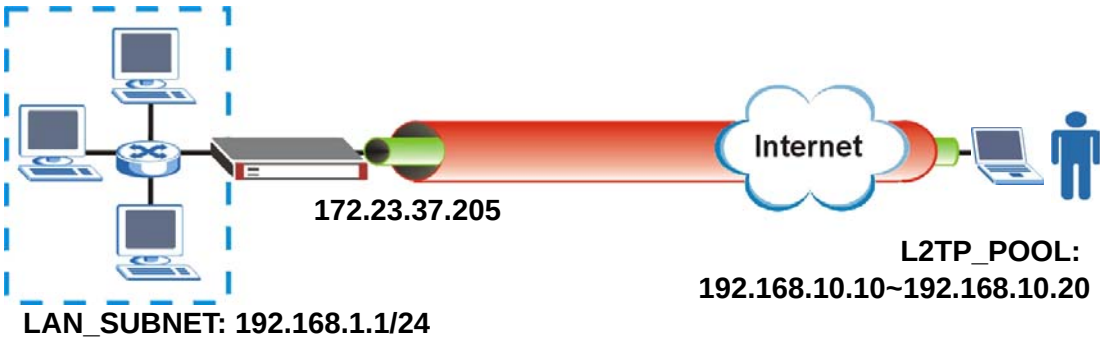
**Table 98** L2TP VPN Commands

| COMMAND | DESCRIPTION |
|---|---|
| certificate *cert_name* | Select the certificate to use to identify the ZyWALL / USG for L2TP VPN connections. The certificate is used with the EAP, PEAP, and MSCHAPv2 authentication protocols. The certificate must already be configured. |
| [no] l2tp-over-ipsec user user_name | Specifies the user or user group that can use the L2TP VPN tunnel. If you do not configure this, any user with a valid account and password on the ZyWALL / USG to log in. The no command removes the user name setting. |
| [no] l2tp-over-ipsec keepalive-timer <1..180> | The ZyWALL / USG sends a Hello message after waiting this long without receiving any traffic from the remote user. The ZyWALL / USG disconnects the VPN tunnel if the remote user does not respond. The no command returns the default setting. |
| [no] l2tp-over-ipsec first-dns-server {*ip* \| *interface_name*} {1st-dns\|2nd-dns\|3rd-dns}\| {*ppp_interface*\|aux}{1st-dns\|2nd-dns}} | Specifies the first DNS server IP address to assign to the remote users. You can specify a static IP address, or a DNS server that an interface received from its DHCP server. The no command removes the setting. |
| [no] l2tp-over-ipsec second-dns-server {*ip* \| *interface_name*} {1st-dns\|2nd-dns\|3rd-dns}\| {*ppp_interface*\|aux}{1st-dns\|2nd-dns}} | Specifies the second DNS server IP address to assign to the remote users. You can specify a static IP address, or a DNS server that an interface received from its DHCP server. The no command removes the setting. |
| [no] l2tp-over-ipsec first-wins-server *ip* | Specifies the first WINS server IP address to assign to the remote users. The no command removes the setting. |
| [no] l2tp-over-ipsec second-wins-server *ip* | Specifies the second WINS server IP address to assign to the remote users. The no command removes the setting. |
| no l2tp-over-ipsec session tunnel-id <0..65535> | Deletes the specified L2TP VPN tunnel. |
| show l2tp-over-ipsec | Displays the L2TP VPN settings. |
| show l2tp-over-ipsec session | Displays current L2TP VPN sessions. |

# 23.5 L2TP VPN Example

This example uses the following settings in creating a basic L2TP VPN tunnel. See the Web Configurator User's Guide for how to configure L2TP in remote user computers using Windows XP and Windows 2000.

**Figure 24** L2TP VPN Example




- The ZyWALL / USG has a static IP address of 172.23.37.205 for the ge3 interface.
- The remote user has a dynamic public IP address and connects through the Internet.

- You configure an IP address pool object named **L2TP_POOL** to assign the remote users IP addresses from 192.168.10.10 to 192.168.10.20 for use in the L2TP VPN tunnel.
- The VPN rule allows the remote user to access the **LAN_SUBNET** which covers the 192.168.1.1/ 24 subnet.

## 23.5.1 Configuring the Default L2TP VPN Gateway Example

The following commands configure the **Default_L2TP_VPN_GW** entry.

- Configure the **My Address** setting. This example uses interface ge3 with static IP address 172.23.37.205.
- Configure the **Pre-Shared Key**. This example uses “top-secret”.

```
Router(config)# isakmp policy Default_L2TP_VPN_GW
Router(config-isakmp Default_L2TP_VPN_GW)# local-ip interface ge3
Router(config-isakmp Default_L2TP_VPN_GW)# authentication pre-share
Router(config-isakmp Default_L2TP_VPN_GW)# keystring top-secret
Router(config-isakmp Default_L2TP_VPN_GW)# activate
Router(config-isakmp Default_L2TP_VPN_GW)# exit
Router(config)#
```

## 23.5.2 Configuring the Default L2TP VPN Connection Example

The following commands configure the **Default_L2TP_VPN_Connection** entry.

Enforce and configure the local and remote policies.

- For the **Local Policy**, create an address object that uses host type and contains the **My Address** IP address that you configured in the **Default_L2TP_VPN_GW**. The address object in this example uses IP address 172.23.37.205 and is named **L2TP_IFACE**.
- For the **Remote Policy**, create an address object that uses host type and an IP address of 0.0.0.0. It is named **L2TP_HOST** in this example.

```
Router(config)# crypto map Default_L2TP_VPN_Connection
Router(config-crypto Default_L2TP_VPN_Connection)# policy-enforcement
Router(config-crypto Default_L2TP_VPN_Connection)# local-policy L2TP_IFACE
Router(config-crypto Default_L2TP_VPN_Connection)# remote-policy L2TP_HOST
Router(config-crypto Default_L2TP_VPN_Connection)# activate
Router(config-crypto Default_L2TP_VPN_Connection)# exit
Router(config)#
```

## 23.5.3 Configuring the L2TP VPN Settings Example

The following commands configure and display the L2TP VPN settings.

- Set it to use the **Default_L2TP_VPN_Connection** VPN connection.
- Configure an IP address pool for the range of 192.168.10.10 to 192.168.10.20. In this example it is already created and called **L2TP_POOL**.
- This example uses the default authentication method (the ZyWALL / USG’s local user data base).
- Select a user or group of users that can use the tunnel. Here a user account named **L2TP-test** has been created.
- The other settings are left to the defaults in this example.

- Enable the connection.

```
Router(config)# l2tp-over-ipsec crypto Default_L2TP_VPN_Connection
Router(config)# l2tp-over-ipsec pool L2TP_POOL
Router(config)# l2tp-over-ipsec authentication default
Router(config)# l2tp-over-ipsec user L2TP-test
Router(config)# l2tp-over-ipsec activate
Router(config)# show l2tp-over-ipsec
L2TP over IPSec:
  activate          : yes
  crypto            : Default_L2TP_VPN_Connection
  address pool      : L2TP_POOL
  authentication    : default
  user              : L2TP-test
  keepalive timer   : 60
  first dns server  : aux 1st-dns
  second dns server : aux 1st-dns
  first wins server :
  second wins server:
```

## 23.5.4 Configuring the Policy Route for L2TP Example

The following commands configure and display the policy route for the L2TP VPN connection entry.

- Set the policy route's **Source Address** to the address object that you want to allow the remote users to access (**LAN_SUBNET** in this example).
- Set the **Destination Address** to the IP address pool that the ZyWALL / USG assigns to the remote users (**L2TP_POOL** in this example).
- Set the next hop to be the **Default_L2TP_VPN_Connection** tunnel.
- Enable the policy route.

```
Router(config)# policy 3
Router(policy-route)# source LAN_SUBNET
Router(policy-route)# destination L2TP_POOL
Router(policy-route)# service any
Router(policy-route)# next-hop tunnel Default_L2TP_VPN_ConnectionRouter(policy-
route)# no deactivate
Router(policy-route)# exit
Router(config)# show policy-route 3
index: 3
  active: yes
  description: WIZ_VPN
  user: any
  schedule: none
  interface: ge1
  tunnel: none
  sslvpn: none
  source: PC_SUBNET
  destination: L2TP_POOL
  service: any
  nexthop type: Tunnel
  nexthop: Default_L2TP_VPN_Connection
  bandwidth: 0
  bandwidth priority: 0
  maximize bandwidth usage: no
  SNAT: none
  amount of port trigger: 0
```

# 24

# Application Patrol

This chapter describes how to set up application patrol for the ZyWALL / USG.

## 24.1 Application Patrol Overview

Application patrol provides a convenient way to manage the use of various applications on the network. It manages general protocols (for example, http and ftp) and instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), and streaming (RSTP) applications. You can even control the use of a particular application's individual features (like text messaging, voice, video conferencing, and file transfers). Application patrol also has powerful bandwidth management including traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

Note: The ZyWALL / USG checks firewall rules before application patrol rules for traffic going through the ZyWALL / USG. To use a service, make sure both the firewall and application patrol allow the service's packets to go through the ZyWALL / USG.

Application patrol examines every TCP and UDP connection passing through the ZyWALL / USG and identifies what application is using the connection. Then, you can specify, by application, whether or not the ZyWALL / USG continues to route the connection.

## 24.2 Application Patrol Commands Summary

The following table describes the values required for many application patrol commands. Other values are discussed with the corresponding commands.

**Table 99** Input Values for Application Patrol Commands

| LABEL | DESCRIPTION |
|---|---|
| *protocol_name* | The name of a pre-defined application. These are listed by category.<br>general: ftp \| smtp \| pop3 \| irc \| http<br>im: msn \| aol-icq \| yahoo \| qq<br>p2p: bittorrent \| eDonkey \| fasttrack \| gnutella \| napster \| h323 \| sip \| soulseek<br>stream: rtsp |
| *rule_number* | The number of an application patrol rule. 1 - *X* where *X* is the highest number of rules the ZyWALL / USG model supports. See the ZyWALL / USG's User's Guide for details. |

**Table 99** Input Values for Application Patrol Commands (continued)

| LABEL | DESCRIPTION |
|---|---|
| *zone_name* | The name of a zone. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *schedule_name* | The name of a schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |

The following sections list the application patrol commands.

## 24.2.1 Pre-defined Application Commands

This table lists the commands for each pre-defined application.

**Table 100** app Commands: Pre-Defined Applications

| COMMAND | DESCRIPTION |
|---|---|
| [no] app *protocol_name* activate | Enables application patrol for the specified application. The no command disables application patrol for the specified application. |
| [no] app *protocol_name* allowport <1..65535> | If the default action is drop or reject. Adds the specified port to the list of ports that are forwarded in spite of the default action. The no command removes the specified port from the list. |
| app *protocol_name* bandwidth <0..102400> | Specifies the bandwidth limit (in kilobits per second) for the specified application. |
| bandwidth-graph | |
| [no] app *protocol_name* bwm | Turns on bandwidth management for the specified application. The no command turns off bandwidth management for the specified application. |
| [no] app *protocol_name* defaultport <1..65535> | For port-base applications. Adds the specified port to the list of ports used to identify the specified application. This port number can only be included in one application's list. The no command removes the specified port from the list. |
| app *protocol_name* {forward \| drop \| reject} | Specifies what action the ZyWALL / USG should take when it identifies this application. |
| app *protocol_name* mode {portless \| portbase} | Specifies how the ZyWALL / USG identifies this application. |
| [no] app *protocol_name* log [alert] | Creates log entries (and alerts) for the specified application. The no command does not create any log entries. |

## 24.2.2 Rule Commands for Pre-defined Applications

This table lists the commands for rules in each pre-defined application.

**Table 101** app Commands: Rules in Pre-Defined Applications

| COMMAND | DESCRIPTION |
|---|---|
| app *protocol_name* rule insert *rule_number* | Creates a new rule at the specified row and enters sub-command mode. See Table 102 on page 201 for the sub-commands. |
| app *protocol_name* rule append | Creates a new rule, appends it to the end of the list, and enters sub-command mode. See Table 102 on page 201 for the sub-commands. |
| app *protocol_name* rule *rule_number*<br>or<br>app *protocol_name* rule modify *rule_number* | Enters sub-command mode for editing the rule at the specified row. See Table 102 on page 201 for the sub-commands. |

**Table 101** app Commands: Rules in Pre-Defined Applications (continued)

| COMMAND | DESCRIPTION |
|---|---|
| app *protocol_name* rule default<br>or<br>app *protocol_name* rule modify default | Enters sub-command mode for editing the default rule for the application. See Table 102 on page 201 for the sub-commands. |
| no app *protocol_name* rule *rule_number* | Deletes the specified rule. |

### 24.2.2.1 Rule Sub-commands

The following table describes the sub-commands for several application patrol rule commands. Note that not all rule commands use all the sub-commands listed here.

**Table 102** app protocol rule Sub-commands

| COMMAND | DESCRIPTION |
|---|---|
| access {forward \| drop \| reject} | Specifies the action when traffic matches the rule. |
| [no] action-block {login\|message\|audio\|video\|file-transfer} | Blocks use of a specific feature. |
| [no] activate | Turns on this rule. The no command turns off this rule. |
| bandwidth {inbound\|outbound} <0..1048576> | Limits inbound or outbound bandwidth, in kilobits per second. 0 disables bandwidth management for traffic matching this rule. |
| [no] bandwidth excess-usage | Enables maximize bandwidth usage to let the traffic matching this policy “borrow” any unused bandwidth on the out-going interface. |
| bandwidth priority <1..7> | Set the priority for traffic that matches this rule. The smaller the number, the higher the priority. |
| [no] destination *profile_name* | Adds the specified destination address to the rule. |
| [no] from *zone_name* | Specifies the source zone. |
| [no] inbound-dscp-mark {<0..63> \| class {default \| *dscp_class*}} | This is how the ZyWALL / USG handles the DSCP value of the outgoing packets to a connection’s initiator that match this policy.<br>Enter a DSCP value to have the ZyWALL / USG apply that DSCP value. Set this to the class default to have the ZyWALL / USG set the DSCP value to 0. |
| [no] log [alert] | Creates log entries (and alerts) for traffic that matches the rule. The no command does not create any log entries. |
| [no] outbound-dscp-mark {<0..63> \| class {default \| *dscp_class*}} | This is how the ZyWALL / USG handles the DSCP value of the outgoing packets from a connection’s initiator that match this policy.<br>Enter a DSCP value to have the ZyWALL / USG apply that DSCP value. Set this to the class default to have the ZyWALL / USG set the DSCP value to 0. |
| port <0..65535> | Specifies the destination port. 0 means any. |
| [no] schedule *profile_name* | Adds the specified schedule to the rule. |
| show | Displays the rule’s configuration |
| [no] source *profile_name* | Adds the specified source address to the rule. |
| [no] to *zone_name* | Specifies the destination zone. |
| [no] user *username* | Adds the specified user to the rule. |

## 24.2.3 Exception Commands for Pre-defined Applications

This table lists the commands for exception rules for application access controls. These commands are used for backward compatible only.

**Table 103** app Commands: Exception Rules in Pre-Defined Applications

| COMMAND | DESCRIPTION |
|---|---|
| app *protocol_name* exception insert *rule_number* | Creates a new rule at the specified row and enters sub-command mode. See Table 104 on page 202 for the sub-commands. |
| app *protocol_name* exception append | Creates a new rule, appends it to the end of the list, and enters sub-command mode. See Table 104 on page 202 for the sub-commands. |
| app *protocol_name* exception *rule_number* | Enters sub-command mode for editing the rule at the specified row. See Table 104 on page 202 for the sub-commands. |
| app *protocol_name* exception *rule_number*<br>or<br>app *protocol_name* exception modify *rule_number* | Enters sub-command mode for editing the rule at the specified row. See Table 104 on page 202 for the sub-commands. |
| app *protocol_name* exception default<br>or<br>app *protocol_name* exception modify default | Enters sub-command mode for editing the default rule for the application. See Table 104 on page 202 for the sub-commands. |
| app *protocol_name* exception move *rule_number* to *rule_number* | Moves the specified rule (first index) to the specified location. The process is (1) remove the specified rule from the table; (2) re-number; (3) insert the rule at the specified location. |

### 24.2.3.1 Exception Rule Sub-commands

The following table describes the sub-commands for several application patrol exception rule commands. Note that not all rule commands use all the sub-commands listed here.

**Table 104** app patrol exception rule Sub-commands

| COMMAND | DESCRIPTION |
|---|---|
| access {forward \| drop \| reject} | Specifies the action when traffic matches the rule. |
| [no] action-block {login\|message\|audio\|video\|file-transfer} | Blocks use of a specific feature. |
| [no] activate | Turns on this rule. The no command turns off this rule. |
| bandwidth {inbound \| outbound} <0..1048576> | Limits inbound or outbound bandwidth, in kilobits per second. 0 disables bandwidth management for traffic matching this rule. |
| [no] bandwidth excess-usage | Enables maximize bandwidth usage to let the traffic matching this policy “borrow” any unused bandwidth on the out-going interface. |
| bandwidth priority <1..7> | Set the priority for traffic that matches this rule. The smaller the number, the higher the priority. |
| [no] destination *profile_name* | Adds the specified destination address to the rule. |
| [no] from *zone_name* | Specifies the source zone. |
| [no] inbound-dscp-mark {<0..63> \| class {default \| *dscp_class*}} | This is how the ZyWALL / USG handles the DSCP value of the outgoing packets to a connection’s initiator that match this policy.<br><br>Enter a DSCP value to have the ZyWALL / USG apply that DSCP value. Set this to the class default to have the ZyWALL / USG set the DSCP value to 0. |
| [no] log [alert] | Creates log entries (and alerts) for traffic that matches the rule. The no command does not create any log entries. |

**Table 104** app patrol exception rule Sub-commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] outbound-dscp-mark {<0..63> \| class {default \| *dscp_class*}} | This is how the ZyWALL / USG handles the DSCP value of the outgoing packets from a connection's initiator that match this policy.<br>Enter a DSCP value to have the ZyWALL / USG apply that DSCP value. Set this to the class default to have the ZyWALL / USG set the DSCP value to 0. |
| port <0..65535> | Specifies the destination port. 0 means any. |
| [no] schedule *profile_name* | Adds the specified schedule to the rule. |
| show | Displays the rule's configuration |
| [no] source *profile_name* | Adds the specified source address to the rule. |
| [no] to *zone_name* | Specifies the destination zone. |
| [no] user *username* | Adds the specified user to the rule. |

## 24.2.4 Other Application Commands

This table lists the commands for other applications in application patrol.

**Table 105** app Commands: Other Applications

| COMMAND | DESCRIPTION |
|---|---|
| app other {del \| forward \| drop \| reject} | Specifies the default action for other applications. |
| [no] app other log [alert] | Creates log entries (and alerts) for other applications. The no command does not create any log entries. |

## 24.2.5 Rule Commands for Other Applications

This table lists the commands for rules in other applications.

**Table 106** app Commands: Rules in Other Applications

| COMMAND | DESCRIPTION |
|---|---|
| app other insert *rule_number* | Creates a new rule at the specified row and enters sub-command mode. |
| app other append | Creates a new rule, appends it to the end of the list, and enters sub-command mode. |
| app other <1..64> | Enters sub-command mode for editing the rule at the specified row. |
| app other default | Enters sub-command mode for editing the default rule for traffic of an unidentified application. |
| app other move *rule_number* to *rule_number* | Moves the specified rule (first index) to the specified location. The process is (1) remove the specified rule from the table; (2) re-number; (3) insert the rule at the specified location. |
| no app other *rule_number* | Deletes the specified rule. |

### 24.2.5.1 Other Rule Sub-commands

The following table describes the sub-commands for several application patrol other rule commands. Note that not all rule commands use all the sub-commands listed here.

**Table 107** app patrol other rule Sub-commands

| COMMAND | DESCRIPTION |
|---|---|
| [no] activate | Turns on this rule. The no command turns off this rule. |
| [no] port <0..65535> | Specifies the destination port. 0 means any. |
| [no] schedule *profile_name* | Adds the specified schedule to the rule. |
| [no] user *username* | Adds the specified user to the rule. |
| [no] from *zone_name* | Specifies the source zone. |
| [no] to *zone_name* | Specifies the destination zone. |
| [no] source *profile_name* | Adds the specified source address to the rule. |
| [no] destination *profile_name* | Adds the specified destination address to the rule. |
| [no] protocol {tcp \| udp} | Adds the specified protocol to the rule. |
| access {forward \| drop \| reject} | Specifies the action when traffic matches the rule. |
| [no] action-block {login\|message\|audio\|video\|file-transfer} | Blocks use of a specific feature. |
| bandwidth {inbound\|outbound} <0..1048576> | Limits inbound or outbound bandwidth, in kilobits per second. 0 disables bandwidth management for traffic matching this rule. |
| [no] bandwidth excess-usage | Enables maximize bandwidth usage to let the traffic matching this policy “borrow” any unused bandwidth on the out-going interface. |
| bandwidth priority <1..7> | Set the priority for traffic that matches this rule. The smaller the number, the higher the priority. |
| [no] inbound-dscp-mark {<0..63> \| class {default \| *dscp_class*}} | This is how the ZyWALL / USG handles the DSCP value of the outgoing packets to a connection’s initiator that match this policy.<br>Enter a DSCP value to have the ZyWALL / USG apply that DSCP value. Set this to the class default to have the ZyWALL / USG set the DSCP value to 0. |
| [no] log [alert] | Creates log entries (and alerts) for traffic that matches the rule. The no command does not create any log entries. |
| [no] outbound-dscp-mark {<0..63> \| class {default \| *dscp_class*}} | This is how the ZyWALL / USG handles the DSCP value of the outgoing packets from a connection’s initiator that match this policy.<br>Enter a DSCP value to have the ZyWALL / USG apply that DSCP value. Set this to the class default to have the ZyWALL / USG set the DSCP value to 0. |
| show | Displays the rule’s configuration |

## 24.2.6 General Commands for Application Patrol

Note: You must register for the IDP/AppPatrol signature service (at least the trial) before you can use it. See Chapter 5 on page 47.

This table lists the general commands for application patrol.

**Table 108** app Commands: Pre-Defined Applications

| COMMAND | DESCRIPTION |
|---|---|
| [no] app activate | Turns on application patrol. The no command turns off application patrol. |
| [no] app highest sip bandwidth priority | Turns the option to maximize the throughput of SIP traffic on or off. |
| [no] app *protocol_name* bandwidth-graph | Sets the specified protocol to display on the bandwidth statistics graph. The no command has it not display on the bandwidth statistics graph. |
| [no] app other *protocol_name* bandwidth-graph | Sets traffic for unidentified applications to display on the bandwidth statistics graph. The no command it not display on the bandwidth statistics graph. |
| [no] bwm activate | Globally enables bandwidth management. You must globally activate bandwidth management to have individual policy routes or application patrol policies apply bandwidth management. The no command globally disables bandwidth management. |
| show app config | Displays whether or not application patrol is active. |
| show app all | Displays the settings for all applications. |
| show app all defaultport | Displays the default port settings for all applications. |
| show app all statistics | Displays statistics for all applications. |
| show app {general\|im\|p2p\|stream} | Displays protocols by category. |
| show app im support action | Displays the supported actions of each Instant Messenger application. |
| show app *protocol_name* config | Displays the basic configuration of this application. |
| show app *protocol_name* defaultport | Displays the default ports of this application. |
| show app *protocol_name* statistics | Display the statistics of this application. |
| show app *protocol_name* rule *rule_number* | Displays the rule configuration of this application. |
| show app *protocol_name* rule *rule_number* statistics | Displays the rule statistics of this application. |
| show app *protocol_name* rule default | Displays the default rule configuration of this application. |
| show app *protocol_name* rule default statistics | Displays the default rule statistics of this application. |
| show app *protocol_name* rule all | Displays the configurations of all the rules for this application. |
| show app *protocol_name* rule all statistics | Displays all the rule statistics for this application. |
| show app other config | Displays the basic configuration for other applications, |
| show app other statistics | Displays statistics for other applications. |
| show app other rule *rule_number* | Displays the rule's configuration. |
| show app other rule *rule_number* statistics | Displays the rule's statistics. |
| show app other rule default | Displays the default rule's configuration. |
| show app other rule default statistics | Displays the default rule's statistics. |
| show app other rule all | Displays the configurations of all the rules for other applications. |
| show app other rule all statistics | Displays all the rule statistics for other applications. |

**Table 108** app Commands: Pre-Defined Applications (continued)

| COMMAND | DESCRIPTION |
|---|---|
| show app highest sip bandwidth priority | Displays whether or not the option to maximize the throughput of SIP traffic is enabled. |
| show bwm activation | Displays whether or not the global setting for bandwidth management on the ZyWALL / USG is enabled. |

### 24.2.6.1 General Command Examples

The following examples show the information that is displayed by some of the `show` commands.

```
Router> configure terminal
Router(config)# show bwm activation
bwm activation: yes
```

```
Router# configure terminal
Router(config)# show app http config
application: http
  active: yes
  mode: portless
  default access: forward
  bandwidth graph: yes
```

```
Router# configure terminal
Router(config)# show app http defaultport
No.   Port
================================================================================
1     80
```

```
Router# configure terminal
Router(config)# show app http rule all
index: default
  activate: yes
  port: 0
  schedule: none
  user: any
  from zone: any
  to zone: any
  source address: any
  destination address: any
  access: forward
  action login: na
  action message: na
  action audio: na
  action video: na
  action file-transfer: na
  DSCP inbound marking: preserve
  DSCP outbound marking: preserve
  bandwidth excess-usage: no
  bandwidth priority: 1
  bandwidth inbound: 0
  bandwidth outbound: 0
  log: no
```

```
Router# configure terminal
Router(config)# show app other config
bandwidth-graph: yes
```

```
Router# configure terminal
Router(config)# show app other rule all
index: 1
  activate: yes
  port: 5963
  schedule: none
  user: any
  from zone: any
  to zone: any
  source address: any
  destination address: any
  protocol: tcp
  access: forward
  DSCP inbound marking: preserve
  DSCP outbound marking: preserve
  bandwidth excess-usage: no
  bandwidth priority: 1
  bandwidth inbound: 0
  bandwidth outbound: 0
  log: no
index: default
  activate: yes
  port: 0
  schedule: none
  user: any
  from zone: any
  to zone: any
  source address: any
  destination address: any
  protocol: any
  access: forward
  DSCP inbound marking: preserve
  DSCP outbound marking: preserve
  bandwidth excess-usage: no
  bandwidth priority: 1
  bandwidth inbound: 0
  bandwidth outbound: 0
  log: no
```

# 25

# Anti-Virus

This chapter introduces and shows you how to configure the anti-virus scanner.

## 25.1 Anti-Virus Overview

A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a self-replicating virus that resides in active memory and duplicates itself. The effect of a virus attack varies from doing so little damage that you are unaware your computer is infected to wiping out the entire contents of a hard drive to rendering your computer inoperable.

## 25.2 Anti-virus Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 109** Input Values for General Anti-Virus Commands

| LABEL | DESCRIPTION |
|---|---|
| *zone_object* | The name of the zone. For ~~the~~some ZyWALL / USG ~~USG 300 and above~~models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.<br><br>~~The~~For other ZyWALL / USG ~~USG 200 and lower~~ models use pre-defined zone names like DMZ, LAN1, SSL VPN, WLAN, IPSec VPN, OPT, and WAN. |
| *av_file_pattern* | Use up to 80 characters to specify a file pattern. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed.<br><br>A question mark (?) lets a single character in the file name vary. For example, use “a?.zip” (without the quotation marks) to specify aa.zip, ab.zip and so on.<br><br>Wildcards (*) let multiple files match the pattern. For example, use “*a.zip” (without the quotation marks) to specify any file that ends with “a.zip”. A file named “testa.zip” would match. There could be any number (of any type) of characters in front of the “a.zip” at the end and the file name would still match. A file named “test.zipa” for example would not match.<br><br>A * in the middle of a pattern has the ZyWALL / USG check the beginning and end of the file name and ignore the middle. For example, with “abc*.zip”, any file starting with “abc” and ending in “.zip” matches, no matter how many characters are in between.<br><br>The whole file name has to match if you do not use a question mark or asterisk.<br><br>If you do not use a wildcard, the ZyWALL / USG checks up to the first 80 characters of a file name. |

## 25.2.1 General Anti-virus Commands

The following table describes general anti-virus commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Note: You must register for the anti-virus service before you can use it (see Chapter 5 on page 47).

**Table 110** General Anti-virus Commands

| COMMAND | DESCRIPTION |
|---|---|
| `[no] anti-virus activate` | Enables anti-virus service. Anti-virus service also depends on anti-virus service registration. |
| `show anti-virus activation` | Displays anti-virus service status. |
| `[no] anti-virus eicar activate` | Turns detection of the EICAR test file on or off. |
| `show anti-virus eicar activation` | Displays whether or not detection of the EICAR test file is turned on. |
| `anti-virus reload signatures` | Recovers the anti-virus signatures. You should only need to do this if instructed to do so by a support technician. |
| `[no] anti-virus skip-unknown-file-type activate` | Sets whether or not anti-virus checks files for which the ZyWALL / USG cannot identify a type. |
| `show anti-virus skip-unknown-file-type activation` | Displays whether or not anti-virus checks files for which the ZyWALL / USG cannot identify a type. |
| `anti-virus mail-infect-ext activate` | Has the ZyWALL / USG add a notification text file to an e-mail after destroying a virus-infected e-mail attachment. |
| `no anti-virus mail-infect-ext activate` | Has the ZyWALL / USG not add a notification text file to an e-mail after destroying a virus-infected e-mail attachment. |

### 25.2.1.1 Activate/Deactivate Anti-Virus Example

This example shows how to activate and deactivate anti-virus on the ZyWALL / USG.

```
Router# configure terminal
Router(config)# anti-virus activate
Router(config)# show anti-virus activation
anti-virus activation: yes
Router(config)# no anti-virus activate
Router(config)# show anti-virus activation
anti-virus activation: no
Router(config)#
```

## 25.2.2 Zone to Zone Anti-virus Rules

The following table describes the commands for configuring the zone to zone rules. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 111** Commands for Zone to Zone Anti-Virus Rules

| COMMAND | DESCRIPTION |
|---|---|
| `anti-virus rule append` | Enters the anti-virus sub-command mode to add a direction specific rule. |
| `anti-virus rule insert <1..32>` | Enters the anti-virus sub-command mode to add a direction specific rule. |

**Table 111** Commands for Zone to Zone Anti-Virus Rules (continued)

| COMMAND | DESCRIPTION |
|---|---|
| `anti-virus rule <1..32>` | Enters the anti-virus sub-command mode to edit the specified direction specific rule. |
| `[no] activate` | Turns a direction specific anti-virus rule on or off. |
| `[no] log [alert]` | Sets the ZyWALL / USG to create a log (and optionally an alert) when packets match this rule and are found to be virus-infected. The `no` command sets the ZyWALL / USG not to create a log or alert when packets match this rule. |
| `[no] from` *zone_object* | Sets the zone on which the packets are received. The `no` command removes the zone on which the packets are received and resets it to the default (`any`). `any` means all interfaces or VPN tunnels. |
| `[no] to` *zone_object* | Sets the zone to which the packets are sent. The `no` command removes the zone to which the packets are sent and resets it to the default (`any`). `any` means all interfaces or VPN tunnels. |
| `[no] scan {http \| ftp \| imap4 \| smtp \| pop3}` | Sets the protocols of traffic to scan for viruses. |
| `[no] infected-action {destroy \| send-win-msg}` | Sets the action to take when the ZyWALL / USG detects a virus in a file. The file can be destroyed (filled with zeros from the point where the virus was found). The ZyWALL / USG can also send a message alert to the file's intended user using a Microsoft Windows computer connected to the to interface. |
| `[no] bypass {white-list \| black-list}` | Have the ZyWALL / USG not check files against a pattern list. |
| `[no] file-decompression [unsupported destroy]` | Enable file decompression to have the ZyWALL / USG attempt to to decompress zipped files for further scanning. You can also have it destroy the zipped files it cannot decompress due to encryption or system resource limitations. |
| `show [all]` | Displays the details of the anti-virus rule you are configuring or all the rules. |
| `anti-virus rule move <1..32> to <1..32>` | Moves a direction specific anti-virus rule to the number that you specified. |
| `anti-virus rule delete <1..32>` | Removes a direction specific anti-virus rule. |

#### 25.2.2.1 Zone to Zone Anti-virus Rule Example

This example shows how to configure (and display) a WAN to LAN antivirus rule to scan HTTP traffic and destroy infected files. The white and black lists are ignored and zipped files are decompressed. Any zipped files that cannot be decompressed are destroyed.

```
Router(config)# anti-virus rule 1
Router(config-av-rule-1)# activate
Router(config-av-rule-1)# from-zone WAN
Router(config-av-rule-1)# to-zone LAN
Router(config-av-rule-1)# scan http
Router(config-av-rule-1)# infected-action destroy
Router(config-av-rule-1)# bypass white-list
Router(config-av-rule-1)# no bypass black-list
Router(config-av-rule-1)# file-decompression
Router(config-av-rule-1)# no file-decompression unsupported destroy
Router(config-av-rule-1)# exit
Router(config)# show anti-virus rule 1
Anti-Virus Rule: 1
 active: yes
 log: log
 from zone: WAN
 to zone: LAN
 scan protocols:
   http: yes
   ftp : yes
   smtp: yes
   pop3: yes
   imap4: yes
 infected action:
   destroy: yes
   send windows message: yes
 bypass white list: yes
 bypass black list: no
 file decompression: yes
   destroy unsupported compressed file: no
```

## 25.2.3 White and Black Lists

The following table describes the commands for configuring the white list and black list. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 112** Commands for Anti-virus White and Black Lists

| COMMAND | DESCRIPTION |
|---|---|
| `[no] anti-virus white-list activate` | Turn on the white list to have the ZyWALL / USG not perform the anti-virus check on files with names that match the white list patterns. |
| `[no] anti-virus white-list file-pattern` *`av_file_pattern`* `{activate\|deactivate}` | Adds or removes a white list file pattern. Turns a file pattern on or off. |
| `anti-virus white-list replace` *`old_av_file_pattern new_av_file_pattern`* `{activate\|deactivate}` | Replaces the specified white list file pattern with a new file pattern. |
| `[no] anti-virus black-list activate` | Turn on the black list to log and delete files with names that match the black list patterns. |

**Table 112** Commands for Anti-virus White and Black Lists (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] anti-virus black-list file-pattern *av_file_pattern* {activate\|deactivate} | Adds or removes a black list file pattern. Turns a file pattern on or off. |
| anti-virus black-list replace *old_av_file_pattern new_av_file_pattern* {activate\|deactivate} | Replaces the specified black list file pattern with a new file pattern. |

### 25.2.3.1 White and Black Lists Example

This example shows how to enable the white list and configure an active white list entry for files with a .exe extension. It also enables the black list and configure an inactive black list entry for files with a .exe extension.

```
Router(config)# anti-virus white-list activate
Router(config)# anti-virus white-list file-pattern
Router(config)# anti-virus white-list file-pattern *.exe activate
Router(config)# anti-virus black-list activate
Router(config)# anti-virus black-list file-pattern *.exe deactivate
Router(config)# show anti-virus white-list status
anti-virus white-list status: yes
Router(config)# show anti-virus white-list
No.  Status
File-Pattern
==========================================================================
1    yes
*.exe
Router(config)# show anti-virus black-list status
anti-virus black-list status: yes
Router(config)# show anti-virus black-list
No.  Status
File-Pattern
==========================================================================
1    no
*.exe
```

## 25.2.4 Signature Search Anti-virus Command

The following table describes the command for searching for signatures. You must use the `configure terminal` command to enter the configuration mode before you can use this command.

**Table 113** Command for Anti-virus Signature Search

| COMMAND | DESCRIPTION |
|---|---|
| anti-virus search signature {all \| category *category* \| id *id* \| name *name* \| severity *severity* [{from *id* to *id*}] | Search for signatures by their ID, name, severity, or category.<br>all: displays all signatures.<br>category: select whether you want to see virus signatures or spyware signatures.<br>*id*: type the ID or part of the ID of the signature you want to find.<br>*name*: type the name or part of the name of the signature(s) you want to find. This search is not case-sensitive.<br>*severity*: type the severity level of the signatures you want to find (high, medium, or low). |

#### 25.2.4.1 Signature Search Example

This example shows how to search for anti-virus signatures with MSN in the name.

```
Router(config)# anti-virus search signature name MSN
signature: 1
 virus id: 41212
 virus name: MSN
 category: virus
 severity: Low
```

## 25.3 Update Anti-virus Signatures

Use these commands to update new signatures. You should have already registered for anti-virus service.

**Table 114** Update Signatures

| COMMAND | DESCRIPTION |
|---|---|
| anti-virus update signatures | Immediately downloads signatures from an update server. |
| [no] anti-virus update auto | Enables (disables) automatic signature downloads at regular times and days. |
| anti-virus update hourly | Enables automatic signature download every hour. |
| anti-virus update daily <0..23> | Enables automatic signature download every day at the time specified. |
| anti-virus update weekly {sun \| mon \| tue \| wed \| thu \| fri \| sat} <0..23> | Enables automatic signature download once-a-week at the time and day specified. |
| show anti-virus update | Displays signature update schedule. |
| show anti-virus update status | Displays signature update status. |
| show anti-virus signatures status | Displays details about the current signature set. |

### 25.3.1 Update Signature Examples

These examples show how to enable/disable automatic anti-virus downloading, schedule updates, display the schedule, display the update status, show the (new) updated signature version number, show the total number of signatures and show the date/time the signatures were created.

```
Router# configure terminal
Router(config)# anti-virus update signatures
ANTI-VIRUS signature update in progress.
Please check system log for future information.
Router(config)# anti-virus update auto
Router(config)# no anti-virus update auto
Router(config)# anti-virus update hourly
Router(config)# anti-virus update daily 10
Router(config)# anti-virus update weekly fri 13
Router(config)# show anti-virus update
auto: yes
schedule: weekly at Friday 13 o'clock
Router(config)# show anti-virus update status
current status: Anti-Virus Current signature version 1.046 on device is latest at
Tue Apr 17 10:18:00 2007
last update time: 2007/04/07 10:41:01
Router(config)# show anti-virus signatures status
current version : 1.046
release date    : 2007/04/06 10:41:29
signature number: 4124
```

## 25.4 Anti-virus Statistics

The following table describes the commands for collecting and displaying anti-virus statistics. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 115** Commands for Anti-virus Statistics

| COMMAND | DESCRIPTION |
|---|---|
| `[no] anti-virus statistics collect` | Turn the collection of anti-virus statistics on or off. |
| `anti-virus statistics flush` | Clears the collected statistics. |
| `show anti-virus statistics summary` | Displays the collected statistics. |
| `show anti-virus statistics collect` | Displays whether the collection of anti-virus statistics is turned on or off. |
| `show anti-virus statistics ranking {destination \| source \| virus-name}` | Query and sort the anti-virus statistics entries by destination IP address, source IP address, or virus name. `virus-name`: lists the most common viruses detected.<br>`source`: lists the source IP addresses of the most virus-infected files.<br>`destination`: lists the most common destination IP addresses for virus-infected files. |

### 25.4.1 Anti-virus Statistics Example

This example shows how to collect and display anti-virus statistics. It also shows how to sort the display by the most common destination IP addresses.

```
Router(config)# anti-virus statistics collect
Router(config)# show anti-virus statistics collect
collect statistics: yes
Router(config)# show anti-virus statistics summary
file scanned  : 0
virus detected: 0
Router(config)# show anti-virus statistics ranking destination
```

# 26

# IDP Commands

This chapter introduces IDP-related commands.

## 26.1 Overview

Commands mostly mirror web configurator features. It is recommended you use the web configurator for IDP features such as searching for web signatures, creating/editing an IDP profile or creating/editing a custom signature. Some web configurator terms may differ from the command-line equivalent.

Note: The “no” command negates the action or returns it to the default value.

The following table lists valid input for IDP commands.

**Table 116** Input Values for IDP Commands

| LABEL | DESCRIPTION |
|---|---|
| *zone_profile* | The name of a zone. For ~~the~~some ZyWALL / USG ~~USG 300 and above~~models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.<br><br>~~The~~For other ZyWALL / USG ~~USG 200 and lower~~ models use pre-defined zone names like DMZ, LAN1, SSL VPN, WLAN, IPSec VPN, OPT, and WAN. |
| *idp_profile* | The name of an IDP profile. It can consist of alphanumeric characters, the underscore, and the dash, and it is 1-31 characters long. Spaces are not allowed. |

## 26.2 General IDP Commands

### 26.2.1 IDP Activation

Note: You must register for the IDP/AppPatrol signature service (at least the trial) before you can use it. See Chapter 5 on page 47.

This table shows the IDP signature, anomaly, and system-protect activation commands.

**Table 117** IDP Activation

| COMMAND | DESCRIPTION |
|---|---|
| [no] idp {signature \| anomaly \| system-protect} activate | Enables IDP signatures, anomaly detection, and/or system-protect. IDP signatures use requires IDP service registration. If you don't have a standard license, you can register for a once-off trial one. Anomaly detection and the self-protect feature do not require registration. The no command disables the specified service. |
| idp system-protect deactivate | Disables system-protect. |
| show idp {signature \| anomaly \| system-protect} activation | Displays IDP signature, anomaly detection, or system protect service status. |
| idp reload | Recovers the IDP signatures. You should only need to do this if instructed to do so by a support technician. |

#### 26.2.1.1 Activate/Deactivate IDP Example

This example shows how to activate and deactivate signature-based IDP on the ZyWALL / USG.

```
Router# configure terminal
Router(config)# idp signature activate
Router(config)# show idp signature activation
idp signature activation: yes
Router(config)# no idp signature activate
Router(config)# show idp signature activation
idp signature activation: no
```

# 26.3 IDP Profile Commands

## 26.3.1 Global Profile Commands

Use these commands to rename or delete existing profiles and show IDP base profiles.

**Table 118** Global Profile Commands

| COMMAND | DESCRIPTION |
|---|---|
| idp rename {signature \| anomaly} *profile1 profile2* | Rename an IDP signature or anomaly profile originally named *profile1* to *profile2*. |
| no idp {signature \| anomaly} *profile3* | Delete an IDP signature or system protect profile named *profile3*. |
| show idp signature *profile* signature all details | Lists the settings for all of the specified profile's signatures. Use \|more to display the settings page by page. |
| show idp signature all details | Lists the settings for all of the signatures. Use \|more to display the settings page by page. |
| show idp {signature \| anomaly} base profile | Displays all IDP signature or system protect base profiles. |
| show idp signature base profile {all\|none\|wan\|lan\|dmz} settings | Lists the specified signature base profile's settings. Use \|more to display the settings page by page. |
| show idp profiles | Displays all IDP signature profiles. |

#### 26.3.1.1 Example of Global Profile Commands

In this example we rename an IDP signature profile from “old_profile” to “new_profile”, delete the “bye_profile” and show all base profiles available.

```
Router# configure terminal
Router(config)# idp rename signature old_profile new_profile
Router(config)# no idp signature bye_profile
Router(config)# show idp signature base profile
No.  Base Profile Name
============================================================
1    none
2    all
3    wan
4    lan
5    dmz
Router(config)#
```

## 26.3.2 IDP Zone to Zone Rules

Use the following rules to apply IDP profiles to specific directions of packet travel.

**Table 119** IDP Zone to Zone Rule Commands

| COMMAND | DESCRIPTION |
|---|---|
| idp {signature\| anomaly } rule { append \| <1..32> \| insert <1..32> } | Create an IDP signature or anomaly rule and enter the sub-command mode. |
| bind *profile* | Binds the IDP profile to the entry’s traffic direction. |
| no bind | Removes the IDP profile’s binding. |
| [no] from-zone *zone_profile* | Specifies the zone the traffic is coming from. The no command removes the zone specification. |
| [no] to-zone *zone_profile* | Specifies the zone the traffic is going to. The no command removes the zone specification. |
| [no] activate | Turns on the IDP profile to traffic direction binding. The no command turns it off. |
| idp {signature\| anomaly } rule { delete <1..32> \| move <1..32> to <1..32> } | Remove or move an IDP profile to traffic direction entry. |
| no idp {signature\| anomaly } rule <1..32> | Removes an IDP profile to traffic direction entry. |
| show idp {signature\| anomaly } rules | Displays the IDP zone to zone rules. |

#### 26.3.2.1 Example of IDP Zone to Zone Rule Commands

The following example creates IDP zone to zone rule one. The rule applies the LAN_IDP profile to all traffic going to the LAN zone.

```
Router# configure terminal
Router(config)# idp signature rule 1
Router(config-idp-signature-1)# from-zone any
Router(config-idp-signature-1)# to-zone LAN
Router(config-idp-signature-1)# bind LAN_IDP
Router(config-idp-signature-1)# activate
Router(config-idp-signature-1)# exit
Router(config)#show idp signature rules
Signature rules
idp rule: 1
  from zone: any
  to zone: LAN
  profile: LAN_IDP
  activate: yes
```

### 26.3.3 Editing/Creating IDP Signature Profiles

Use these commands to create a new IDP signature profile or edit an existing one. It is recommended you use the web configurator to create/edit profiles. If you do not specify a base profile, the default base profile is none.

Note: You CANNOT change the base profile later!

**Table 120** Editing/Creating IDP Signature Profiles

| COMMAND | DESCRIPTION |
|---|---|
| idp signature *newpro* [base {all \| lan \| wan \| dmz \| none}] | Creates a new IDP signature profile called *newpro*. *newpro* uses the base profile you specify. Enters sub-command mode. All the following commands relate to the new profile. Use exit to quit sub-command mode. |
| [no] signature *sid* activate | Activates or deactivates an IDP signature. |
| signature *sid* log [alert] | Sets log or alert options for an IDP signature |
| no signature *sid* log | Deactivates log options for an IDP signature |
| signature *sid* action {drop \| reject-sender \| reject-receiver \| reject-both} | Sets an action for an IDP signature |
| no signature *sid* action | Deactivates an action for an IDP signature. |
| show idp *profile* signature *sid* details | Shows signature ID details of the specified profile. |
| show idp *profile* signature {all \| custom-signature} details | Shows the signature details of the specified profile. |

### 26.3.4 Editing/Creating Anomaly Profiles

Use these commands to create a new anomaly profile or edit an existing one. It is recommended you use the web configurator to create/edit profiles. If you do not specify a base profile, the default base profile is none.

Note: You CANNOT change the base profile later!

**Table 121** Editing/Creating Anomaly Profiles

| COMMAND | DESCRIPTION |
|---|---|
| idp anomaly *newpro* [base {all \| none}] | Creates a new IDP anomaly profile called *newpro*. *newpro* uses the base profile you specify. Enters sub-command mode. All the following commands relate to the new profile. Use exit to quit sub-command mode. |
| scan-detection sensitivity {low \| medium \| high} | Sets scan-detection sensitivity. |
| no scan-detection sensitivity | Clears scan-detection sensitivity. The default sensitivity is medium. |
| scan-detection block-period <1..3600> | Sets for how many seconds the ZyWALL / USG blocks all packets from being sent to the victim (destination) of a detected anomaly attack. |
| [no] scan-detection {tcp-xxx} {activate \| log [alert] \| block} | Activates TCP scan detection options where {tcp-xxx} = {tcp-portscan \| tcp-decoy-portscan \| tcp-portsweep \| tcp-distributed-portscan \| tcp-filtered-portscan \| tcp-filtered-decoy-portscan \| tcp-filtered-distributed-portscan \| tcp-filtered-portsweep}. Also sets TCP scan-detection logs or alerts and blocking. no deactivates TCP scan detection, its logs, alerts or blocking. |
| [no] scan-detection {udp-xxx} {activate \| log [alert] \| block} | Activates or deactivates UDP scan detection options where {udp-xxx} = {udp-portscan \| udp-decoy-portscan \| udp-portsweep \| udp-distributed-portscan \| udp-filtered-portscan \| udp-filtered-decoy-portscan \| udp-filtered-distributed-portscan \| udp-filtered-portsweep}. Also sets UDP scan-detection logs or alerts and blocking. no deactivates UDP scan detection, its logs, alerts or blocking. |
| [no] scan-detection {ip-xxx} {activate \| log [alert] \| block} | Activates or deactivates IP scan detection options where {ip-xxx} = {ip-protocol-scan \| ip-decoy-protocol-scan \| ip-protocol-sweep \| ip-distributed-protocol-scan \| ip-filtered-protocol-scan \| ip-filtered-decoy-protocol-scan \| ip-filtered-distributed-protocol-scan \| ip-filtered-protocol-sweep}. Also sets IP scan-detection logs or alerts and blocking. no deactivates IP scan detection, its logs, alerts or blocking. |
| [no] scan-detection {icmp-sweep \| icmp-filtered-sweep} {activate \| log [alert] \| block} | Activates or deactivates ICMP scan detection options. Also sets ICMP scan-detection logs or alerts and blocking. no deactivates ICMP scan detection, its logs, alerts or blocking. |
| [no] scan-detection open-port {activate \| log [alert] \| block} | Activates or deactivates open port scan detection options. Also sets open port scan-detection logs or alerts and blocking. no deactivates open port scan detection, its logs, alerts or blocking. |
| flood-detection block-period <1..3600> | Sets for how many seconds the ZyWALL / USG blocks all packets from being sent to the victim (destination) of a detected anomaly attack. |
| [no] flood-detection {tcp-flood \| udp-flood \| ip-flood \| icmp-flood} {activate \| log [alert] \| block} | Activates or deactivates TCP, UDP, IP or ICMP flood detection. Also sets flood detection logs or alerts and blocking. no deactivates flood detection, its logs, alerts or blocking. |

**Table 121** Editing/Creating Anomaly Profiles (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] http-inspection {http-xxx} activate | Activates or deactivates http-inspection options where http-xxx = {ascii-encoding \| u-encoding \| bare-byte-unicode-encoding \| base36-encoding \| utf-8-encoding \| iis-unicode-codepoint-encoding \| multi-slash-encoding \| iis-backslash-evasion \| self-directory-traversal \| directory-traversal \| apache-whitespace \| non-rfc-http-delimiter \| non-rfc-defined-char \| oversize-request-uri-directory \| oversize-chunk-encoding \| webroot-directory-traversal} |
| http-inspection {http-xxx} log [alert] | Sets http-inspection log or alert. |
| no http-inspection {http-xxx} log | Deactivates http-inspection logs. |
| [no] http-inspection {http-xxx} action {drop \| reject-sender \| reject-receiver \| reject-both}} | Sets http-inspection action |
| [no] tcp-decoder {tcp-xxx} activate | Activates or deactivates tcp decoder options where {tcp-xxx} = {undersize-len \| undersize-offset \| oversize-offset \| bad-length-options \| truncated-options \| ttcp-detected \| obsolete-options \| experimental-options} |
| tcp-decoder {tcp-xxx} log [alert] | Sets tcp decoder log or alert options. |
| no tcp-decoder {tcp-xxx} log | Deactivates tcp decoder log or alert options. |
| [no] tcp-decoder {tcp-xxx} action {drop \| reject-sender \| reject-receiver \| reject-both}} | Sets tcp decoder action |
| [no] udp-decoder {truncated-header \| undersize-len \| oversize-len} activate | Activates or deactivates udp decoder options |
| udp-decoder {truncated-header \| undersize-len \| oversize-len} log [alert] | Sets udp decoder log or alert options. |
| no udp-decoder {truncated-header \| undersize-len \| oversize-len} log | Deactivates udp decoder log options. |
| udp-decoder {truncated-header \| undersize-len \| oversize-len} action {drop \| reject-sender \| reject-receiver \| reject-both} | Sets udp decoder action |
| no udp-decoder {truncated-header \| undersize-len \| oversize-len} action | Deactivates udp decoder actions. |
| [no] icmp-decoder {truncated-header \| truncated-timestamp-header \| truncated-address-header} activate | Activates or deactivates icmp decoder options |
| icmp-decoder {truncated-header \| truncated-timestamp-header \| truncated-address-header} log [alert] | Sets icmp decoder log or alert options. |
| no icmp-decoder {truncated-header \| truncated-timestamp-header \| truncated-address-header} log | Deactivates icmp decoder log options. |
| icmp-decoder {truncated-header \| truncated-timestamp-header \| truncated-address-header} action {drop \| reject-sender \| reject-receiver \| reject-both}} | Sets icmp decoder action |
| no icmp-decoder {truncated-header \| truncated-timestamp-header \| truncated-address-header} action | Deactivates icmp decoder actions. |
| show idp anomaly *profile* scan-detection [all details] | Shows all scan-detection settings of the specified IDP profile. |

**Table 121** Editing/Creating Anomaly Profiles (continued)

| COMMAND | DESCRIPTION |
|---|---|
| show idp anomaly *profile* scan-detection {tcp-portscan \| tcp-decoy-portscan \| tcp-portsweep \| tcp-distributed-portscan \| tcp-filtered-portscan \| tcp-filtered-decoy-portscan \| tcp-filtered-distributed-portscan \| tcp-filtered-portsweep} details | Shows selected TCP scan-detection settings for the specified IDP profile. |
| show idp anomaly *profile* scan-detection {udp-portscan \| udp-decoy-portscan \| udp-portsweep \| udp-distributed-portscan \| udp-filtered-portscan \| udp-filtered-decoy-portscan \| udp-filtered-distributed-portscan \| udp-filtered-portsweep} details | Shows UDP scan-detection settings for the specified IDP profile. |
| show idp anomaly *profile* scan-detection {ip-protocol-scan \| ip-decoy-protocol-scan \| ip-protocol-sweep \| ip-distributed-protocol-scan \| ip-filtered-protocol-scan \| ip-filtered-decoy-protocol-scan \| ip-filtered-distributed-protocol-scan \| ip-filtered-protocol-sweep} details | Shows IP scan-detection settings for the specified IDP profile. |
| show idp anomaly *profile* scan-detection {icmp-sweep \| icmp-filtered-sweep \| open-port} details | Shows ICMP scan-detection settings for the specified IDP profile. |
| show idp anomaly *profile* flood-detection [all details] | Shows all flood-detection settings for the specified IDP profile. |
| show idp anomaly *profile* flood-detection {tcp-flood \| udp-flood \| ip-flood \| icmp-flood} details | Shows flood-detection settings for the specified IDP profile. |
| show idp anomaly *profile* http-inspection all details | Shows http-inspection settings for the specified IDP profile. |
| show idp anomaly *profile* http-inspection {ascii-encoding \| u-encoding \| bare-byte-unicode-encoding \| base36-encoding \| utf-8-encoding \| iis-unicode-codepoint-encoding \| multi-slash-encoding \| iis-backslash-evasion \| self-directory-traversal \| directory-traversal \| apache-whitespace \| non-rfc-http-delimiter \| non-rfc-defined-char \| oversize-request-uri-directory \| oversize-chunk-encoding \| webroot-directory-traversal} details | Shows http-inspection settings for the specified IDP profile. |
| show idp anomaly *profile* tcp-decoder all details | Shows tcp-decoder settings for the specified IDP profile. |
| show idp anomaly *profile* tcp-decoder {undersize-len \| undersize-offset \| oversize-offset \| bad-length-options \| truncated-options \| ttcp-detected \| obsolete-options \| experimental-options} details | Shows tcp-decoder settings for the specified IDP profile. |
| show idp anomaly *profile* udp-decoder all details | Shows udp-decoder settings for the specified IDP profile. |
| show idp anomaly *profile* udp-decoder {truncated-header \| undersize-len \| oversize-len} details | Shows specified udp-decoder settings for the specified IDP profile. |
| show idp anomaly *profile* icmp-decoder all details | Shows all icmp-decoder settings for the specified IDP profile. |
| show idp anomaly *profile* icmp-decoder {truncated-header \| truncated-timestamp-header \| truncated-address-header} details | Shows specified icmp-decoder settings for the specified IDP profile. |

### 26.3.4.1 Creating an Anomaly Profile Example

In this example we create a profile named “test”, configure some settings, display them, and then return to global command mode.

```
Router# configure terminal
Router(config)# idp anomaly test
Router(config-idp-anomaly-profile-test)# tcp-decoder oversize-offset action drop
Router(config-idp-anomaly-profile-test)# tcp-decoder oversize-offset log alert
Router(config-idp-anomaly-profile-test)# tcp-decoder oversize-offset activate
Router(config-idp-anomaly-profile-test)# no tcp-decoder oversize-offset activate
Router(config-idp-anomaly-profile-test)# exit
Router(config)# show idp anomaly test tcp-decoder oversize-offset details
message: (tcp_decoder) OVERSIZE-OFFSET ATTACK
  keyword: tcp-decoder oversize-offset
  activate: no
  action: drop
  log: log alert
Router(config)#
```

## 26.3.5 Editing System Protect

Use these commands to edit the system protect profiles.

**Table 122** Editing System Protect Profiles

| COMMAND | DESCRIPTION |
|---|---|
| `idp system-protect` | Configure the system protect profile. Enters sub-command mode. All the following commands relate to the new profile. Use `exit` to quit sub-command mode. |
| `[no] signature sid activate` | Activates or deactivates an IDP signature. |
| `signature sid log [alert]` | Sets log or alert options for an IDP signature |
| `no signature sid log` | Deactivates log options for an IDP signature |
| `signature sid action {drop \| reject-sender \| reject-receiver \| reject-both}` | Sets an action for an IDP signature |
| `no signature SID action` | Deactivates an action for an IDP signature. |
| `show idp system-protect all details` | Displays the system protect profile details. |

## 26.3.6 Signature Search

Use this command to search for signatures in the named profile.

Note: It is recommended you use the web configurator to search for signatures.

**Table 123** Signature Search Command

| COMMAND | DESCRIPTION |
|---|---|
| idp search signature *my_profile* name *quoted_string* sid SID severity *severity_mask* platform *platform_mask* policytype *policytype_mask* service *service_mask* activate {any \| yes \| no} log {any \| no \| log \| log-alert} action *action_mask* | Searches for signature(s) in a profile by the parameters specified. The quoted string is any text within the signature name in quotes, for example, [idp search LAN_IDP name "WORM" sid 0 severity 0 platform 0 policytype 0 service 0 activate any log any action] searches for all signatures in the LAN_IDP profile containing the text “worm” within the signature name. |
| idp search system-protect *my_profile* name *quoted_string* sid SID severity *severity_mask* platform *platform_mask* policytype *policytype_mask* service *service_mask* activate {any \| yes \| no} log {any \| no \| log \| log-alert} action *action_mask* | Searches for signature(s) in a system-protect profile by the parameters specified. The quoted string is any text within the signature name in quotes, for example, [idp search LAN_IDP name "WORM" sid 0 severity 0 platform 0 policytype 0 service 0 activate any log any action] searches for all signatures in the LAN_IDP profile containing the text “worm” within the signature name. |
| show idp search signature *my_profile* name *quoted_string* sid SID severity *severity_mask* platform *platform_mask* policytype *policytype_mask* service *service_mask* activate {any \| yes \| no} log {any \| no \| log \| log-alert} action *action_mask* | Searches for signature(s) in a profile by the parameters specified. The quoted string is any text within the signature name in quotes, for example, [idp search LAN_IDP name "WORM" sid 0 severity 0 platform 0 policytype 0 service 0 activate any log any action] searches for all signatures in the LAN_IDP profile containing the text “worm” within the signature name. |
| show idp search system-protect *my_profile* name *quoted_string* sid SID severity *severity_mask* platform *platform_mask* policytype *policytype_mask* service *service_mask* activate {any \| yes \| no} log {any \| no \| log \| log-alert} action *action_mask* | Searches for signature(s) in a system-protect profile by the parameters specified. The quoted string is any text within the signature name in quotes, for example, [idp search LAN_IDP name "WORM" sid 0 severity 0 platform 0 policytype 0 service 0 activate any log any action] searches for all signatures in the LAN_IDP profile containing the text “worm” within the signature name. |

### 26.3.6.1 Search Parameter Tables

The following table displays the command line severity, platform and policy type equivalent values. If you want to combine platforms in a search, then add their respective numbers together. For

example, to search for signatures for Windows NT, Windows XP and Windows 2000 computers, then type “12” as the platform parameter.

**Table 124** Severity, Platform and Policy Type Command Values

| SEVERITY | PLATFORM | POLICY TYPE |
|---|---|---|
| 1 = Very Low | 1 = All | 1 = DoS |
| 2 = Low | 2 = Win95/98 | 2 = Buffer-Overflow |
| 3 = Medium | 4 = WinNT | 3 = Access-Control |
| 4 = High | 8 = WinXP/2000 | 4 = Scan |
| 5 = Severe | 16 = Linux | 5 = Backdoor/Trojan |
| | 32 = FreeBSD | 6 = Others |
| | 64 = Solaris | 7 = P2P |
| | 128 = SGI | 8 = IM |
| | 256 = Other-Unix | 9 = Virtus/Worm |
| | 512 = Network-Device | 10 = Porn |
| | | 11 = Web-Attack |
| | | 12 = Spam |

The following table displays the command line service and action equivalent values. If you want to combine services in a search, then add their respective numbers together. For example, to search for signatures for DNS, Finger and FTP services, then type “7” as the service parameter.

**Table 125** Service and Action Command Values

| SERVICE | SERVICE | ACTION |
|---|---|---|
| 1 = DNS | 65536 = SMTP | 1 = None |
| 2 = FINGER | 131072 = SNMP | 2 = Drop |
| 4 = FTP | 262144 = SQL | 4 = Reject-sender |
| 8 = MYSQL | 524288 = TELNET | 8 = Reject-receiver |
| 16 = ICMP | 1048576 = TFTP | 16 = Reject-both |
| 32 = IM | 2097152 = n/a | |
| 64 = IMAP | 4194304 = WEB_ATTACKS | |
| 128 = MISC | 8388608 = WEB_CGI | |
| 256 = NETBIOS | 16777216 = WEB_FRONTPAGE | |
| 512 = NNTP | 33554432 = WEB_IIS | |
| 1024 = ORACLE | 67108864 = WEB_MISC | |
| 2048 = P2P | 134217728 = WEB_PHP | |
| 4096 = POP2 | 268435456 = MISC_BACKDOOR | |
| 8192 = POP3 | 536870912 = MISC_DDOS | |
| 16384 = RPC | 1073741824 = MISC_EXPLOIT | |
| 32768 = RSERVICES | | |

### 26.3.6.2 Signature Search Example

This example command searches for all signatures in the LAN_IDP profile:

- Containing the text “worm” within the signature name
- With an ID of 12345
- Has a very low severity level
- Operates on the Windows NT platform
- Is a scan policy type, DNS service
- Is enabled
- Generates logs.

```
Router# configure terminal
Router(config)#
Router(config)# idp search signature LAN_IDP name “worm” sid 12345 severity 1
platform 4 policytype 4 service 1 activate yes log log action 2
```

# 26.4 IDP Custom Signatures

Use these commands to create a new signature or edit an existing one.

Note: It is recommended you use the web configurator to create/edit signatures using the web configurator **Anti-X > IDP > Custom Signatures** screen.

Note: You must use the web configurator to import a custom signature file.

**Table 126** Custom Signatures

| COMMAND | DESCRIPTION |
|---|---|
| `idp customize signature` *quoted_string* | Create a new custom signature. The quoted string is the signature command string enclosed in quotes. for example. "alert tcp any any <> any any (msg: \"test\"; sid: 9000000 ; )". |
| `idp customize signature edit` *quoted_string* | Edits an existing custom signature. |
| `no idp customize signature` *custom_sid* | Deletes a custom signature. |
| `show idp signatures custom-signature` *custom_sid* `{details \| contents \| non-contents}` | Displays custom signature information. |
| `show idp signatures custom-signature all details` | Displays all custom signatures’ information. |
| `show idp signatures custom-signature number` | Displays the total number of custom signatures. |

## 26.4.1 Custom Signature Examples

These examples show how to create a custom signature, edit one, display details of one, all and show the total number of custom signatures.

```
Router# configure terminal
Router(config)# idp customize signature "alert tcp any any <> any any  (msg:
\"test\"; sid: 9000000 ;  )"
sid: 9000000
  message: test
  policy type:
  severity:
  platform:
    all: no
    Win95/98: no
    WinNT: no
    WinXP/2000: no
    Linux: no
    FreeBSD: no
    Solaris: no
    SGI: no
    other-Unix: no
    network-device: no
  service:
  outbreak: no
```

This example shows you how to edit a custom signature.

```
Router(config)# idp customize signature edit "alert tcp any any <> any any  (msg :
\"test edit\"; sid: 9000000 ;  )"
sid: 9000000
  message: test edit
  policy type:
  severity:
  platform:
    all: no
    Win95/98: no
    WinNT: no
    WinXP/2000: no
    Linux: no
    FreeBSD: no
    Solaris: no
    SGI: no
    other-Unix: no
    network-device: no
  service:
  outbreak: no
```

This example shows you how to display custom signature details.

```
Router(config)# show idp signatures custom-signature 9000000 details
sid: 9000000
  message: test edit
  policy type:
  severity:
  platform:
    all: no
    Win95/98: no
    WinNT: no
    WinXP/2000: no
    Linux: no
    FreeBSD: no
    Solaris: no
    SGI: no
    other-Unix: no
    network-device: no
  service:
  outbreak: no
```

This example shows you how to display custom signature contents.

```
Router(config)# show idp signatures custom-signature 9000000 contents
sid: 9000000
Router(config)# show idp signatures custom-signature 9000000 non-contents
sid: 9000000
  ack:
  dport: 0
  dsize:
  dsize_rel:
  flow_direction:
  flow_state:
  flow_stream:
  fragbits_reserve:
  fragbits_dontfrag:
  fragbits_morefrag:
  fragoffset:
  fragoffset_rel:
  icmp_id:
  icmp_seq:
  icode:
  icode_rel:
  id:
  ipopt:
  itype:
  itype_rel:
  sameip:
  seq:
  sport: 0
  tcp_flag_ack:
  tcp_flag_fin:
  tcp_flag_push:
  tcp_flag_r1:
  tcp_flag_r2:
  tcp_flag_rst:
  tcp_flag_syn:
  tcp_flag_urg:
  threshold_type:
  threshold_track:
  threshold_count:
  threshold_second:
  tos:
  tos_rel:
  transport: tcp
  ttl:
  ttl_rel:
  window:
  window_rel:
```

This example shows you how to display all details of a custom signature.

```
Router(config)# show idp signatures custom-signature all details
sid: 9000000
  message: test edit
  policy type:
  severity:
  platform:
    all: no
    Win95/98: no
    WinNT: no
    WinXP/2000: no
    Linux: no
    FreeBSD: no
    Solaris: no
    SGI: no
    other-Unix: no
    network-device: no
  service:
  outbreak: no
```

This example shows you how to display the number of custom signatures on the ZyWALL / USG.

```
Router(config)# show idp signatures custom-signature number
signatures:  1
```

# 26.5 Update IDP Signatures

Use these commands to update new signatures. You register for IDP service before you can update IDP signatures, although you do not have to register in order to update system-protect signatures.

Note: You must use the web configurator to import a custom signature file.

**Table 127** Update Signatures

| COMMAND | DESCRIPTION |
|---|---|
| idp {signature \| system-protect} update signatures | Immediately downloads IDP or system protect signatures from an update server. |
| [no] idp {signature \| system-protect} update auto | Enables (disables) automatic signature downloads at regular times and days. |
| idp {signature \| system-protect} update hourly | Enables automatic signature download every hour. |
| idp {signature \| system-protect} update daily <0..23> | Enables automatic signature download every day at the time specified. |
| idp {signature \| system-protect} update weekly {sun \| mon \| tue \| wed \| thu \| fri \| sat} <0..23> | Enables automatic signature download once-a-week at the time and day specified. |
| show idp {signature \| system-protect} update | Displays signature update schedule. |
| show idp {signature \| system-protect} update status | Displays signature update status. |
| show idp {signature \| system-protect} signatures {version \| date \| number} | Displays signature information |

### 26.5.1 Update Signature Examples

These examples show how to enable/disable automatic IDP downloading, schedule updates, display the schedule, display the update status, show the (new) updated signature version number, show the total number of signatures and show the date/time the signatures were created.

```
Router# configure terminal
Router(config)# idp signature update signatures
IDP signature update in progress.
Please check system log for future information.
Router(config)# idp update auto
Router(config)# no idp update auto
Router(config)# idp update hourly
Router(config)# idp update daily 10
Router(config)# idp update weekly fri 13
Router(config)# show idp update
auto: yes
schedule: weekly at Friday 13 o'clock
Router(config)# show idp signature update status
current status: IDP signature download failed, do 1 retry at Sat Jan  4 22:47:47
2003
last update time: 2003-01-01 01:34:39
Router(config)# show idp signature signatures version
version: 1.2000
Router(config)# show idp signature signatures number
signatures: 2000
Router(config)# show idp signature signatures date
date: 2005/11/13 13:56:03
```

## 26.6 IDP Statistics

The following table describes the commands for collecting and displaying IDP statistics. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 128** Commands for IDP Statistics

| COMMAND | DESCRIPTION |
|---|---|
| `[no] idp statistics collect` | Turn the collection of IDP statistics on or off. |
| `idp statistics flush` | Clears the collected statistics. |
| `show idp statistics summary` | Displays the collected statistics. |
| `show idp statistics collect` | Displays whether the collection of IDP statistics is turned on or off. |
| `show idp statistics ranking {signature-name \| source \| destination}` | Query and sort the IDP statistics entries by signature name, source IP address, or destination IP address.<br>`signature-name`: lists the most commonly detected signatures.<br>`source`: lists the source IP addresses from which the ZyWALL / USG has detected the most intrusion attempts.<br>`destination`: lists the most common destination IP addresses for detected intrusion attempts. |

## 26.6.1 IDP Statistics Example

This example shows how to collect and display IDP statistics. It also shows how to sort the display by the most common signature name, source IP address, or destination IP address.

```
Router# configure terminal
Router(config)# idp statistics collect
Router(config)# no idp statistics activate
Router(config)# idp statistics flush
Router(config)# show idp statistics collect status
IDP collect statistics status: yes
Router(config)# show idp statistics summary
scanned session : 268
packet dropped: 0
packet reset: 0
Router(config)# show idp statistics ranking signature-name
ranking: 1
  signature id: 8003796
  signature name: ICMP L3retriever Ping
  type: Scan
  severity: verylow
  occurence: 22
ranking: 2
  signature id: 8003992
  signature name: ICMP Large ICMP Packet
  type: DDOS
  severity: verylow
  occurence: 4
Router(config)# show idp statistics ranking destination
ranking: 1
  destination ip: 172.23.5.19
  occurence: 22
ranking: 2
  destination ip: 172.23.5.1
  occurence: 4
Router(config)# show idp statistics ranking source
ranking: 1
  source ip: 192.168.1.34
  occurence: 26
```

# 27

# Content Filtering

This chapter covers how to use the content filtering feature to control web access.

## 27.1 Content Filtering Overview

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific web sites. It can also block access to specific categories of web site content. You can create different content filtering policies for different addresses, schedules, users or groups and content filtering profiles. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages during the workday and another policy that lets him access them after work.

## 27.2 Content Filtering Policies

A content filtering policy allows you to do the following.

- Use schedule objects to define when to apply a content filtering profile.
- Use address and/or user/group objects to define to whose web access to apply the content filtering profile.
- Apply a content filtering profile that you have custom-tailored.

## 27.3 External Web Filtering Service

When you register for and enable the external web filtering service, your ZyWALL / USG accesses an external database that has millions of web sites categorized based on content. You can have the ZyWALL / USG block, block and/or log access to web sites based on these categories.

## 27.4 Content Filtering Reports

See the web configurator User's Guide to see how to view content filtering reports after you have activated the category-based content filtering subscription service.

# 27.5 Content Filter Command Input Values

The following table explains the values you can input with the `content-filter` commands.

**Table 129** Content Filter Command Input Values

| LABEL | DESCRIPTION |
|---|---|
| *policy_number* | The number of the policy <0 - *X* > where *X* depends on the number of content filtering policies the ZyWALL / USG model supports. See the CLI help for details. |
| *address* | The name (up to 63 characters) of an existing address object or group to which the policy should be applied. |
| *schedule* | The name (up to 63 characters) of an existing schedule to control when the policy should be applied. |
| *filtering_profile* | The filtering profile defines how to filter web URLs or content. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *category_name* | The name of a web category.<br><br>{adult-mature-content\| pornography\| sexeducation\| intimate-apparel-swimsuit\| nudity\| alcohol-tobacco\| illegal-questionable\| gambling\| violence-hate-racism\| weapons\| abortion\| hacking\| phishing\| arts-entertainment\| business-economy\| alternative-spirituality-occult\| illegal-drugs\| education\| cultural-charitable-organization\| financial-services\| brokerage-trading\| online-games\| government-legal\| military\| political-activist-groups\| health\| computers-internet\| search-engines-portals\| spyware-malware-sources\| spyware-effects-privacy-concerns\| job-search-careers\| news-media\| personals-dating\| reference\| open-image-media-search\| chat-instant-messaging\| email\| blogs-newsgroups\| religion\| social-networking\| online-storage\| remote-access-tools\| shopping\| auctions\| real-estate\| society-lifestyle\| sexuality-alternative-lifestyles\| restaurants-dining-food\| sports-recreation-hobbies\| travel\| vehicles\| humor-jokes\| software-downloads\| pay-to-surf\| peer-to-peer\| streaming-media-mp3s\| proxy-avoidance\| for-kids\| web-advertisements\| web-hosting\| extreme\| alcohol\| tobacco\| blogs-personal-pages\| web-applications\| suspicious\| alternative-sexuality-lifestyles\| lgbt\| non-viewable\| content-servers\| placeholders} |
| *trust_hosts* | The IP address or domain name of a trusted web site. Use a host name such as www.good-site.com. Do not use the complete URL of the site – that is, do not include “http://”. All subdomains are allowed. For example, entering “zyxel.com” also allows “www.zyxel.com”, “partner.zyxel.com”, “press.zyxel.com”, etc. Use up to 63 case-insensitive characters (0-9a-z-).<br><br>You can enter a single IP address in dotted decimal notation like 192.168.2.5.<br><br>You can enter a subnet by entering an IP address in dotted decimal notation followed by a slash and the bit number of the subnet mask of an IP address. The range is 0 to 32.<br><br>To find the bit number, convert the subnet mask to binary and add all of the 1’s together. Take “255.255.255.0” for example. 255 converts to eight 1’s in binary. There are three 255’s, so add three eights together and you get the bit number (24).<br><br>An example is 192.168.2.1/24<br><br>You can enter an IP address range by entering the start and end IP addresses separated by a hyphen, for example 192.168.2.5-192.168.2.23. |

**Table 129** Content Filter Command Input Values (continued)

| LABEL | DESCRIPTION |
|---|---|
| *forbid_hosts* | The IP address or domain name of a forbidden web site.<br><br>Use a host name such as www.bad-site.com into this text field. Do not use the complete URL of the site – that is, do not include "http://". All subdomains are also blocked. For example, entering "bad-site.com" also blocks "www.bad-site.com", "partner.bad-site.com", "press.bad-site.com", etc. Use up to 63 case-insensitive characters (0-9a-z-).<br><br>You can enter a single IP address in dotted decimal notation like 192.168.2.5.<br><br>You can enter a subnet by entering an IP address in dotted decimal notation followed by a slash and the bit number of the subnet mask of an IP address. The range is 0 to 32.<br><br>To find the bit number, convert the subnet mask to binary and add all of the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1's in binary. There are three 255's, so add three eights together and you get the bit number (24).<br><br>An example is 192.168.2.1/24<br><br>You can enter an IP address range by entering the start and end IP addresses separated by a hyphen, for example 192.168.2.5-192.168.2.23. |
| *keyword* | A keyword or a numerical IP address to search URLs for and block access to if they contain it. Use up to 63 case-insensitive characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,) in double quotes. For example enter "Bad_Site" to block access to any web page that includes the exact phrase "Bad_Site". This does not block access to web pages that only include part of the phrase (such as "Bad" in this example). |
| *message* | The message to display when a web site is blocked. Use up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,) in quotes. For example, "Access to this web page is not allowed. Please contact the network administrator." |
| *redirect_url* | The URL of the web page to which you want to send users when their web access is blocked by content filtering. The web page you specify here opens in a new frame below the denied access message.<br><br>Use "http://" followed by up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%) in quotes. For example, "http://192.168.1.17/blocked access". |
| *license* | The license key (up to 15 characters) for the external web filtering service. |
| *service_timeout* | The value specifies the maximum querying time in seconds <1…60> |
| *_timeout* | The value specifies the maximum life time in hours <1..720>. |
| *url* | The URL of a web site in http://xxx.xxx.xxx format. |
| *rating_server* | The hostname or IP address of the rating server. |
| *query_timeout* | The value specifies the maximum querying time when testing the connection to an external content filtering server or checking its rating for a URL. <1..60> seconds. |

# 27.6 General Content Filter Commands

The following table lists the commands that you can use for general content filter configuration such as enabling content filtering, viewing and ordering your list of content filtering policies, creating a denial of access message or specifying a redirect URL and checking your external web filtering service registration status. Use the `configure terminal` command to enter the configuration

mode to be able to use these commands. See Table 129 on page 236 for details about the values you can input with these commands.

**Table 130** content-filter General Commands

| COMMAND | DESCRIPTION |
|---|---|
| [no] content-filter active | Turns on content filtering. The no command turns it off. |
| [no] content-filter block message *message* | Sets the message to display when content filtering blocks access to a web page. The no command clears the setting. |
| [no] content-filter block redirect *redirect_url* | Sets the URL of the web page to which to send users when their web access is blocked by content filtering. The no command clears the setting. |
| [no] content-filter -timeout *_timeout* | Sets how long the ZyWALL / USG is to keep an entry in the content filtering URL before discarding it. The no command clears the setting. |
| [no] content-filter default block | Has the ZyWALL / USG block sessions that do not match a content filtering policy. The no command allows sessions that do not match a content filtering policy. |
| [no] content-filter license *license* | Sets the license key for the external web filtering service. The no command clears the setting. |
| content-filter passed warning flush | Clears the ZyWALL / USG's record of sessions for which it has given the user a warning before allowing access. |
| content-filter passed warning timeout <1..1440> | Sets how long to keep records of sessions for which the ZyWALL / USG has given the user a warning before allowing access. |
| [no] content-filter policy *policy_number address schedule filtering_profile* | Sets a content filtering policy. The no command removes it. |
| content-filter policy *policy_number* shutdown | Disables a content filtering policy. |
| content-filter url-server test bluecoat | Enters the sub-command mode for testing whether or not a web site is saved in the BlueCoat external content filter server's database of restricted web pages. |
| *url* [ server *rating_server* ] [ timeout *query_timeout* ] | Tests whether or not a web site is saved in the external content filter server's database of restricted web pages. |
| exit | Leaves the sub-command mode. |
| content-filter url-server test commtouch | Enters the sub-command mode for testing the Commtouch external content filter server's reachability. |
| *url* timeout *query_timeout* | Specify the Commtouch server's URL and how long to wait for a response. |
| exit | Leaves the sub-command mode. |
| content-filter zsb port <1..65535> | Sets the port the ZyWALL / USG uses to check if requested web pages pose a threat to users or their computers. |
| content-filter common-list {trust\|forbid} | Enters the sub-command for configuring a common list of trusted or forbidden web sites.<br><br>The content filtering profile commands let you configure trusted or forbidden URLs for individual profiles. URL checking is applied in the following order: profile trusted web sites, common trusted web sites, profile forbidden web sites, common forbidden web sites, and then profile keywords. |

**Table 130** content-filter General Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] {*ipv4* \| *ipv4_cidr* \| *ipv4_range* \| *wildcard_domainname* \| *tld*} | Adds or removes a common trusted or forbidden web site entry.<br>*ipv4*: IPv4 address <W.X.Y.Z><br>*ipv4_cidr*: IPv4 subnet in CIDR format, i.e. 192.168.1.0/32 <W.X.Y.Z>/<1..32><br>*ipv4_range*: Range of IPv4 addresses. <W.X.Y.Z>-<W.X.Y.Z><br>*wildcard_domainname*: wildcard domain name, i.e. zyxel*.co* (([*a-z0-9\-]){1,63}\.)+([*a-z0-9\-]){1,63}<br>*tld*: top level domain. |
| exit | Leaves the sub-command mode. |
| show content-filter passed warning | Displays the ZyWALL / USG's record of sessions for which it has given the user a warning before allowing access. |
| show content-filter policy | Displays the content filtering policies. |
| show content-filter settings | Displays the general content filtering settings. |
| show content-filter common-list {trust\|forbid} | Displays the common list of trusted or forbidden web sites. |

# 27.7 Content Filter Filtering Profile Commands

The following table lists the commands that you can use to configure a content filtering policy. A content filtering policy defines which content filter profile should be applied, when it should be applied, and to whose web access it should be applied. Use the `configure terminal` command to enter the configuration mode to be able to use these commands. See Table 129 on page 236 for details about the values you can input with these commands.

**Table 131** content-filter Filtering Profile Commands Summary

| COMMAND | DESCRIPTION |
|---|---|
| [no] content-filter license *license* | Sets the license key for the external web filtering service. The no command clears the setting. |
| [no] content-filter profile *filtering_profile* | Creates a content filtering profile. The no command removes the profile. |
| [no] content-filter profile *filtering_profile* custom | Sets a content filtering profile to use a profile's custom settings (lists of trusted web sites and forbidden web sites and blocking of certain web features). The no command has the profile not use the custom settings. |
| [no] content-filter profile *filtering_profile* custom activex | Sets a content filtering profile to block ActiveX controls. The no command sets the profile to allow ActiveX. |
| [no] content-filter profile *filtering_profile* custom cookie | Sets a content filtering profile to block Cookies. The no command sets the profile to allow Cookies. |
| content-filter profile *filtering_profile* custom-list forbid | Enters the sub-command for configuring the content filtering profile's list of forbidden hosts. |
| [no] *forbid_hosts* | Adds a forbidden host to the content filtering profile's list. The no command removes it. |
| exit | Leaves the sub-command mode. |
| [no] content-filter profile *filtering_profile* custom java | Sets a content filtering profile to block Java. The no command sets the profile to allow Java. |

**Table 131** content-filter Filtering Profile Commands Summary (continued)

| COMMAND | DESCRIPTION |
|---|---|
| content-filter profile *filtering_profile* custom-list keyword | Enters the sub-command for configuring the content filtering profile's list of forbidden keywords. This has the content filtering profile block access to Web sites with URLs that contain the specified keyword or IP address in the URL. |
| [no] *keyword* | Adds a forbidden keyword or IP address to the content filtering profile's list. The no command removes it. |
| exit | Leaves the sub-command mode. |
| [no] content-filter profile *filtering_profile* custom proxy | Sets a content filtering profile to block access to web proxy servers. The no command sets the profile to allow access to proxy servers. |
| content-filter profile *filtering_profile* custom-list trust | Enters the sub-command for configuring the content filtering profile's list of trusted hosts. |
| [no] *trust_hosts* | Adds a trusted host to the content filtering profile's list. The no command removes it. |
| exit | Leaves the sub-command mode. |
| [no] content-filter profile *filtering_profile* custom trust-allow-features | Sets a content filtering profile to permit Java, ActiveX and Cookies from sites on the trusted list. The no command has the content filtering profile not permit Java, ActiveX and Cookies from sites on the trusted list |
| [no] content-filter profile *filtering_profile* custom trust-only | Sets a content filtering profile to only allow access to web sites that are on the trusted list. The no command has the profile allow access to web sites that are not on the trusted list. |
| [no] content-filter profile *filtering_profile* url category {category_name} | Sets a content filtering profile to check for specific web site categories. The no command has the profile not check for the specified categories. |
| content-filter profile *filtering_profile* url match-unsafe {block \| log \| pass} | Sets the action for attempted access to web pages that match the profile's selected unsafe categories.<br>Block access, log access, or allow access. |
| content-filter profile *filtering_profile* url match {block \| log \| warn \| pass} | Sets the action for attempted access to web pages that match the profile's selected managed categories.<br>Block access, allow and log access, display a warning message before allowing access, or allow access. |
| content-filter profile *filtering_profile* url offline {block \| log \| warn \| pass} | Sets the action for attempted access to web pages if the external content filtering database is unavailable.<br>Block access, allow and log access, display a warning message before allowing access, or allow access. |
| content-filter profile *filtering_profile* url unrate {block \| log \| warn \| pass} | Sets the action for attempted access to web pages that the external web filtering service has not categorized.<br>Block access, allow and log access, display a warning message before allowing access, or allow access. |
| no content-filter profile *filtering_profile* url match-unsafe {log} | Has the ZyWALL / USG not log attempted access to web pages that match the profile's selected unsafe categories. |
| no content-filter profile *filtering_profile* url match {log} | Has the ZyWALL / USG not log attempted access to web pages that match the profile's selected managed categories. |
| no content-filter profile *filtering_profile* url offline {log} | Has the ZyWALL / USG not log access to web pages if the external content filtering database is unavailable. |

**Table 131** content-filter Filtering Profile Commands Summary (continued)

| COMMAND | DESCRIPTION |
|---|---|
| `no content-filter profile filtering_profile url unrate {log}` | Has the ZyWALL / USG not log access to web pages that the external web filtering service has not categorized. |
| `[no] content-filter profile filtering_profile url url-server` | Sets a content filtering profile to use the external web filtering service. The `no` command has the profile not use the external web filtering service. |
| `[no] content-filter service-timeout service_timeout` | Sets how many seconds the ZyWALL / USG is to wait for a response from the external content filtering server. The `no` command clears the setting. |
| `[no] content-filter profile filtering_profile commtouch-url category {category_name}` | Sets a CommTouch content filtering profile to check for specific web site categories. The `no` command has the profile not check for the specified categories. |
| `content-filter profile filtering_profile commtouch-url match-unsafe {block \| log \| pass}` | Sets the action for attempted access to web pages that match the CommTouch profile's selected unsafe categories.<br>Block access, log access, or allow access. |
| `content-filter profile filtering_profile commtouch-url match {block \| log \| warn \| pass}` | Sets the action for attempted access to web pages that match the CommTouch profile's selected managed categories.<br>Block access, allow and log access, display a warning message before allowing access, or allow access. |
| `content-filter profile filtering_profile commtouch-url offline {block \| log \| warn \| pass}` | Sets the action for attempted access to web pages if the CommTouch external content filtering database is unavailable.<br>Block access, allow and log access, display a warning message before allowing access, or allow access. |
| `content-filter profile filtering_profile commtouch-url unrate {block \| log \| warn \| pass}` | Sets the action for attempted access to web pages that the CommTouch external web filtering service has not categorized.<br>Block access, allow and log access, display a warning message before allowing access, or allow access. |
| `no content-filter profile filtering_profile commtouch-url match-unsafe {log}` | Has the ZyWALL / USG not log attempted access to web pages that match the CommTouch profile's selected unsafe categories. |
| `no content-filter profile filtering_profile commtouch-url match {log}` | Has the ZyWALL / USG not log attempted access to web pages that match the CommTouch profile's selected managed categories. |
| `no content-filter profile filtering_profile commtouch-url offline {log}` | Has the ZyWALL / USG not log access to web pages if the CommTouch external content filtering database is unavailable. |
| `no content-filter profile filtering_profile commtouch-url unrate {log}` | Has the ZyWALL / USG not log access to web pages that the CommTouch external web filtering service has not categorized. |
| `show content-filter profile [filtering_profile]` | Displays the specified content filtering profile's settings or the settings of all them if you don't specify one. |

# 27.8 Content Filter URL Cache Commands

The following table lists the commands that you can use to view and configure your ZyWALL / USG's URL caching. You can configure how long a categorized web site address remains in the  as well as

view those web site addresses to which access has been allowed or blocked based on the responses from the external content filtering server. The ZyWALL / USG only queries the external content filtering database for sites not found in the cache.

Use the `configure terminal` command to enter the configuration mode to be able to use these commands. See Table 129 on page 236 for details about the values you can input with these commands.

**Table 132** content-filter url-cache Commands

| COMMAND | DESCRIPTION |
|---|---|
| `[no] content-filter -timeout _timeout` | Sets how long to keep a content filtering URL cache entry before discarding it. The `no` command clears the setting. |
| `show content-filter url-cache [all-category] [begin url_cache_range end url_cache_range] [_count]` | Displays the contents of the content filtering URL cache. You can specify a range and number of entries to display. |
| `show content-filter url-cache` | Displays the contents of the content filtering URL cache. |
| `content-filter url-cache test` | Enters the sub-command mode for testing whether or not a web site is saved in the ZyWALL / USG's database of restricted web pages. |
| `url` | Tests whether or not a web site is saved in the ZyWALL / USG's database of restricted web pages. |
| `exit` | Leaves the sub-command mode. |

# 27.9 Content Filtering Statistics

The following table describes the commands for collecting and displaying content filtering statistics. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 133** Commands for Content Filtering Statistics

| COMMAND | DESCRIPTION |
|---|---|
| `[no] content-filter statistics collect` | Turn the collection of content filtering statistics on or off. |
| `content-filter statistics flush` | Clears the collected statistics. |
| `show content-filter statistics summary` | Displays the collected statistics. |
| `show content-filter statistics collect` | Displays whether the collection of content filtering statistics is turned on or off. |
| `show content-filter statistics summary` | Displays the current content filtering statistics. |

### 27.9.1 Content Filtering Statistics Example

This example shows how to collect and display content filtering statistics.

```
Router(config)# content-filter statistics collect
Router(config)# show content-filter statistics summary
total web pages inspected               : 0
  web pages warned by category service  : 0
  web pages blocked by category service: 0
  web pages blocked by custom service   : 0
    restricted web features             : 0
    forbidden web sites                 : 0
    url keywords                        : 0
  web pages blocked without policy      : 0
  web pages passed                      : 0

  unsafe web pages                      : 0
  other web pages                       : 0
```

## 27.10 Content Filtering Commands Example

The following example shows how to limit the web access for a sales group.

1. First, create a sales address object. This example uses a subnet that covers IP addresses 172.21.3.1 to 172.21.3.254.
2. Then create a schedule for all day.
3. Create a filtering profile for the group.
4. You can use the following commands to block sales from accessing adult and pornography websites.
5. Enable the external web filtering service.

   Note: You must register for the external web filtering service before you can use it (see Chapter 5 on page 47).
6. You can also customize the filtering profile. The following commands block active-X, java and proxy access.
7. Append a content filter policy.

**8** Activate the customization.

```
Router# configure terminal
Router(config)# address-object sales 172.21.3.0/24
Router(config)# schedule-object all_day 00:00 23:59
Router(config)# content-filter profile sales_CF_PROFILE
Router(config)# content-filter profile sales_CF_PROFILE url category adult-mature-content
Router(config)# content-filter profile sales_CF_PROFILE url category pornography
Router(config)# content-filter profile sales_CF_PROFILE url url-server
Router(config)# content-filter profile sales_CF_PROFILE custom java
Router(config)# content-filter profile sales_CF_PROFILE custom activex
Router(config)# content-filter profile sales_CF_PROFILE custom proxy
Router(config)# content-filter profile sales_CF_PROFILE custom
Router(config)# content-filter policy append all_day any RD RD_CF_PROFILE
Router(config)# content-filter activate
```

Use this command to display the settings of the profile.

```
Router(config)# show content-filter profile sales_CF_PROFILE commtouch
service active : yes
url match unsafe: block:  no, warn: yes, log:  no
url match other : block: yes, warn:  no, log:  no
url unrate      : block:  no, warn: yes, log:  no
service offline : block:  no, warn: yes, log:  no

category settings:
Adult/Mature Content            : yes, Pornography                      : yes
Sex Education                   :  no, Intimate Apparel/Swimsuit        :  no
Nudity                          :  no, Alcohol/Tobacco                  :  no
Illegal/Questionable            :  no, Gambling                         :  no
Violence/Hate/Racism            :  no, Weapons                          :  no
Abortion                        :  no, Hacking                          :  no
Phishing                        :  no, Arts/Entertainment               :  no
Business/Economy                :  no, Alternative Spirituality/Occult :  no
Illegal Drugs                   :  no, Education                        :  no
Cultural/Charitable Organization:  no, Financial Services               :  no
Brokerage/Trading               :  no, Online Games                     :  no
Government/Legal                :  no, Military                         :  no
Political/Activist Groups       :  no, Health                           :  no
Computers/Internet              :  no, Search Engines/Portals           :  no
Spyware/Malware Sources         :  no, Spyware Effects/Privacy Concerns:  no
Job Search/Careers              :  no, News/Media                       :  no
Personals/Dating                :  no, Reference                        :  no
Open Image/Media Search         :  no, Chat/Instant Messaging           :  no
Email                           :  no, Blogs/Newsgroups                 :  no
Religion                        :  no, Social Networking                :  no
Online Storage                  :  no, Remote Access Tools              :  no
Shopping                        :  no, Auctions                         :  no
Real Estate                     :  no, Society/Lifestyle                :  no
Sexuality/Alternative Lifestyles:  no, Restaurants/Dining/Food          :  no
Sports/Recreation/Hobbies       :  no, Travel                           :  no
Vehicles                        :  no, Humor/Jokes                      :  no
Software Downloads              :  no, Pay to Surf                      :  no
Peer-to-Peer                    :  no, Streaming Media/MP3s             :  no
Proxy Avoidance                 :  no, For Kids                         :  no
Web Advertisements              :  no, Web Hosting                      :  no
Extreme                         :  no, Alcohol                          :  no
Tobacco                         :  no, Blogs/Personal Pages             :  no
Web Applications                :  no, Suspicious                       :  no
Alternative Sexuality/Lifestyles:  no, LGBT                             :  no
Non-viewable                    :  no, Content Servers                  :  no
Placeholders                    :  no, Open/Mixed Content               :  no
Potentially Unwanted Software   :  no, Greeting Cards                   :  no
Audio/Video Clips               :  no, Media Sharing                    :  no
Radio/Audio Streams             :  no, TV/Video Streams                 :  no
Internet Telephony              :  no, Online Meetings                  :  no
Newsgroups/Forums               :  no, Art/Culture                      :  no
Entertainment                   :  no, Games                            :  no
Sports/Recreation               :  no, Translation                      :  no
Alternative Spirituality/Belief :  no, Society/Daily Living             :  no
-------------------------------------SNIP!-----------------------------------------
```

# 28

# Anti-Spam

This chapter introduces and shows you how to configure the anti-spam scanner.

## 28.1 Anti-Spam Overview

The anti-spam feature marks or discards spam. Activate the anti-spam subscription service for sender IP reputation checking, mail content analysis, and virus outbreak detection. Use the white list to identify legitimate e-mail. Use the black list to identify spam e-mail. You can also check e-mail against a DNS black list (DNSBL) of IP addresses of servers suspected of being used by spammers.

## 28.2 Anti-Spam Commands

The following table identifies the values used in some of these commands. Other input values are discussed with the corresponding commands.

**Table 134** Input Values for General Anti-Spam Commands

| LABEL | DESCRIPTION |
|---|---|
| *rule_number* | The index number of an anti-spam rule. 1 - *X* where *X* is the highest number of anti-spam rules the ZyWALL / USG model supports. See the ZyWALL / USG's User's Guide for details. |
| *zone_object* | The name of the zone. ~~The~~Some ZyWALL / USG ~~USG 200 and lower~~ models use pre-defined zone names like DMZ, LAN1, SSL VPN, WLAN, IPSec VPN, OPT, and WAN. |
| *xheader-name* | The name (part that comes before the colon) of a field to add to an e-mail header. Use up to 16 ASCII characters. |
| *xheader-value* | The value (part that comes after the colon) of a field to add to an e-mail header. Use up to 16 ASCII characters. |

### 28.2.1 General Anti-Spam Commands

The following table describes general anti-spam commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 135** General Anti-Spam Commands

| COMMAND | DESCRIPTION |
|---|---|
| `[no] anti-spam activate` | Enables or disables anti-spam service. |
| `show anti-spam activation` | Displays anti-spam service status. |

#### 28.2.1.1 Activate/Deactivate Anti-Spam Example

This example shows how to activate and deactivate anti-spam on the ZyWALL / USG.

```
Router# configure terminal
Router(config)# anti-spam activate
Router(config)# show anti-spam activation
anti-spam activation: yes
Router(config)# no anti-spam activate
Router(config)# show anti-spam activation
anti-spam activation: no
Router(config)#
```

### 28.2.2 Zone to Zone Anti-spam Rules

The following table describes the commands for configuring the zone to zone rules. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 136** Commands for Zone to Zone Anti-Spam Rules

| COMMAND | DESCRIPTION |
|---|---|
| `anti-spam rule append` | Enters the anti-spam sub-command mode to add a direction specific rule. |
| `anti-spam rule insert` *`rule_number`* | Enters the anti-spam sub-command mode to add a direction specific rule. |
| `anti-spam rule` *`rule_number`* | Enters the anti-spam sub-command mode to edit the specified direction specific rule. |
| `[no] activate` | Turns a direction specific anti-spam rule on or off. |
| `[no] log [alert]` | Sets the ZyWALL / USG to create a log (and optionally an alert) when packets match this rule and are found to be spam. The `no` command sets the ZyWALL / USG not to create a log or alert when packets match this rule. |
| `[no] from-zone` *`zone_object`* | Sets the zone on which the packets are received. The `no` command removes the zone setting. This is equal to any, so the rule applies to all packets the ZyWALL / USG sends out. |
| `[no] to-zone` *`zone_object`* | Sets the zone to which the packets are sent. The `no` command removes the zone setting. This is equal to any, so the rule applies to all packets the ZyWALL / USG sends out. |
| `[no] scan {smtp \| pop3}` | Sets the protocols of traffic to scan for spam. |
| `[no] match-action pop3 {forward \| forward-with-tag}` | Sets the action to take when the ZyWALL / USG detects a spam POP3 e-mail. The file can be forwarded or forwarded with a spam tag. |
| `[no] match-action smtp {drop \| forward \| forward-with-tag}` | Sets the action to take when the ZyWALL / USG detects a spam SMTP e-mail. The file can be deleted, forwarded, or forwarded with a spam tag. |
| `[no] bypass {white-list \| black-list \| dnsbl}` | Bypassing has the ZyWALL / USG not check files against your configured white (allowed) list, black (spam) list, or DNSBL servers list. |
| `[no] bypass {ip-reputation \| mail-content \| virus-outbreak}` | Have the ZyWALL / USG not check mail's IP reputation, content, or for viruses. |
| `show` | Displays the details of the anti-spam rule you are configuring. |
| `anti-spam rule move` *`rule_number`* `to` *`rule_number`* | Moves a direction specific anti-spam rule to the number that you specified. |
| `anti-spam rule delete` *`rule_number`* | Removes a direction specific anti-spam rule. |
| `show anti-spam rule [`*`rule_number`*`]` | Displays the details of all the configured anti-spam rules or a specific anti-spam rule. |

**Table 136** Commands for Zone to Zone Anti-Spam Rules (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] anti-spam {smtp \| pop3} defaultport *port_number* | Specify a custom SMTP or POP3 TCP port to check. |
| show anti-spam {smtp \| pop3} defaultport | Display the SMTP or POP3 TCP ports the ZyWALL / USG checks for spam. |
| [no] anti-spam ip-reputation activate | Set whether or not to use IP reputation to identify spam by the sender's IP address. |
| anti-spam ip-reputation query-timeout time [*timeout*] | Set how many seconds the ZyWALL / USG waits for a reply when checking the IP reputation of a sender's IP address. |
| show anti-spam ip-reputation query-timeout time | Display how many seconds the ZyWALL / USG waits for a reply when checking the IP reputation of a sender's IP address. |
| [no] anti-spam ip-reputation private-check activate | Set whether or not to check the IP reputation of private sender IP addresses. |
| show anti-spam ip-reputation private-check | Display the setting for checking the IP reputation of private sender IP addresses. |
| [no] anti-spam mail-content activate | Set whether or not to identify spam by content, such as malicious content. |
| [no] anti-spam virus-outbreak activate | Set whether or not to scan emails for attached viruses. |
| anti-spam tag {mail-content \| virus-outbreak} [*tag*] | Specify the labels to add to the beginning of the mail subject if content-analysis identified it as spam or it contains a virus. |
| [no] anti-spam xheader {mail-content \| virus-outbreak} *xheader-name xheader-value* | Specify the name and value for the X-Header to add to content-analysis identified spam or e-mails containing a virus. |
| show anti-spam tag {mail-content \| virus-outbreak} | Display the labels for content-analysis identified spam or e-mails containing a virus. |
| show anti-spam xheader {mail-content \| virus-outbreak} | Display the name and value for the X-Header to add to content-analysis identified spam or e-mails containing a virus. |
| anti-spam mail-scan query-timeout pop3 {forward \| forward-with-tag} | Select how to handle POP3 mail if querying the mail scan server times out. Use forward to send it or forward-with-tag to add a tag to the mail subject and send it. |
| anti-spam mail-scan query-timeout smtp {drop \| forward \| forward-with-tag} | Select how to handle SMTP mail if querying the mail scan server times out. Use drop to discard the SMTP mail, forward to send it, or forward-with-tag to add a tag to the mail subject and send it. |
| anti-spam mail-scan query-timeout time [*timeout*] | Set how many seconds the ZyWALL / USG waits for a reply from the mail scan server before taking the relevant timeout action. |
| anti-spam tag query-timeout [*tag*] | Specify the label to add to the mail subject of e-mails the ZyWALL / USG tags and forwards when queries to the mail scan servers time out. |
| [no] anti-spam xheader query-timeout *xheader-name xheader-value* | Specify the name and value for the X-Header to add to e-mails the ZyWALL / USG forwards when queries to the mail scan servers time out. |
| show anti-spam mail-scan query-timeout smtp | Display the action the ZyWALL / USG takes on SMTP mail if querying the mail scan server times out. |
| show anti-spam mail-scan query-timeout pop3 | Display the action the ZyWALL / USG takes on POP3 mail if querying the mail scan server times out. |
| show anti-spam mail-scan query-timeout time | Display how many seconds the ZyWALL / USG waits for a reply from the mail scan server before taking the relevant timeout action. |
| show anti-spam mail-scan status | Displays the ZyWALL / USG's settings for IP reputation, mail content, and virus outbreak checking. |
| show anti-spam tag query-timeout | Display the label the ZyWALL / USG adds to the mail subject of e-mails that it tags and forwards when queries to the mail scan servers time out. |
| show anti-spam xheader query-timeout | Display the name and value for the X-Header the ZyWALL / USG adds to e-mails that it tags and forwards when queries to the mail scan servers time out. |

#### 28.2.2.1 Zone to Zone Anti-spam Rule Example

This example shows how to configure (and display) a WAN to DMZ anti-spam rule to scan POP3 and SMTP traffic. SMTP spam is forwarded. POP3 spam is marked with a spam tag. The ZyWALL / USG logs the event when an e-mail matches the DNSBL (see Section 28.2.4 on page 252 for more on DNSBL). The white and black lists are ignored.

```
Router(config)# anti-spam rule 1
Router(config-as-rule-1)# activate
Router(config-as-rule-1)# from-zone WAN
Router(config-as-rule-1)# to-zone DMZ
Router(config-as-rule-1)# scan smtp
Router(config-as-rule-1)# scan pop3
Router(config-as-rule-1)# match-action smtp forward
Router(config-as-rule-1)# match-action pop3 forward-with-tag
Router(config-as-rule-1)# log
Router(config-as-rule-1)# bypass white-list
Router(config-as-rule-1)# bypass black-list
Router(config-as-rule-1)# exit
Router(config)# show anti-spam rule 1
Anti-Spam Rule: 1
  active: yes
  log: log
  from zone: WAN
  to zone: DMZ
  scan protocols:
    smtp: yes
    pop3: yes
  match action:
    smtp: forward
    pop3: forward-with-tag
  bypass white list: yes
  bypass black list: yes
  bypass ip reputation: no
  bypass mail content: no
  bypass virus outbreak: no
  bypass dnsbl: no
```

### 28.2.3 White and Black Lists

The following table identifies values used in these commands. Other input values are discussed with the corresponding commands.

**Table 137** Input Values for White and Black list Anti-Spam Commands

| LABEL | DESCRIPTION |
|---|---|
| *mail_header* | The name part of an e-mail header (the part that comes before the colon). Use up to 63 ASCII characters.<br><br>For example, if you want the entry to check the “Received:” header for a specific mail server’s domain, use “Received”. |
| *mail_header_value* | The value part of an e-mail header (the part that comes after the colon). Use up to 63 ASCII characters.<br><br>For example, if you want the entry to check the “Received:” header for a specific mail server’s domain, specify the mail server’s domain.<br><br>See Section 28.2.3.2 on page 252 for more details. |

**Table 137** Input Values for White and Black list Anti-Spam Commands (continued)

| LABEL | DESCRIPTION |
|---|---|
| *rule_number* | The index number of an anti-spam white or black list entry. 1 - *X* where *X* is the highest number of entries the ZyWALL / USG model supports. See the ZyWALL / USG's User's Guide for details. |
| *subject* | A keyword in the content of the e-mail Subject headers. Use up to 63 ASCII characters. Spaces are not allowed, although you could substitute a question mark (?). See Section 28.2.3.2 on page 252 for more details. |

Use the white list to identify legitimate e-mail and the black list to identify spam e-mail. The following table describes the commands for configuring the white list and black list. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 138** Commands for Anti-spam White and Black Lists

| COMMAND | DESCRIPTION |
|---|---|
| `[no] anti-spam white-list activate` | Turns the white list checking on or off. Turn on the white list to forward e-mail that matches (an active) white list entry without doing any more anti-spam checking on that individual e-mail. |
| `[no] anti-spam white-list [rule_number] ip-address ip subnet_mask {activate\|deactivate}` | Adds, edits, or removes a white list entry to check e-mail for a specific source or relay IP address. Also turns the entry on or off. |
| `[no] anti-spam white-list [rule_number] e-mail email {activate\|deactivate}` | Adds, edits, or removes a white list entry to check e-mail for a specific source e-mail address or domain name. Also turns the entry on or off. |
| `[no] anti-spam white-list [rule_number] mail-header mail-header mail-header-value {activate\|deactivate}` | Adds, edits, or removes a white list entry to check e-mail for specific header fields and values. Also turns the entry on or off. |
| `[no] anti-spam white-list [rule_number] subject subject {activate\|deactivate}` | Adds, edits, or removes a white list entry to check e-mail for specific content in the subject line. Also turns the entry on or off. |
| `[no] anti-spam black-list activate` | Turns the black list checking on or off. Turn on the black list to treat e-mail that matches (an active) black list entry as spam. |
| `[no] anti-spam black-list [rule_number] ip-address ip subnet_mask {activate\|deactivate}` | Adds, edits, or removes a black list entry to check e-mail for a specific source or relay IP address. Also turns the entry on or off. |
| `[no] anti-spam black-list [rule_number] e-mail email {activate\|deactivate}` | Adds, edits, or removes a black list entry to check e-mail for a specific source e-mail address or domain name. Also turns the entry on or off. |
| `[no] anti-spam black-list [rule_number] mail-header mail-header mail-header-value {activate\|deactivate}` | Adds, edits, or removes a black list entry to check e-mail for specific header fields and values. Also turns the entry on or off. |
| `[no] anti-spam black-list [rule_number] subject subject {activate\|deactivate}` | Adds, edits, or removes a black list entry to check e-mail for specific content in the subject line. Also turns the entry on or off. |
| `anti-spam tag black-list [tag]` | Configures a message or label (up to 15 ASCII characters) to add to the mail subject of e-mails that match an anti-spam black list entry. |
| `show anti-spam white-list [status]` | Displays the current anti-spam white list. Use `status` to show the activation status only. |
| `show anti-spam black-list [status]` | Displays the current anti-spam black list. Use `status` to show the activation status only. |
| `show anti-spam tag black-list` | Show the configured anti-spam black list tag. |
| `[no] anti-spam xheader {white-list \| black-list} mail-header mail-header-value` | Specify the name and value for the X-Header to add to e-mails that match the ZyWALL / USG's spam white list or black list. |
| `show anti-spam xheader {white-list \| black-list}` | Display the name and value for the X-Header to add to e-mails that match the ZyWALL / USG's spam white list or black list. |

#### 28.2.3.1 White and Black Lists Example

This example shows how to configure and enable a white list entries for e-mails with “testwhite” in the subject, e-mails from whitelist@ourcompany.com, e-mails with the Date header set to 2007, and e-mails from (or forwarded by) IP address 192.168.1.0 with subnet 255.255.255.0.

```
Router(config)# anti-spam white-list subject testwhite activate
Router(config)# anti-spam white-list e-mail whitelist@ourcompany.com activate
Router(config)# anti-spam white-list mail-header Date 2007 activate
Router(config)# anti-spam white-list ip-address 192.168.1.0 255.255.255.0 activate
Router(config)# show anti-spam white-list
No.   Type        Status
Content
================================================================================
1     subject     yes
testwhite
2     e-mail      yes
whitelist@ourcompany.com
3     mail-header yes
Date : 2007
4     ip-address  yes
192.168.1.0 / 255.255.255.0
```

#### 28.2.3.2 Regular Expressions in Black or White List Entries

The following applies for a black or white list entry based on an e-mail subject, e-mail address, or e-mail header value.

- Use a question mark (?) to let a single character vary. For example, use “a?c” (without the quotation marks) to specify abc, acc and so on.
- You can also use a wildcard (*). For example, if you configure *def.com, any e-mail address that ends in def.com matches. So “mail.def.com” matches.
- The wildcard can be anywhere in the text string and you can use more than one wildcard. You cannot use two wildcards side by side, there must be other characters between them.
- The ZyWALL / USG checks the first header with the name you specified in the entry. So if the e-mail has more than one “Received” header, the ZyWALL / USG checks the first one.

### 28.2.4 DNSBL Anti-Spam Commands

This section describes the commands for checking the sender and relay IP addresses in e-mail headers against DNS (Domain Name Service)-based spam Black Lists (DNSBLs). You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 139** Input Values for DNSBL Commands

| LABEL | DESCRIPTION |
|---|---|
| *dnsbl_domain* | A domain that is maintaining a DNSBL. You may use 0-254 alphanumeric characters, or dashes (-). |

This table describes the DNSBL commands.

**Table 140** DNSBL Commands

| COMMAND | DESCRIPTION |
|---|---|
| [no] anti-spam dnsbl activate | Turns DNSBL checking on or off. |
| anti-spam dnsbl [1..5] domain *dnsbl_domain* {activate\|deactivate} | Adds or edits a DNSBL domain for checking e-mail header IP addresses. |
| no anti-spam dnsbl domain *dnsbl_domain* | Removes the specified DNSBL domain. |
| anti-spam dnsbl query-timeout smtp {drop \| forward \| forward-with-tag} | Sets how the ZyWALL / USG handles SMTP mail (mail going to an e-mail server) if the queries to the DNSBL domains time out. |
| anti-spam dnsbl query-timeout pop3 {forward \| forward-with-tag} | Sets how the ZyWALL / USG handles POP3 mail (mail coming to an e-mail client) if the queries to the DNSBL domains time out. |
| anti-spam dnsbl max-query-ip [1..5] | Sets up to how many sender and relay server IP addresses in the mail header to check against the DNSBL. |
| anti-spam dnsbl ip-check-order {forward \| backward} | Configures the order in which anti-spam checks e-mail header IP addresses against the DNSBLs.<br>• forward checks the first N IP addresses. Checking starts from the first IP address in the mail header. This is the IP of the sender or the first server that forwarded the mail.<br>• backward checks the last N IP addresses. Checking starts from the last IP address in the mail header. This is the IP of the last server that forwarded the mail. |
| anti-spam tag {dnsbl \| dnsbl-timeout} [*tag*] | dnsbl configures the message or label to add to the beginning of the mail subject of e-mails that have a sender or relay IP address in the header that matches a blacklist maintained by a DNSBL domain listed in the ZyWALL / USG.<br>dnsbl-timeout configures the message or label to add to the mail subject of e-mails that the ZyWALL / USG forwards if queries to the DNSBL domains time out.<br>Use up to 15 alphanumeric characters, underscores (_), colons (:), or dashes (-). |
| show anti-spam dnsbl status | Displays the activation status of the anti-spam DNSBL checking. |
| show anti-spam dnsbl domain | Displays the ZyWALL / USG's configured anti-spam DNSBL domain entries. |
| show anti-spam dnsbl max-query-ip | Displays how many sender and relay server IP addresses in the mail header anti-spam checks against the DNSBL. |
| show anti-spam dnsbl ip-check-order | Displays the order in which anti-spam checks e-mail header IP addresses against the DNSBLs. |
| show anti-spam dnsbl query-timeout {smtp \| pop3} | Displays how the ZyWALL / USG handles SMTP or POP3 mail if the queries to the DNSBL domains time out. |
| show anti-spam tag {dnsbl \| dnsbl-timeout} | dnsbl displays the anti-spam tag for e-mails that have a sender or relay IP address in the header that matches a blacklist maintained by a DNSBL domain.<br>dnsbl-timeout displays the message or label to add to the mail subject of e-mails that the ZyWALL / USG forwards if queries to the DNSBL domains time out. |
| show anti-spam dnsbl statistics | Displays anti-spam DNSBL statistics for each configured DNSBL domain. |
| anti-spam dnsbl statistics flush | Clears the anti-spam DNSBL statistics for each configured DNSBL domain. |
| anti-spam dnsbl query-timeout time [1..10] | Sets how long the ZyWALL / USG waits for a reply from the DNSBL domains. |
| show anti-spam dnsbl query-timeout time | Displays how long the ZyWALL / USG waits for a reply from the DNSBL domains. |

**Table 140** DNSBL Commands

| COMMAND | DESCRIPTION |
|---|---|
| `[no] anti-spam xheader dnsbl` *`mail-header mail-header-value`* | Specify the name and value for the X-Header to add to e-mails with a sender or relay IP address in the header that matches a black list maintained by a DNSBL domain in the ZyWALL / USG's list |
| `show anti-spam xheader dnsbl` | Display the name and value for the X-Header to add to e-mails with a sender or relay IP address in the header that matches a black list maintained by a DNSBL domain in the ZyWALL / USG's list |

### 28.2.4.1 DNSBL Example

This example:

- Sets the ZyWALL / USG to use "DNSBL-example.com" as a DNSBL.
- Turns DNSBL checking on.
- Sets the ZyWALL / USG to forward POP3 mail with a tag if the queries to the DNSBL domains time out.
- Sets the ZyWALL / USG to check up to 4 sender and relay server IP addresses in e-mail headers against the DNSBL.
- Sets the ZyWALL / USG to start DNSBL checking from the first IP address in the mail header.
- Sets the DNSBL tag to "DNSBL".
- Sets the DNSBL timeout tag to "DNSBL-timeout".

- Displays the DNSBL statistics.

```
Router(config)# anti-spam dnsbl domain DNSBL-example.com activate
Router(config)# show anti-spam dnsbl domain
No.   Status
Domain
================================================================================
1     yes
DNSBL-example.com
Router(config)# anti-spam dnsbl activate
Router(config)# show anti-spam  dnsbl status
anti-spam dnsbl status: yes
Router(config)# anti-spam dnsbl query-timeout pop3 forward-with-tag
Router(config)# show anti-spam  dnsbl query-timeout pop3
dnsbl query timeout action: forward-with-tag
Router(config)# anti-spam dnsbl max-query-ip 4
Router(config)# show anti-spam  dnsbl max-query-ip
dnsbl max query ip: 4
Router(config)# anti-spam dnsbl ip-check-order forward
Router(config)# show anti-spam  dnsbl ip-check-order
anti-spam dnsbl IP check order: forward
Router(config)# anti-spam tag dnsbl DNSBL
Router(config)# show anti-spam tag dnsbl
dnsbl tag: DNSBL
Router(config)# anti-spam tag dnsbl-timeout DNSBL-timeout
Router(config)# show anti-spam tag dnsbl-timeout
dnsbl-timeout tag: DNSBL-timeout
Router(config)# show anti-spam dnsbl statistics
DNSBL domain: 1
  domain: DNSBL-example.com
  average time: 0.00
  total query: 0
    spam: 0
    clear: 0
    no timeout: 0
    timeout: 0
    no response: 0
```

# 28.3 Anti-Spam Statistics

The following table describes the commands for collecting and displaying anti-spam statistics. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 141** Commands for Anti-spam Statistics

| COMMAND | DESCRIPTION |
|---|---|
| `[no] anti-spam statistics collect` | Turn the collection of anti-spam statistics on or off. |
| `anti-spam statistics flush` | Clears the collected statistics. |
| `show anti-spam statistics summary` | Displays an overview of the collected statistics. |
| `show anti-spam statistics collect` | Displays whether the collection of anti-spam statistics is turned on or off. |
| `show anti-spam statistics ranking {source \| mail-address}` | Query and sort the anti-spam statistics entries by source IP address or mail address.<br>`source`: lists the source IP addresses of the most spam.<br>`mail-address`: lists the most common source mail address for spam. |

**Table 141** Commands for Anti-spam Statistics (continued)

| COMMAND | DESCRIPTION |
|---|---|
| show anti-spam ip-reputation statistics | Displays the mail sender IP reputation checking statistics. |
| show anti-spam mail-scan statistics | Displays the mail scan statistics. |

## 28.3.1 Anti-Spam Statistics Example

This example shows how to collect anti-spam statistics and display a summary.

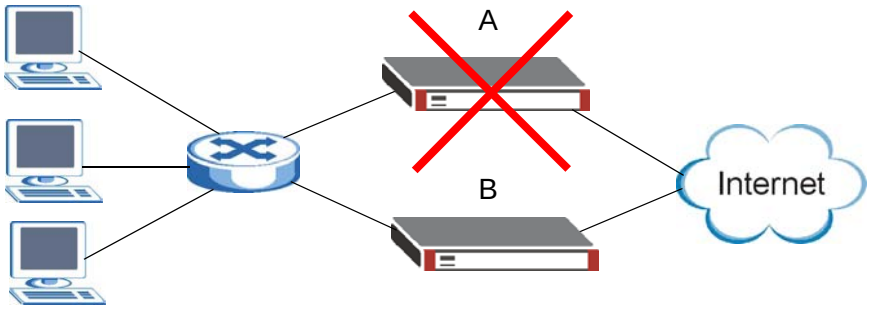
```
Router(config)# anti-spam statistics  collect
Router(config)# show anti-spam statistics collect
collect statistics: yes
collect statistics time: since 2008-03-11 07:16:01 to 2008-03-11 07:16:13
Router(config)# show anti-spam statistics summary
total mails scanned: 0
total clear mails: 0
clear mail by whitelist: 0
total spam mails: 0
spam detected by blacklist: 0
spam detected by ip reputation: 0
spam detected by mail content: 0
spam detected by dnsbl: 0
spam detected with virus: 0
total virus mails: 0
dnsbl timeout: 0
mail session forwarded: 0
mail session dropped: 0
```

# 29

# Device HA

Use device HA to increase network reliability. Device HA lets a backup ZyWALL / USG (**B**) automatically take over if a master ZyWALL / USG (**A**) fails.

**Figure 25** Device HA Backup Taking Over for the Master




## 29.1 Device HA Overview

### Active-Passive Mode and Legacy Mode

- Active-passive mode lets a backup ZyWALL / USG take over if the master ZyWALL / USG fails.
- Legacy mode uses VRRP (Virtual Router Redundancy Protocol) groups and allows for more complex relationships between the master and backup ZyWALL / USGs, such as active-active or using different ZyWALL / USGs as the master ZyWALL / USG for individual interfaces. Legacy mode configuration involves a greater degree of complexity. Active-passive mode is recommended for general failover deployments.
- The ZyWALL / USGs must all support and be set to use the same device HA mode (either active-passive or legacy).

### Management Access

You can configure a separate management IP address for each interface. You can use it to access the ZyWALL / USG for management whether the ZyWALL / USG is the master or a backup. The management IP address should be in the same subnet as the interface IP address.

### Synchronization

Use synchronization to have a backup ZyWALL / USG copy the master ZyWALL / USG's configuration, signatures (anti-virus, IDP/application patrol, and system protect), and certificates.

Note: Only ZyWALL / USGs of the same model and firmware version can synchronize.

Otherwise you must manually configure the master ZyWALL / USG's settings on the backup (by editing copies of the configuration files in a text editor for example).

### 29.1.1 Before You Begin

- Configure a static IP address for each interface that you will have device HA monitor.

Note: Subscribe to services on the backup ZyWALL / USG before synchronizing it with the master ZyWALL / USG.

- Synchronization includes updates for services to which the master and backup ZyWALL / USGs are both subscribed. For example, a backup subscribed to IDP/AppPatrol, but not anti-virus, gets IDP/AppPatrol updates from the master, but not anti-virus updates. It is highly recommended to subscribe the master and backup ZyWALL / USGs to the same services.

## 29.2 General Device HA Commands

This table lists the general commands for device HA.

**Table 142** device-ha General Commands

| COMMAND | DESCRIPTION |
|---|---|
| `show device-ha status` | Displays whether or not device HA is activated, the configured device HA mode, and the status of the monitored interfaces. |
| `[no] device-ha activate` | Turns device HA on or off. |
| `device-ha mode {active-passive \| legacy}` | Sets the ZyWALL / USG to use active-passive or legacy (VRRP group based) device HA. |

## 29.3 Active-Passive Mode Device HA

### Virtual Router

The master and backup ZyWALL / USG form a single 'virtual router'.

### Cluster ID

You can have multiple ZyWALL / USG virtual routers on your network. Use a different cluster ID to identify each virtual router.

### Monitored Interfaces in Active-Passive Mode Device HA

You can select which interfaces device HA monitors. If a monitored interface on the ZyWALL / USG loses its connection, device HA has the backup ZyWALL / USG take over.

Enable monitoring for the same interfaces on the master and backup ZyWALL / USGs. Each monitored interface must have a static IP address and be connected to the same subnet as the corresponding interface on the backup or master ZyWALL / USG.

### Virtual Router and Management IP Addresses

- If a backup takes over for the master, it uses the master's IP addresses. These IP addresses are know as the virtual router IP addresses.
- Each interface can also have a management IP address. You can connect to this IP address to manage the ZyWALL / USG regardless of whether it is the master or the backup.

# 29.4 Active-Passive Mode Device HA Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 143** Input Values for device-ha Commands

| LABEL | DESCRIPTION |
|---|---|
| *interface_name* | The name of the interface. This depends on the ZyWALL / USG model.<br><br>For ~~the~~some ZyWALL / USG ~~USG 300 and above~~models, use ge*x*, *x* = 1 ~ N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model.<br><br>For ~~the~~other ~~ZyWALL~~ZyWALL / USG ~~USG 200 and below~~models, use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.<br><br>Besides, in HA AP mode, the interface can also be a bridge interface.<br><br>In HA Legacy mode, the interface can also be a VLAN interface. |

The following sections list the `device-ha` commands.

## 29.4.1 Active-Passive Mode Device HA Commands

This table lists the commands for configuring active-passive mode device HA.

**Table 144** device-ha ap-mode Commands

| COMMAND | DESCRIPTION |
|---|---|
| `[no] device-ha ap-mode preempt` | Turn on preempt if this ZyWALL / USG should become the master ZyWALL / USG if a lower-priority ZyWALL / USG is the master when this ZyWALL / USG is enabled. |
| `device-ha ap-mode role {master\|backup}` | Sets the ZyWALL / USG to be the master or a backup in the virtual router. |
| `device-ha ap-mode cluster-id <1..32>` | Sets the cluster ID number. A virtual router consists of a master ZyWALL / USG and all of its backup ZyWALL / USGs. If you have multiple ZyWALL / USG virtual routers on your network, use a different cluster ID for each virtual router. |
| `device-ha ap-mode priority <1..254>` | Sets backup ZyWALL / USG's priority. The backup ZyWALL / USG with the highest value takes over the role of the master ZyWALL / USG if the master ZyWALL / USG becomes unavailable. The priority must be between 1 and 254. (The master interface has priority 255.) |

**Table 144** device-ha ap-mode Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] device-ha ap-mode authentication {string *key* \| ah-md5 *key*} | Sets the authentication method the virtual router uses. Every interface in a virtual router must use the same authentication method and password. The no command disables authentication.<br>string: Use a plain text password for authentication. *key* - Use up to eight characters including alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ () ).<br>ah-md5: Use an encrypted MD5 password for authentication. *key* - Use up to eight characters including alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ () ). |
| [no] device-ha ap-mode *interface_name* manage-ip *ip subnet_mask* | Sets the management IP address for an interface. |
| [no] device-ha ap-mode *interface_name* activate | Has device HA monitor the status of an interface’s connection. |
| [no] device-ha ap-mode master sync authentication password *password* | This is for a master ZyWALL / USG. It specifies the password to require from synchronizing backup ZyWALL / USGs. Every router in the virtual router must use the same password. The no command sets the password setting to blank (which means no backups can synchronize with this master).<br>*password*: Use 4-63 alphanumeric characters, underscores (_), dashes (-), and #%^*={}:,.~ characters. |
| [no] device-ha ap-mode backup sync authentication password *password* | Sets the password the backup ZyWALL / USG uses when synchronizing with the master. The no command sets the password setting to blank (which means this backup ZyWALL / USG cannot synchronize with the master).<br>*password*: Use 4-63 alphanumeric characters, underscores (_), dashes (-), and #%^*={}:,.~ characters. |
| [no] device-ha ap-mode backup sync auto | Turns on automatic synchronization according to the interval you specify in device-ha ap-mode backup sync interval. The first synchronization begins after the specified interval (not immediately). |
| [no] device-ha ap-mode backup sync interval <1..1440> | When you use automatic synchronization, this sets how often (in minutes) the ZyWALL / USG synchronizes with the master. |
| [no] device-ha ap-mode backup sync from *master_address* port *port* | Sets the address of the master ZyWALL / USG with which this backup ZyWALL / USG is to synchronize.<br>*master_address*: The master ZyWALL / USG’s IP address or fully-qualified domain name (FQDN).<br>*port*: The master ZyWALL / USG’s FTP port number. |
| device-ha ap-mode backup sync now | Synchronize now. |
| show device-ha ap-mode interfaces | Displays the device HA AP mode interface settings and status. |
| show device-ha ap-mode next-sync-time | Displays the next time and date (in hh:mm yyyy-mm-dd format) the ZyWALL / USG will synchronize with the master. |
| show device-ha ap-mode status | Displays the ZyWALL / USG’s key device HA settings. |
| show device-ha ap-mode master sync | Displays the master ZyWALL / USG’s synchronization settings. |
| show device-ha ap-mode backup sync | Displays the backup ZyWALL / USG’s synchronization settings. |
| show device-ha ap-mode backup sync status | Displays the backup ZyWALL / USG’s current synchronization status. |

**Table 144** device-ha ap-mode Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| `show device-ha ap-mode backup sync summary` | Displays the backup ZyWALL / USG's synchronization settings. |
| `show device-ha ap-mode forwarding-port` *`interface_name`* | If you apply Device HA on a bridge interface on a backup ZyWALL / USG, you can use this command to see which port in the bridge interface is chosen to receive VRRP packets used to monitor if the master ZyWALL / USG goes down.<br>*`interface_name`*: This is a bridge interface, For example, brx. |

### 29.4.2 Active-Passive Mode Device HA Command Example

This example configures a ZyWALL / USG to be a master ZyWALL / USG for active-passive mode device HA. There is a management IP address of 192.168.1.3 on lan1. wan1 and lan1 are monitored. The synchronization password is set to "mySyncPassword".

```
Router(config)# device-ha ap-mode lan1 manage-ip 192.168.1.3 255.255.255.0
Router(config)# device-ha ap-mode role master
Router(config)# device-ha ap-mode master sync authentication password mySyncPassword
Router(config)# device-ha ap-mode wan1 activate
Router(config)# device-ha ap-mode lan1 activate
Router(config)# device-ha activate
```

## 29.5 Legacy Mode (VRRP) Device HA

This section covers device HA using VRRP, VRRP groups, and synchronization.

### Virtual Router Redundancy Protocol (VRRP) Overview

Every computer on a network may send packets to a default gateway, which can become a single point of failure. Virtual Router Redundancy Protocol (VRRP), allows you to create redundant backup gateways to ensure that the default gateway is always available. The ZyWALL / USG uses a custom VRRP implementation and is not compatible with standard VRRP.

### VRRP Group Overview

In the ZyWALL / USG, you should create a VRRP group to add one of its interfaces to a virtual router. You can add any Ethernet interface, VLAN interface, or virtual interface (created on top of Ethernet interfaces or VLAN interfaces) with a static IP address. You can only enable one VRRP group for each interface, and you can only have one active VRRP group for each virtual router.

# 29.6 Legacy Mode (VRRP) Device HA Commands

The following table identifies the values required for many `device-ha` commands. Other input values are discussed with the corresponding commands.

**Table 145** Input Values for device-ha Commands

| LABEL | DESCRIPTION |
|---|---|
| *vrrp_group_name* | The name of the VRRP group. The name can consist of alphanumeric characters, the underscore, and the dash and may be up to fifteen alphanumeric characters long. |

The following sections list the `device-ha` commands.

## 29.6.1 VRRP Group Commands

This table lists the commands for VRRP groups.

**Table 146** device-ha Commands: VRRP Groups

| COMMAND | DESCRIPTION |
|---|---|
| `show device-ha vrrp-group` | Displays information about all VRRP groups. |
| `[no] device-ha vrrp-group` *vrrp_group_name* | Creates the specified VRRP group if necessary and enters sub-command mode. The `no` command deletes the specified VRRP group. |
| `[no] vrid <1..254>` | Sets the specified VRRP group's ID to the specified VR ID. The `no` command clears the VR ID. |
| `[no] interface` *interface_name* | Specifies the interface that is part of the specified VRRP group. The `no` command removes the specified interface from the specified VRRP group. |
| `[no] role {master \| backup}` | Specifies the role of the specified VRRP group in the virtual router. The `no` command clears the role, which makes the configuration incomplete. |
| `[no] priority <1..254>` | Sets the priority of the specified VRRP group in the virtual router. The `no` command resets the priority to 100. |
| `[no] preempt` | Lets the ZyWALL / USG preempt lower-priority routers in the virtual router. The `no` command prevents the ZyWALL / USG from preempting lower-priority routers. |
| `[no] manage-ip IP` | Specifies the IP address of the specified VRRP group when it is not the master. The `no` command clears the IP address. |
| `[no] authentication {string` *password* `\| ah-md5` *password*`}` | Specifies the authentication method and password for the specified VRRP group. The `no` command means that the specified VRRP group does not use authentication.<br>*password*: You may use alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ () ), and it can be up to eight characters long. |
| `[no] description` *description* | Specifies the description for the specified VRRP group. The `no` command clears the description.<br>*description*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long. |
| `[no] activate` | Turns on the specified VRRP group. The `no` command turns off the VRRP group. |

## 29.6.2 VRRP Synchronization Commands

This table lists the commands for synchronization. You can synchronize with other ZyWALL's of the same model that are running the same firmware version.

**Table 147** device-ha Commands: Synchronization

| COMMAND | DESCRIPTION |
|---|---|
| show device-ha sync | Displays the current settings for synchronization. |
| show device-ha sync backup next-sync-time | Displays the next time and date (in hh:mm yyyy-mm-dd format) the ZyWALL / USG will synchronize with the master. |
| show device-ha sync status | Displays the current status of synchronization. |
| [no] device-ha sync from {*hostname* \| *ip*} | Specifies the fully-qualified domain name (FQDN) or IP address of the ZyWALL / USG router. Usually, this is the IP address or FQDN of the virtual router. The no command clears this field.<br>*hostname*: You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period. |
| [no] device-ha sync port <1..65535> | Specifies the port number to use to synchronize with the specified ZyWALL / USG router. The no command resets the port to 21. |
| [no] device-ha sync authentication password *password* | Specifies the password to use when synchronizing. Every router in the virtual router should use the same password. The no command resets the password to "1234".<br>*password*: You can use 4-63 alphanumeric characters, underscores (_), dashes (-), and #%^*={}:,.~ characters. |
| [no] device-ha sync auto | Specifies whether or not to automatically synchronize at regular intervals. |
| [no] device-ha sync interval <5..1440> | Specifies the number of minutes between each synchronization if the ZyWALL / USG automatically synchronizes with the specified ZyWALL / USG router. The no command resets the interval to five minutes. |
| [no] device-ha sync now | Synchronize now. |

## 29.6.3 Link Monitoring Commands

This table lists the commands for link monitoring. Link monitoring has the master ZyWALL / USG shut down all of its VRRP interfaces if one of its VRRP interface links goes down. This way the backup ZyWALL / USG takes over all of the master ZyWALL / USG's functions.

**Table 148** device-ha Commands: Synchronization

| COMMAND | DESCRIPTION |
|---|---|
| device-ha link-monitoring activate | Turns on device HA link monitoring. |
| no device-ha link-monitoring | Turns off device HA link monitoring. |
| show device-ha link-monitoring | Displays the current link monitoring setting. |
| device-ha stop-stub-interface activate | Has the master ZyWALL / USG shut down any 3G or wireless LAN interfaces if one of its VRRP interface links goes down. |
| no device-ha stop-stub-interface | Has the master ZyWALL / USG not shut down any 3G or wireless LAN interfaces if one of its VRRP interface links goes down. |
| show device-ha stop-stub-interface | Displays whether or not the ZyWALL / USG is set to have the master ZyWALL / USG shut down any 3G or wireless LAN interfaces if one of its VRRP interface links goes down. |

# 30

# User/Group

This chapter describes how to set up user accounts, user groups, and user settings for the ZyWALL / USG. You can also set up rules that control when users have to log in to the ZyWALL / USG before the ZyWALL / USG routes traffic for them.

## 30.1 User Account Overview

A user account defines the privileges of a user logged into the ZyWALL / USG. User accounts are used in firewall rules and application patrol, in addition to controlling access to configuration and services in the ZyWALL / USG.

### 30.1.1 User Types

There are the types of user accounts the ZyWALL / USG uses.

**Table 149** Types of User Accounts

| TYPE | ABILITIES | LOGIN METHOD(S) |
|---|---|---|
| **Admin Users** | | |
| Admin | Change ZyWALL / USG configuration (web, CLI) | WWW, TELNET, SSH, FTP |
| Limited-Admin | Look at ZyWALL / USG configuration (web, CLI)<br>Perform basic diagnostics (CLI) | WWW, TELNET, SSH |
| **Access Users** | | |
| User | Access network services<br>Browse user-mode commands (CLI) | WWW, TELNET, SSH |
| Guest | Access network services | WWW |
| Ext-User | External user account | WWW |
| ext-group-user | External group user account | WWW |

Note: The default **admin** account is always authenticated locally, regardless of the authentication method setting. (See Chapter 35 on page 291 for more information about authentication methods.)

# 30.2 User/Group Commands Summary

The following table identifies the values required for many `username/groupname` commands. Other input values are discussed with the corresponding commands.

**Table 150** username/groupname Command Input Values

| LABEL | DESCRIPTION |
|---|---|
| *username* | The name of the user (account). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *groupname* | The name of the user group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. It cannot be the same as the user name. |

The following sections list the `username/groupname` commands.

## 30.2.1 User Commands

The first table lists the commands for users.

**Table 151** username/groupname Commands Summary: Users

| COMMAND | DESCRIPTION |
|---|---|
| `show username [`*username*`]` | Displays information about the specified user or about all users set up in the ZyWALL / USG. |
| `username` *username* `nopassword user-type {admin \| guest \| limited-admin \| user}` | Creates the specified user (if necessary), disables the password, and sets the user type for the specified user. |
| `username` *username* `password` *password* `user-type {admin \| guest \| limited-admin \| user}` | Creates the specified user (if necessary); enables and sets the password; and sets the user type for the specified user.<br>*password*: You can use 1-63 printable ASCII characters, except double quotation marks (“) and question marks (?). |
| `username` *username* `user-type ext-user` | Creates the specified user (if necessary) and sets the user type to **Ext-User**. |
| `username` *username* `user-type ext-group-user associated-aaa-server` *server_profile* `group-id` *id* | Specify the value of the AD or LDAP server’s Group Membership Attribute that identifies the group to which the specified ext-group-user type user account belongs. |
| `no username` *username* | Deletes the specified user. |
| `username rename` *username username* | Renames the specified user (first *username*) to the specified username (second *username*). |
| `username` *username* `[no] description` *description* | Sets the description for the specified user. The `no` command clears the description.<br>*description*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long. |
| `username` *username* `[no] logon-time-setting <default \| manual>` | Sets the account to use the factory default lease and reauthentication times or custom ones. |

**Table 151** username/groupname Commands Summary: Users (continued)

| COMMAND | DESCRIPTION |
|---|---|
| username *username* [no] logon-lease-time <0..1440> | Sets the lease time for the specified user. Set it to zero to set unlimited lease time. The no command sets the lease time to five minutes (regardless of the current default setting for new users). |
| username *username* [no] logon-re-auth-time <0..1440> | Sets the reauthorization time for the specified user. Set it to zero to set unlimited reauthorization time. The no command sets the reauthorization time to thirty minutes (regardless of the current default setting for new users). |

## 30.2.2 User Group Commands

This table lists the commands for groups.

**Table 152** username/groupname Commands Summary: Groups

| COMMAND | DESCRIPTION |
|---|---|
| show groupname [*groupname*] | Displays information about the specified user group or about all user groups set up in the ZyWALL / USG. |
| [no] groupname *groupname* | Creates the specified user group if necessary and enters sub-command mode. The no command deletes the specified user group. |
| [no] description *description* | Sets the description for the specified user group. The no command clears the description for the specified user group. |
| [no] groupname *groupname* | Adds the specified user group (second *groupname*) to the specified user group (first *groupname*). |
| [no] user *username* | Adds the specified user to the specified user group. |
| show | Displays information about the specified user group. |
| groupname rename *groupname groupname* | Renames the specified user group (first *groupname*) to the specified group-name (second *groupname*). |

## 30.2.3 User Setting Commands

This table lists the commands for user settings, except for forcing user authentication.

**Table 153** username/groupname Commands Summary: Settings

| COMMAND | DESCRIPTION |
|---|---|
| show users default-setting {all \| user-type {admin\|user\|guest\|limited-admin\|ext-user\| ext-group-user}} | Displays the default lease and reauthentication times for the specified type of user accounts. |
| users default-setting [no] logon-lease-time <0..1440> | Sets the default lease time (in minutes) for each new user. Set it to zero to set unlimited lease time. The no command sets the default lease time to five. |
| users default-setting [no] logon-re-auth-time <0..1440> | Sets the default reauthorization time (in minutes) for each new user. Set it to zero to set unlimited reauthorization time. The no command sets the default reauthorization time to thirty. |
| users default-setting [no] user-type <admin \|ext-user\|guest\|limited-admin\|user\|ext-group-user> | Sets the default user type for each new user. The no command sets the default user type to user. |
| users default-setting [no] user-type <admin \|ext-user\|guest\|limited-admin\|user\|ext-group-user> logon-lease-time <0..1440> | Sets the default lease time (in minutes) for each type of new user. Set it to zero for unlimited lease time. The no command sets the default lease time to five. |

**Table 153** username/groupname Commands Summary: Settings (continued)

| COMMAND | DESCRIPTION |
|---|---|
| users default-setting [no] user-type <admin \|ext-user\|guest\|limited-admin\|user\|ext-group-user> logon-re-auth-time <0..1440> | Sets the default reauthorization time (in minutes) for each type of new user. Set it to zero for unlimited reauthorization time. The no command sets the default reauthorization time to thirty. |
| show users retry-settings | Displays the current retry limit settings for users. |
| [no] users retry-limit | Enables the retry limit for users. The no command disables the retry limit. |
| [no] users retry-count <1..99> | Sets the number of failed login attempts a user can have before the account or IP address is locked out for lockout-period minutes. The no command sets the retry-count to five. |
| [no] users lockout-period <1..65535> | Sets the amount of time, in minutes, a user or IP address is locked out after retry-count number of failed login attempts. The no command sets the lockout period to thirty minutes. |
| show users simultaneous-logon-settings | Displays the current settings for simultaneous logins by users. |
| [no] users simultaneous-logon {administration \| access} enforce | Enables the limit on the number of simultaneous logins by users of the specified account-type. The no command disables the limit, or allows an unlimited number of simultaneous logins. |
| [no] users simultaneous-logon {administration \| access} limit <1..1024> | Sets the limit for the number of simultaneous logins by users of the specified account-type. The no command sets the limit to one. |
| show users update-lease-settings | Displays whether or not access users can automatically renew their lease time. |
| [no] users update-lease automation | Lets users automatically renew their lease time. The no command prevents them from automatically renewing it. |
| show users idle-detection-settings | Displays whether or not users are automatically logged out, and, if so, how many minutes of idle time must pass before they are logged out. |
| [no] users idle-detection | Enables logging users out after a specified number of minutes of idle time. The no command disables logging them out. |
| [no] users idle-detection timeout <1..60> | Sets the number of minutes of idle time before users are automatically logged out. The no command sets the idle-detection timeout to three minutes. |

### 30.2.3.1 User Setting Command Examples

The following commands show the current settings for the number of simultaneous logins.

```
Router# configure terminal
Router(config)# show users simultaneous-logon-settings
enable simultaneous logon limitation for administration account: yes
maximum simultaneous logon per administration account          : 1
enable simultaneous logon limitation for access account        : yes
maximum simultaneous logon per access account                  : 3
```

## 30.2.4 Force User Authentication Commands

This table lists the commands for forcing user authentication.

**Table 154** username/groupname Commands Summary: Forcing User Authentication

| COMMAND | DESCRIPTION |
|---|---|
| `[no] force-auth activate` | Enables force user authentication that force users to log in to the ZyWALL / USG before the ZyWALL / USG routes traffic for them. The no command means the user authentication is not required. |
| `force-auth default-rule authentication {required \| unnecessary} {no log \| log [alert]}` | Sets the default authentication policy that the ZyWALL / USG uses on traffic that does not match any exceptional service or other authentication policy.<br>`required`: Users need to be authenticated. They must manually go to the ZyWALL / USG's login screen. The ZyWALL / USG will not redirect them to the login screen.<br>`unnecessary`: Users do not need to be authenticated.<br>`no log \| log [alert]`: Select whether to have the ZyWALL / USG generate a log (`log`), log and alert (`log alert`) or not (`no log`) for packets that match this default policy. |
| `force-auth [no] exceptional-service` *`service_name`* | Sets a service which you want users to be able to access without user authentication. The `no` command removes the specified service from the exceptional list. |
| `force-auth policy <1..1024>` | Creates the specified condition for forcing user authentication, if necessary, and enters sub-command mode. The conditions are checked in sequence, starting at 1. See Table 155 on page 270 for the sub-commands. |
| `force-auth policy append` | Creates a new condition for forcing user authentication at the end of the current list and enters sub-command mode. See Table 155 on page 270 for the sub-commands. |
| `force-auth policy insert <1..1024>` | Creates a new condition for forcing user authentication at the specified location, renumbers the other conditions accordingly, and enters sub-command mode. See Table 155 on page 270 for the sub-commands. |
| `force-auth policy delete <1..1024>` | Deletes the specified condition.<br>To modify a condition, you can insert a new condition (N) and then delete the one (N+1) that you want to modify. |
| `force-auth policy flush` | Deletes every condition. |
| `force-auth policy move <1..1024> to <1..1024>` | Moves the specified condition to the specified location and renumbers the other conditions accordingly. |
| `show force-auth activation` | Displays whether forcing user authentication is enabled or not. |
| `show force-auth exceptional-service` | Displays services that users can access without user authentication. |
| `show force-auth policy {<1..1024> \| all}` | Displays details about the policies for forcing user authentication. |

### 30.2.4.1 force-auth Sub-commands

The following table describes the sub-commands for several force-auth policy commands. Note that not all rule commands use all the sub-commands listed here.

**Table 155** force-auth policy Sub-commands

| COMMAND | DESCRIPTION |
|---|---|
| [no] activate | Activates the specified condition. The no command deactivates the specified condition. |
| [no] authentication {force \| required} | Select the authentication requirement for users when their traffic matches this policy. The no command means user authentication is not required.<br>force: Users need to be authenticated and the ZyWALL / USG automatically display the login screen when users who have not logged in yet try to send HTTP traffic.<br>required: Users need to be authenticated. They must manually go to the login screen. The ZyWALL / USG will not redirect them to the login screen. |
| [no] description *description* | Sets the description for the specified condition. The no command clears the description.<br>*description*: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long. |
| [no] destination {*address_object* \| *group_name*} | Sets the destination criteria for the specified condition. The no command removes the destination criteria, making the condition effective for all destinations. |
| [no] eps <1..8> *eps_object_name* | Associates the specified End Point Security (EPS) object with the specified condition. The ZyWALL / USG checks authenticated users' computers against the condition's endpoint security objects in the order of 1 to 8. You have to configure order 1 and then the others if any. The no command removes the specified EPS object's association with the condition.<br>To apply EPS for this condition, you have to also make sure you enable EPS and set authentication to either required or force for this condition. |
| [no] eps activate | Enables EPS for the specified condition. The no command means to disable EPS for the condition. |
| eps insert <1..8> *eps_object_name* | Inserts the specified EPS object for the condition. The number determines the order that this EPS rule is executed in the condition. |
| eps move <1..8> to <1..8> | Changes an endpoint object's position in the execution order of the condition. |
| [no] eps periodical-check <1..1440> | Sets a number of minutes the ZyWALL / USG has to repeat the endpoint security check. The no command means that the ZyWALL / USG only perform the endpoint security check when users log in to the ZyWALL / USG. |
| [no] force | Forces users to log in to the ZyWALL / USG if the specified condition is satisfied. The no command means that users do not log in to the ZyWALL / USG. |
| [no] schedule *schedule_name* | Sets the time criteria for the specified condition. The no command removes the time criteria, making the condition effective all the time. |
| [no] source {*address_object* \| *group_name*} | Sets the source criteria for the specified condition. The no command removes the source criteria, making the condition effective for all sources. |
| show | Displays information about the specified condition. |

### 30.2.4.2 Force Authentication Policy Insert Command Example

The following commands show how to insert a force authentication policy at position 1 of the checking order. This policy applies endpoint security policies and uses the following settings:

- Activate: yes
- Description: EPS-on-LAN
- Source: use address object “LAN1_SUBNET”
- Destination: use address object “DMZ_Servers”
- User Authentication: required
- Schedule: no specified
- Endpoint security: Activate
- endpoint security object: use “EPS-WinXP” and “EPS-WinVista” for the first and second checking EPS objects

```
Router# configure terminal
Router(config)# force-auth policy insert 1
Router(config-force-auth-1)# activate
Router(config-force-auth-1)# description EPS-on-LAN
Router(config-force-auth-1)# source LAN1_SUBNET
Router(config-force-auth-1)# destination DMZ_Servers
Router(config-force-auth-1)# authentication force
Router(config-force-auth-1)# no schedule
Router(config-force-auth-1)# eps activate
Router(config-force-auth-1)# eps 1 EPS-WinXP
Router(config-force-auth-1)# eps 2 EPS-WinVista
Router(config-force-auth-1)# exit
```

## 30.2.5 Additional User Commands

This table lists additional commands for users.

**Table 156** username/groupname Commands Summary: Additional

| COMMAND | DESCRIPTION |
|---|---|
| `show users {`*`username`*` \| all \| current}` | Displays information about the users logged onto the system. |
| `show lockout-users` | Displays users who are currently locked out. |
| `unlock lockout-users {`*`ip`*` \| console\|` *`ipv6_addr`*`}` | Unlocks the specified IP address. |
| `users force-logout` *`username`* `\|` *`ip`* `\|` *`ipv6_addr`* | Logs out the specified login. |

### 30.2.5.1 Additional User Command Examples

The following commands display the users that are currently logged in to the ZyWALL / USG and forces the logout of all logins from a specific IP address.

```
Router# configure terminal
Router(config)# show users all
No: 0
  Name: admin
  Type: admin
  From: console
  Service: console
  Session_Time: 25:46:00
  Idle_Time: unlimited
  Lease_Timeout: unlimited
  Re_Auth_Timeout: unlimited
  User_Info: admin
No: 1
  Name: admin
  Type: admin
  From: 192.168.1.34
  Service: http/https
  Session_Time: 00:02:26
  Idle_Time: unlimited
  Lease_Timeout: unlimited
  Re_Auth_Timeout: unlimited
  User_Info: admin
Router(config)# users force-logout 192.168.1.34
Logout user 'admin'(from 192.168.1.34 ): OK
Total 1 user has been forced logout
Router(config)# show users all
No: 0
  Name: admin
  Type: admin
  From: console
  Service: console
  Session_Time: 25:48:33
  Idle_Time: unlimited
  Lease_Timeout: unlimited
  Re_Auth_Timeout: unlimited
  User_Info: admin
```

The following commands display the users that are currently locked out and then unlocks the user who is displayed.

```
Router# configure terminal
Router(config)# show lockout-users
No.  Username Tried                  From            Lockout Time Remaining
================================================================================
No.  From            Failed Login Attempt    Record Expired Timer
================================================================================1
172.16.1.5             2                       46

Router(config)# unlock lockout-users 172.16.1.5
User from 172.16.1.5 is unlocked
Router(config)# show lockout-users
No.  Username Tried                  From            Lockout Time Remaining
================================================================================
No.  From            Failed Login Attempt    Record Expired Timer
================================================================================
```

# 31

# Addresses

This chapter describes how to set up addresses and address groups for the ZyWALL / USG.

## 31.1 Address Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

You can create IP address objects based on an interface's IP address, subnet, or gateway. The ZyWALL / USG automatically updates these objects whenever the interface's IP address settings change. This way every rule or setting that uses the object uses the updated IP address settings. For example, if you change the LAN1 interface's IP address, the ZyWALL / USG automatically updates the corresponding interface-based, LAN1 subnet address object. So any configuration that uses the LAN1 subnet address object is also updated.

Address objects and address groups are used in dynamic routes, firewall rules, application patrol, content filtering, and VPN connection policies. For example, addresses are used to specify where content restrictions apply in content filtering. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

## 31.2 Address Commands Summary

The following table describes the values required for many address object and address group commands. Other values are discussed with the corresponding commands.

**Table 157** Input Values for Address Commands

| LABEL | DESCRIPTION |
|---|---|
| *object_name* | The name of the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *group_name* | The name of the address group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *interface_name* | The name of the interface. This depends on the ZyWALL / USG model.<br><br>For some modelsFor some models, use ge*x*, *x* = 1 ~ N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model.<br><br>~~For the ZyWALL USG 200 and below~~For other models, use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. |

The following sections list the address object and address group commands.

## 31.2.1 Address Object Commands

This table lists the commands for address objects.

**Table 158** address-object and address6-object Commands

| COMMAND | DESCRIPTION |
|---|---|
| show {address-object \| address6-object \| service-object \| schedule-object} [*object_name*] | Displays information about the specified object or all the objects of the specified type. |
| address-object *object_name* {*ip* \| *ip_range* \| *ip_subnet* \| interface-ip \| interface-subnet \| interface-gateway} {*interface*} | Creates the specified IPv4 address object using the specified parameters.<br>*ip_range*: <1..255>.<0..255>.<0..255>.<1..255>-<1..255>.<0..255>.<0..255>.<1..255><br>*ip_subnet*: <1..255>.<0..255>.<0..255>.<0..255>/<1..32><br>*interface*: Specify an interface when you create an object based on an interface. |
| no address-object *object_name* | Deletes the specified address object. |
| address-object rename *object_name object_name* | Renames the specified address (first *object_name*) to the second *object_name*. |
| [no] address6-object *object_name* {*ipv6_address* \| *ipv6_range* \| *ipv6_subnet*} | Creates the specified IPv6 address object using the specified parameters. The no command removes the specified address object.<br>*ipv6_address*: IPv6 address<br>*ipv6_range*: IPv6 address range. For example: fe80:1234::1-fe80:1234::ffff<br>*ipv6_subnet*: IPv6 prefix format. For example: fe80::211:85ff:fe0e:dec/128 |
| [no] address6-object *object_name* interface-ip *interface* {dhcpv6 \| link-local \| slaac \| static} {*addr_index*} | Creates the specified IPv6 address object based on the specified interface object. Specify whether it is a DHCPv6 server, link-local IP address, StateLess Address Auto Configuration IP address (slaac), or static IPv6 address. The no command removes the specified address object. |
| [no] address6-object *object_name* interface-subnet *interface* {dhcpv6 \| slaac \| static} {*addr_index*} | Creates the specified IPv6 address object based on the specified interface subnet object. Specify whether it is a DHCPv6 server, SLAAC, or static IPv6 address. The no command removes the specified address object. |
| [no]adderss6-object *object_name* interface-gateway *interface* { slaac \| static} {*addr_index*} | Creates the specified IPv6 address object based on the specified interface gateway object. Specify whether it is a SLAAC or static IPv6 address. The no command removes the specified address object. |

### 31.2.1.1 Address Object Command Examples

The following example creates three IPv4 address objects and then deletes one.

```
Router# configure terminal
Router(config)# address-object A0 192.168.1.1
Router(config)# address-object A1 192.168.1.1-192.168.1.20
Router(config)# address-object A2 192.168.1.0/24
Router(config)# show address-object
Object name                     Type    Address                         Ref.
=====================================================================
A0                              HOST    192.168.1.1                       0
A1                              RANGE   192.168.1.1-192.168.1.20      0
A2                              SUBNET 192.168.1.0/24                  0
Router(config)# no address-object A2
Router(config)# show address-object
Object name                     Type    Address                         Ref.
=====================================================================
A0                              HOST    192.168.1.1                       0
A1                              RANGE   192.168.1.1-192.168.1.20      0
```

The following example creates host, range, subnet, and link local IPv6 address objects and then deletes the subnet IPv6 address object.

```
> enable
Router# configure terminal
Router(config)# address6-object B0 fe80::211:85ff:fe0e:cdec
Router(config)# address6-object B1 fe80::211:85ff:fe0e:1-fe80::211:85ff:fe0e:ff
Router(config)# address6-object B2 fe80::211:85ff:fe0e:cdec/128
Router(config)# address6-object B3 interface-ip ge1 link-local
Router(config)# show address6-object
Object name                     Type              Address Type              Index
Address
Note            Ref.
=============================================================================
B0                              HOST
fe80::211:85ff:fe0e:cdec
                0
B1                              RANGE
fe80::211:85ff:fe0e:1-fe80::211:85ff:fe0e:ff
                0
B2                              SUBNET
fe80::211:85ff:fe0e:cdec/128
                0
B3                              INTERFACE IP      LINK LOCAL                1
fe80::213:49ff:feaa:cb88
ge1             0

Router(config)# no address6-object B2
Router(config)# show address6-object
Object name                     Type              Address Type              Index
Address
Note            Ref.
=============================================================================
B0                              HOST
fe80::211:85ff:fe0e:cdec
                0
B1                              RANGE
fe80::211:85ff:fe0e:1-fe80::211:85ff:fe0e:ff
                0
B3                              INTERFACE IP      LINK LOCAL                1
fe80::213:49ff:feaa:cb88
ge1             0
```

## 31.2.2 Address Group Commands

This table lists the commands for address groups.

**Table 159** object-group Commands: Address Groups

| COMMAND | DESCRIPTION |
|---|---|
| `show object-group {address \| address6} [group_name]` | Displays information about the specified address group or about all address groups. |
| `[no] object-group address group_name` | Creates the specified address group if necessary and enters sub-command mode. The `no` command deletes the specified address group. |
| `[no] address-object object_name` | Adds the specified address to the specified address group. The `no` command removes the specified address from the specified group. |
| `[no] object-group group_name` | Adds the specified address group (second *group_name*) to the specified address group (first *group_name*). The `no` command removes the specified address group from the specified address group. |

**Table 159** object-group Commands: Address Groups (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] description *description* | Sets the description to the specified value. The no command clears the description.<br>*description*: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long. |
| object-group address rename *group_name group_name* | Renames the specified address group from the first *group_name* to the second *group_name*. |

### 31.2.2.1 Address Group Command Examples

The following commands create three address objects A0, A1, and A2 and add A1 and A2 to address group RD.

```
Router# configure terminal
Router(config)# address-object A0 192.168.1.1
Router(config)# address-object A1 192.168.1.2-192.168.2.20
Router(config)# address-object A2 192.168.3.0/24
Router(config)# object-group address RD
Router(group-address)# address-object A1
Router(group-address)# address-object A2
Router(group-address)# exit
Router(config)# show object-group address
Group name                      Reference
Description
================================================================================
TW_TEAM                         5

RD                              0

Router(config)# show object-group address RD
Object/Group name               Type   Reference
================================================================================
A1                              Object 1
A2                              Object 1
```

# 32

# Services

Use service objects to define TCP applications, UDP applications, and ICMP messages. You can also create service groups to refer to multiple service objects in other features.

## 32.1 Services Overview

See the appendices in the web configurator's User Guide for a list of commonly-used services.

## 32.2 Services Commands Summary

The following table describes the values required for many service object and service group commands. Other values are discussed with the corresponding commands.

**Table 160** Input Values for Service Commands

| LABEL | DESCRIPTION |
|---|---|
| *group_name* | The name of the service group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *object_name* | The name of the service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |

The following sections list the service object and service group commands.

### 32.2.1 Service Object Commands

The first table lists the commands for service objects.

**Table 161** service-object Commands: Service Objects

| COMMAND | DESCRIPTION |
|---|---|
| `show service-object [object_name]` | Displays information about the specified service or about all the services. |
| `no service-object object_name` | Deletes the specified service. |
| `service-object object_name {tcp \| udp} {eq <1..65535> \| range <1..65535> <1..65535>}` | Creates the specified TCP service or UDP service using the specified parameters. |

**Table 161** service-object Commands: Service Objects (continued)

| COMMAND | DESCRIPTION |
|---|---|
| service-object *object_name* icmp *icmp_value* | Creates the specified ICMP message using the specified parameters.<br>*icmp_value*: <0..255> \| alternate-address \| conversion-error \| echo \| echo-reply \| information-reply \| information-request \| mask-reply \| mask-request \| mobile-redirect \| parameter-problem \| redirect \| router-advertisement \| router-solicitation \| source-quench \| time-exceeded \| timestamp-reply \| timestamp-request \| unreachable |
| service-object *object_name* protocol <1..255> | Creates the specified user-defined service using the specified parameters. |
| service-object rename *object_name object_name* | Renames the specified service from the first *object_name* to the second *object_name*. |
| service-object *object_name* icmpv6 {<0..255> \| neighbor-solicitation \| router-advertisement \| echo \| packet-toobig \| router-solicitation \| echo-reply \| parameter-problem \| time-exceeded \| neighbor-advertisement \| redirect \| unreachable} | Creates the specified ICMPv6 message using the specified parameters. |

### 32.2.1.1 Service Object Command Examples

The following commands create four services, displays them, and then removes one of them.

```
Router# configure terminal
Router(config)# service-object TELNET tcp eq 23
Router(config)# service-object FTP tcp range 20 21
Router(config)# service-object ICMP_ECHO icmp echo
Router(config)# service-object MULTICAST protocol 2
Router(config)# show service-object
Object name                 Protocol         Minmum port  Maxmum port  Ref.
=========================================================================TELNET
TCP               23            23             0
FTP                           TCP              20             21             0
ICMP_ECHO                   ICMP              0              0              0
MULTICAST                   2                  0              0              0
Router(config)# no service-object ICMP_ECHO
Router(config)# show service-object
Object name                 Protocol         Minmum port  Maxmum port  Ref.
=========================================================================TELNET
TCP               23            23             0
FTP                           TCP              20             21             0
MULTICAST                   2                  0              0              0
```

## 32.2.2 Service Group Commands

The first table lists the commands for service groups.

**Table 162** object-group Commands: Service Groups

| COMMAND | DESCRIPTION |
|---|---|
| show object-group service *group_name* | Displays information about the specified service group. |
| [no] object-group service *group_name* | Creates the specified service group if necessary and enters sub-command mode. The no command removes the specified service group. |
| [no] service-object *object_name* | Adds the specified service to the specified service group. The no command removes the specified service from the specified group. |

**Table 162** object-group Commands: Service Groups (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] object-group *group_name* | Adds the specified service group (second *group_name*) to the specified service group (first *group_name*). The no command removes the specified service group from the specified service group. |
| [no] description *description* | Sets the description to the specified value. The no command removes the description.<br>*description*: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long. |
| object-group service rename *group_name group_name* | Renames the specified service group from the first *group_name* to the second *group_name*. |

### 32.2.2.1 Service Group Command Examples

The following commands create service ICMP_ECHO, create service group SG1, and add ICMP_ECHO to SG1.

```
Router# configure terminal
Router(config)# service-object ICMP_ECHO icmp echo
Router(config)# object-group service SG1
Router(group-service)# service-object ICMP_ECHO
Router(group-service)# exit
Router(config)# show service-object ICMP_ECHO
Object name                    Protocol         Minmum port  Maxmum port  Ref.
==============================================================================
ICMP_ECHO                      ICMP             8            8            1
Router(config)# show object-group service SG1
Object/Group name              Type   Reference
==============================================================================
ICMP_ECHO                      Object 1
```

# 33

# Schedules

Use schedules to set up one-time and recurring schedules for policy routes, firewall rules, application patrol, and content filtering.

## 33.1 Schedule Overview

The ZyWALL / USG supports two types of schedules: one-time and recurring. One-time schedules are effective only once, while recurring schedules usually repeat.

Note: Schedules are based on the current date and time in the ZyWALL / USG.

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.

## 33.2 Schedule Commands Summary

The following table describes the values required for many schedule commands. Other values are discussed with the corresponding commands.

**Table 163** Input Values for Schedule Commands

| LABEL | DESCRIPTION |
|---|---|
| *object_name* | The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *time* | 24-hour time, hours and minutes; <0..23>:<0..59>. |

The following table lists the schedule commands.

**Table 164** schedule Commands

| COMMAND | DESCRIPTION |
|---|---|
| `show schedule-object` | Displays information about the schedules in the ZyWALL / USG. |
| `no schedule-object` *object_name* | Deletes the schedule object. |

**Table 164** schedule Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| schedule-object *object_name date time date time* | Creates or updates a one-time schedule.<br>*date*: yyyy-mm-dd date format; yyyy-<01..12>-<01..31> |
| schedule-object *object_name time time* [*day*] [*day*] [*day*] [*day*] [*day*] [*day*] [*day*] | Creates or updates a recurring schedule.<br>*day*: 3-character day of the week; sun \| mon \| tue \| wed \| thu \| fri \| sat |

## 33.2.1 Schedule Command Examples

The following commands create recurring schedule SCHEDULE1 and one-time schedule SCHEDULE2 and then delete SCHEDULE1.

```
Router# configure terminal
Router(config)# schedule-object SCHEDULE1 11:00 12:00 mon tue wed thu fri
Router(config)# schedule-object SCHEDULE2 2006-07-29 11:00 2006-07-31 12:00
Router(config)# show schedule-object
Object name                     Type      Start/End                         Ref.
=============================================================================
SCHEDULE1                       Recurring 11:00/12:00 ===MonTueWedThuFri=== 0
SCHEDULE2                       Once      2006-07-29 11:00/2006-07-31 12:00 0

Router(config)# no schedule-object SCHEDULE1
Router(config)# show schedule-object
Object name                     Type      Start/End                         Ref.
=============================================================================
SCHEDULE2                       Once      2006-07-29 11:00/2006-07-31 12:00 0
```

# 34

# AAA Server

This chapter introduces and shows you how to configure the ZyWALL / USG to use external authentication servers.

## 34.1 AAA Server Overview

You can use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network.

The following lists the types of authentication server the ZyWALL / USG supports.

- Local user database

  The ZyWALL / USG uses the built-in local user database to authenticate administrative users logging into the ZyWALL / USG's web configurator or network access users logging into the network through the ZyWALL / USG. You can also use the local user database to authenticate VPN users.
- Directory Service (LDAP/AD)

  LDAP (Lightweight Directory Access Protocol)/AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.
- RADIUS

  RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

## 34.2 Authentication Server Command Summary

This section describes the commands for authentication server settings.

### 34.2.1 ad-server Commands

The following table lists the `ad-server` commands you use to set the default AD server.

**Table 165** ad-server Commands

| COMMAND | DESCRIPTION |
|---|---|
| `show ad-server` | Displays the default AD server settings. |
| `[no] ad-server basedn` *basedn* | Sets a base distinguished name (DN) for the default AD server. A base DN identifies an AD directory. The `no` command clears this setting. |

**Table 165** ad-server Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] ad-server binddn *binddn* | Sets the user name the ZyWALL / USG uses to log into the default AD server. The no command clears this setting. |
| [no] ad-server cn-identifier *uid* | Sets the unique common name (cn) to identify a record. The no command clears this setting. |
| [no] ad-server host *ad_server* | Sets the AD server address. Enter the IP address (in dotted decimal notation) or the domain name. The no command clears this setting. |
| [no] ad-server password *password* | Sets the bind password. This password will be encrypted when you use the show ad-server command to display. The no command clears this setting. |
| [no] ad-server password-encrypted *password* | Sets the encrypted password (less than 32 alphanumerical characters) in order to hide the real password from people behind you when you are configuring AD server password. This password is displayed as what you typed when you use the show ad-server command. |
| [no] ad-server port *port_no* | Sets the AD port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting. |
| [no] ad-server search-time-limit *time* | Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting. |
| [no] ad-server ssl | Enables the ZyWALL / USG to establish a secure connection to the AD server. The no command disables this feature. |

## 34.2.2 ldap-server Commands

The following table lists the ldap-server commands you use to set the default LDAP server.

**Table 166** ldap-server Commands

| COMMAND | DESCRIPTION |
|---|---|
| show ldap-server | Displays current LDAP server settings. |
| [no] ldap-server basedn *basedn* | Sets a base distinguished name (DN) for the default LDAP server. A base DN identifies an LDAP directory. The no command clears this setting. |
| [no] ldap-server binddn *binddn* | Sets the user name the ZyWALL / USG uses to log into the default LDAP server.<br>The no command clears this setting. |
| [no] ldap-server cn-identifier *uid* | Sets the unique common name (cn) to identify a record.<br>The no command clears this setting. |
| [no] ldap-server host *ldap_server* | Sets the LDAP server address. Enter the IP address (in dotted decimal notation) or the domain name. The no command clears this setting. |
| [no] ldap-server password *password* | Sets the bind password. The no command clears this setting. |
| [no] ldap-server password-encrypted *password* | Sets an encrypted bind password. The no command clears this setting. |
| [no] ldap-server port *port_no* | Sets the LDAP port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting. |
| [no] ldap-server search-time-limit *time* | Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting. |
| [no] ldap-server ssl | Enables the ZyWALL / USG to establish a secure connection to the LDAP server. The no command disables this feature. |

## 34.2.3 radius-server Commands

The following table lists the `radius-server` commands you use to set the default RADIUS server.

**Table 167** radius-server Commands

| COMMAND | DESCRIPTION |
|---|---|
| `show radius-server` | Displays the default RADIUS server settings. |
| `[no] radius-server host` *radius_server* `auth-port` *auth_port* | Sets the RADIUS server address and service port number. Enter the IP address (in dotted decimal notation) or the domain name of a RADIUS server. The `no` command clears the settings. |
| `[no] radius-server key` *secret* | Sets a password (up to 15 alphanumeric characters) as the key to be shared between the RADIUS server and the ZyWALL / USG. The `no` command clears this setting. |
| `[no] radius-server timeout` *time* | Sets the search timeout period (in seconds). Enter a number between 1 and 300. The `no` command clears this setting. |

## 34.2.4 radius-server Command Example

The following example sets the secret key and timeout period of the default RADIUS server (172.23.10.100) to “87643210” and 80 seconds.

```
Router# configure terminal
Router(config)# radius-server host 172.23.10.100 auth-port 1812
Router(config)# radius-server key 876543210
Router(config)# radius-server timeout 80
Router(config)# show radius-server
host                : 172.23.10.100
authentication port: 1812
key                 : 876543210
timeout             : 80
Router(config)#
```

## 34.2.5 aaa group server ad Commands

The following table lists the `aaa group server ad` commands you use to configure a group of AD servers.

**Table 168** aaa group server ad Commands

| COMMAND | DESCRIPTION |
|---|---|
| `clear aaa group server ad [`*group-name*`]` | Deletes all AD server groups or the specified AD server group.<br><br>Note: You can NOT delete a server group that is currently in use. |
| `show aaa group server ad` *group-name* | Displays the specified AD server group settings. |
| `[no] aaa group server ad` *group-name* | Sets a descriptive name for an AD server group. Use this command to enter the sub-command mode.<br><br>The `no` command deletes the specified server group. |
| `aaa group server ad rename` *group-name group-name* | Changes the descriptive name for an AD server group. |
| `aaa group server ad` *group-name* | Enter the sub-command mode to configure an AD server group. |
| `[no] case-sensitive` | Specify whether or not the server checks the username case. Set this to be the same as the server’s behavior. |

**Table 168** aaa group server ad Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] server alternative-cn-identifier *uid* | Sets the second type of identifier that the users can use to log in if any. For example “name” or “e-mail address”. The no command clears this setting. |
| [no] server basedn *basedn* | Sets the base DN to point to the AD directory on the AD server group. The no command clears this setting. |
| [no] server binddn *binddn* | Sets the user name the ZyWALL / USG uses to log into the AD server group. The no command clears this setting. |
| [no] server cn-identifier *uid* | Sets the user name the ZyWALL / USG uses to log into the AD server group. The no command clears this setting. |
| [no] server description *description* | Sets the descriptive information for the AD server group. You can use up to 60 printable ASCII characters. The no command clears the setting. |
| [no] server group-attribute *group-attribute* | Sets the name of the attribute that the ZyWALL / USG is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values.<br>For example you could have an attribute named “memberOf” with values like “sales”, “RD”, and “management”. Then you could also create an ext-group-user user object for each group. One with “sales” as the group identifier, another for “RD” and a third for “management”. The no command clears the setting. |
| [no] server host *ad_server* | Enter the IP address (in dotted decimal notation) or the domain name of an AD server to add to this group. The no command clears this setting. |
| [no] server password *password* | Sets the bind password (up to 15 alphanumerical characters). The no command clears this setting. |
| [no] server port *port_no* | Sets the AD port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting. |
| [no] server search-time-limit *time* | Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting and set this to the default setting of 5 seconds. |
| [no] server ssl | Enables the ZyWALL / USG to establish a secure connection to the AD server. The no command disables this feature. |

## 34.2.6 aaa group server ldap Commands

The following table lists the aaa group server ldap commands you use to configure a group of LDAP servers.

**Table 169** aaa group server ldap Commands

| COMMAND | DESCRIPTION |
|---|---|
| clear aaa group server ldap [*group-name*] | Deletes all LDAP server groups or the specified LDAP server group.<br>Note: You can NOT delete a server group that is currently in use. |
| show aaa group server ldap *group-name* | Displays the specified LDAP server group settings. |
| [no] aaa group server ldap *group-name* | Sets a descriptive name for an LDAP server group. Use this command to enter the sub-command mode.<br>The no command deletes the specified server group. |
| aaa group server ldap rename *group-name group-name* | Changes the descriptive name for an LDAP server group. |
| aaa group server ldap *group-name* | Enter the sub-command mode. |

**Table 169** aaa group server ldap Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] case-sensitive | Specify whether or not the server checks the username case. Set this to be the same as the server's behavior. |
| [no] server alternative-cn-identifier *uid* | Sets the second type of identifier that the users can use to log in if any. For example "name" or "e-mail address". The no command clears this setting. |
| [no] server basedn *basedn* | Sets the base DN to point to the LDAP directory on the LDAP server group. The no command clears this setting. |
| [no] server binddn *binddn* | Sets the user name the ZyWALL / USG uses to log into the LDAP server group. The no command clears this setting. |
| [no] server cn-identifier *uid* | Sets the user name the ZyWALL / USG uses to log into the LDAP server group. The no command clears this setting. |
| [no] server description *description* | Sets the descriptive information for the LDAP server group. You can use up to 60 printable ASCII characters. The no command clears this setting. |
| [no] server group-attribute *group-attribute* | Sets the name of the attribute that the ZyWALL / USG is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values.<br>For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create an ext-group-user user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management". The no command clears the setting. |
| [no] server host *ldap_server* | Enter the IP address (in dotted decimal notation) or the domain name of an LDAP server to add to this group. The no command clears this setting. |
| [no] server password *password* | Sets the bind password (up to 15 characters). The no command clears this setting. |
| [no] server port *port_no* | Sets the LDAP port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting. |
| [no] server search-time-limit *time* | Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting and set this to the default setting of 5 seconds. |
| [no] server ssl | Enables the ZyWALL / USG to establish a secure connection to the LDAP server. The no command disables this feature. |

## 34.2.7 aaa group server radius Commands

The following table lists the aaa group server radius commands you use to configure a group of RADIUS servers.

**Table 170** aaa group server radius Commands

| COMMAND | DESCRIPTION |
|---|---|
| clear aaa group server radius *group-name* | Deletes all RADIUS server groups or the specified RADIUS server group.<br>Note: You can NOT delete a server group that is currently in use. |
| show aaa group server radius *group-name* | Displays the specified RADIUS server group settings. |
| [no] aaa group server radius *group-name* | Sets a descriptive name for the RADIUS server group. The no command deletes the specified server group. |
| aaa group server radius rename {*group-name-old*} *group-name-new* | Sets the server group name. |

**Table 170** aaa group server radius Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| aaa group server radius *group-name* | Enter the sub-command mode. |
| [no] case-sensitive | Specify whether or not the server checks the username case. Set this to be the same as the server's behavior. |
| [no] server description *description* | Sets the descriptive information for the RADIUS server group. You can use up to 60 printable ASCII characters. The no command clears the setting. |
| [no] server group-attribute <1-255> | Sets the value of an attribute that the ZyWALL / USG is used to determine to which group a user belongs.<br>This attribute's value is called a group identifier. You can add **ext-group-user** user objects to identify groups based on different group identifier values.<br>For example, you could configure attributes 1,10 and 100 and create a **ext-group-user** user object for each of them. The no command clears the setting. |
| [no] server host *radius_server* | Enter the IP address (in dotted decimal notation) or the domain name of a RADIUS server to add to this server group. The no command clears this setting. |
| [no] server key *secret* | Sets a password (up to 15 alphanumeric characters) as the key to be shared between the RADIUS server(s) and the ZyWALL / USG. The no command clears this setting. |
| [no] server timeout *time* | Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting and set this to the default setting of 5 seconds. |

## 34.2.8 aaa group server Command Example

The following example creates a RADIUS server group with two members and sets the secret key to "12345678" and the timeout to 100 seconds. Then this example also shows how to view the RADIUS group settings.

```
Router# configure terminal
Router(config)# aaa group server radius RADIUSGroup1
Router(group-server-radius)# server host 192.168.1.100 auth-port 1812
Router(group-server-radius)# server host 172.23.22.100 auth-port 1812
Router(group-server-radius)# server key 12345678
Router(group-server-radius)# server timeout 100
Router(group-server-radius)# exit
Router(config)# show aaa group server radius RADIUSGroup1
key                : 12345678
timeout            : 100
description        :
group attribute    : 11

No.  Host Member                                                    Auth. Port

=========================================================================
1    192.168.1.100                                                 1812

2    172.23.22.100                                                 1812
```

# 35

# Authentication Objects

This chapter shows you how to select different authentication methods for user authentication using the AAA servers or the internal user database.

## 35.1 Authentication Objects Overview

After you have created the AAA server objects, you can specify the authentication objects (containing the AAA server information) that the ZyWALL / USG uses to authenticate users (using VPN or managing through HTTP/HTTPS).

## 35.2 aaa authentication Commands

The following table lists the `aaa authentication` commands you use to configure an authentication profile.

**Table 171** aaa authentication Commands

| COMMAND | DESCRIPTION |
|---|---|
| `aaa authentication rename` *`profile-name-old profile-name-new`* | Changes the profile name.<br>*`profile-name`*: You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| `clear aaa authentication` *`profile-name`* | Deletes all authentication profiles or the specified authentication profile.<br>Note: You can NOT delete a profile that is currently in use. |
| `show aaa authentication {`*`group-name`*`\|default}` | Displays the specified authentication server profile settings. |
| `[no] aaa authentication` *`profile-name`* | Sets a descriptive name for the authentication profile. The `no` command deletes a profile. |
| `[no] aaa authentication default` *`member1 [member2] [member3] [member4]`* | Sets the default profile to use the authentication method(s) in the order specified.<br>*`member`* = group ad, group ldap, group radius, or local.<br>Note: You must specify at least one member for each profile. Each type of member can only be used once in a profile.<br>The `no` command clears the specified authentication method(s) for the profile. |

**Table 171** aaa authentication Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] aaa authentication *profile-name member1* [*member2*] [*member3*] [*member4*] | Sets the profile to use the authentication method(s) in the order specified.<br>*member* = group ad, group ldap, group radius, or local.<br>Note: You must specify at least one member for each profile. Each type of member can only be used once in a profile.<br>The no command clears the specified authentication method(s) for the profile. |
| aaa authentication [no] match-default-group | Enable this to treat a user successfully authenticated by a remote auth server as a defat-ext-user. If the remote authentication server is LDAP, the default-ext-user account is an ldap-user. If the remote authentication server is AD, the default-ext-user account is an ad-user. If the remote authentication server is RADIUS, the default-ext-user account is a radius-user. |

## 35.2.1 aaa authentication Command Example

The following example creates an authentication profile to authentication users using the LDAP server group and then the local user database.

```
Router# configure terminal
Router(config)# aaa authentication LDAPuser group ldap local
Router(config)# show aaa authentication LDAPuser
No.  Method
================================================================================
0    ldap
1    local
Router(config)#
```

# 35.3 test aaa Command

The following table lists the test aaa command you use to teat a user account on an authentication server.

**Table 172** test aaa Command

| COMMAND | DESCRIPTION |
|---|---|
| test aaa {server\|secure-server} {ad\|ldap} host {*hostname*\|*ipv4-address*} [host {*hostname*\|*ipv4-address*}] port <1..65535> base-dn *base-dn-string* [bind-dn *bind-dn-string* password *password*] login-name-attribute *attribute* [alternative-login-name-attribute *attribute*] account *account-name* | Tests whether a user account exists on the specified authentication server. |

## 35.3.1 Test a User Account Command Example

The following example shows how to test whether a user account named userABC exists on the AD authentication server which uses the following settings:

- IP address: 172.16.50.1
- Port: 389
- Base-dn: DC=ZyXEL,DC=com

- Bind-dn: zyxel\engineerABC
- Password: abcdefg
- Login-name-attribute: sAMAccountName

The result shows the account exists on the AD server. Otherwise, the ZyWALL / USG responds an error.

```
Router> test aaa server ad host 172.16.50.1 port 389 base-dn DC=ZyXEL,DC=com bind-dn
zyxel\engineerABC password abcdefg login-name-attribute sAMAccountName account
userABC

dn:: Q049MTIzNzco546L5aOr56uRKSxPVT1XaXRoTWFpbCxEQz1aeVhFTCxEQz1jb20=
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn:: MTIzNzco546L5aOr56uRKQ==
sn: User
l: 2341100
-------------------------SNIP!-----------------------------------------
```

# 36

# Certificates

This chapter explains how to use the **Certificates**.

## 36.1 Certificates Overview

The ZyWALL / USG can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyWALL / USG to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

## 36.2 Certificate Commands

This section describes the commands for configuring certificates.

## 36.3 Certificates Commands Input Values

The following table explains the values you can input with the `certificate` commands.

**Table 173** Certificates Commands Input Values

| LABEL | DESCRIPTION |
|---|---|
| *certificate_name* | The name of a certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters. |
| *cn_address* | A common name IP address identifies the certificate's owner. Type the IP address in dotted decimal notation. |
| *cn_domain_name* | A common name domain name identifies the certificate's owner. The domain name is for identification purposes only and can be any string. The domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods. |
| *cn_email* | A common name e-mail address identifies the certificate's owner. The e-mail address is for identification purposes only and can be any string. The e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore. |
| *organizational_unit* | Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore. |

**Table 173** Certificates Commands Input Values (continued)

| LABEL | DESCRIPTION |
|---|---|
| *organization* | Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore. |
| *country* | Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore. |
| *key_length* | Type a number to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space. |
| *password* | When you have the ZyWALL / USG enroll for a certificate immediately online, the certification authority may want you to include a key (password) to identify your certification request. Use up to 31 of the following characters. a-zA-Z0-9;\|`~!@#$%^&*()_+\{}':,./<>=- |
| *ca_name* | When you have the ZyWALL / USG enroll for a certificate immediately online, you must have the certification authority's certificate already imported as a trusted certificate. Specify the name of the certification authority's certificate. It can be up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters. |
| *url* | When you have the ZyWALL / USG enroll for a certificate immediately online, enter the IP address (or URL) of the certification authority server. You can use up to 511 of the following characters. a-zA-Z0-9'()+,/:.=?;!*#@$_%- |

# 36.4 Certificates Commands Summary

The following table lists the commands that you can use to display and manage the ZyWALL / USG's summary list of certificates and certification requests. You can also create certificates or certification requests. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

**Table 174** ca Commands Summary

| COMMAND | DESCRIPTION |
|---|---|
| ca enroll cmp name *certificate_name* cn-type {ip cn *cn_address*\|fqdn cn *cn_domain_name*\|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa\|dsa} key-len *key_length* num <0..99999999> password *password* ca *ca_name* url *url*; | Enrolls a certificate with a CA using Certificate Management Protocol (CMP). The certification authority may want you to include a reference number and key (password) to identify your certification request. |
| ca enroll scep name *certificate_name* cn-type {ip cn *cn_address*\|fqdn cn *cn_domain_name*\|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa\|dsa} key-len *key_length* password *password* ca *ca_name* url *url* | Enrolls a certificate with a CA using Simple Certificate Enrollment Protocol (SCEP). The certification authority may want you to include a key (password) to identify your certification request. |
| ca generate pkcs10 name *certificate_name* cn-type {ip cn *cn_address*\|fqdn cn *cn_domain_name*\|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa\|dsa} key-len *key_length* | Generates a PKCS#10 certification request. |
| ca generate pkcs12 name *name* password *password* | Generates a PKCS#12 certificate. |
| ca generate x509 name *certificate_name* cn-type {ip cn *cn_address*\|fqdn cn *cn_domain_name*\|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa\|dsa} key-len *key_length* | Generates a self-signed x509 certificate. |
| ca rename category {local\|remote} *old_name new_name* | Renames a local (my certificates) or remote (trusted certificates) certificate. |

**Table 174** ca Commands Summary (continued)

| COMMAND | DESCRIPTION |
|---|---|
| ca validation *remote_certificate* | Enters the sub command mode for validation of certificates signed by the specified remote (trusted) certificates. |
| cdp {activate\|deactivate} | Turns certificate revocation on or off. When it is turned on, the ZyWALL / USG validates a certificate by getting a Certificate Revocation List (CRL) through HTTP or LDAP (can be configured after activating the LDAP checking option) and online responder (can be configured after activating the OCSP checking option). You also need to configure the OSCP or LDAP server details. |
| ldap {activate\|deactivate} | Has the ZyWALL / USG check (or not check) incoming certificates that are signed by this certificate against a Certificate Revocation List (CRL) on a LDAP (Lightweight Directory Access Protocol) directory server. |
| ldap ip {*ip*\|*fqdn*} port <1..65535> [id *name* password *password*] [deactivate] | Sets the validation configuration for the specified remote (trusted) certificate where the directory server uses LDAP.<br>*ip*: Type the IP address (in dotted decimal notation) or the domain name of the directory server. The domain name can use alphanumeric characters, periods and hyphens. Up to 255 characters.<br>port: Specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.<br>The ZyWALL / USG may need to authenticate itself in order to access the CRL directory server. Type the login name (up to 31 characters) from the entity maintaining the server (usually a certification authority). You can use alphanumeric characters, the underscore and the dash.<br>Type the password (up to 31 characters) from the entity maintaining the CRL directory server (usually a certification authority). You can use the following characters: a-zA-Z0-9;\|`~!@#$%^&*()_+\{}':,./<>=- |
| ocsp {activate\|deactivate} | Has the ZyWALL / USG check (or not check) incoming certificates that are signed by this certificate against a directory server that uses OCSP (Online Certificate Status Protocol). |
| ocsp url *url* [id *name* password *password*] [deactivate] | Sets the validation configuration for the specified remote (trusted) certificate where the directory server uses OCSP.<br>*url*: Type the protocol, IP address and pathname of the OCSP server.<br>name: The ZyWALL / USG may need to authenticate itself in order to access the OCSP server. Type the login name (up to 31 characters) from the entity maintaining the server (usually a certification authority). You can use alphanumeric characters, the underscore and the dash.<br>password: Type the password (up to 31 characters) from the entity maintaining the OCSP server (usually a certification authority). You can use the following characters: a-zA-Z0-9;\|`~!@#$%^&*()_+\{}':,./<>=- |
| no ca category {local\|remote} *certificate_name* | Deletes the specified local (my certificates) or remote (trusted certificates) certificate. |
| no ca validation *name* | Removes the validation configuration for the specified remote (trusted) certificate. |

**Table 174** ca Commands Summary (continued)

| COMMAND | DESCRIPTION |
|---|---|
| `show ca category {local\|remote} name certificate_name certpath` | Displays the certification path of the specified local (my certificates) or remote (trusted certificates) certificate. |
| `show ca category {local\|remote} [name certificate_name format {text\|pem}]` | Displays a summary of the certificates in the specified category (local for my certificates or remote for trusted certificates) or the details of a specified certificate. |
| `show ca validation name name` | Displays the validation configuration for the specified remote (trusted) certificate. |
| `show ca spaceusage` | Displays the storage space in use by certificates. |

# 36.5 Certificates Commands Examples

The following example creates a self-signed X.509 certificate with IP address 10.0.0.58 as the common name. It uses the RSA key type with a 512 bit key. Then it displays the list of local certificates. Finally it deletes the pkcs12request certification request.

```
Router# configure terminal
Router(config)# ca generate x509 name test_x509 cn-type ip cn 10.0.0.58 key-type rsa
key-len 512
Router(config)# show ca category local
certificate: default
  type: SELF
  subject: CN=ZyWALL-1050_Factory_Default_Certificate
  issuer: CN=ZyWALL-1050_Factory_Default_Certificate
  status: VALID
  ID: ZyWALL-1050_Factory_Default_Certificate
    type: EMAIL
  valid from: 2003-01-01 00:38:30
  valid to: 2022-12-27 00:38:30
certificate: test
  type: REQ
  subject: CN=1.1.1.1
  issuer: none
  status: VALID
  ID: 1.1.1.1
    type: IP
  valid from: none
  valid to: none
certificate: pkcs12request
  type: REQ
  subject: CN=1.1.1.2
  issuer: none
  status: VALID
  ID: 1.1.1.2
    type: IP
  valid from: none
  valid to: none
certificate: test_x509
  type: SELF
  subject: CN=10.0.0.58
  issuer: CN=10.0.0.58
  status: VALID
  ID: 10.0.0.58
    type: IP
  valid from: 2006-05-29 10:26:08
  valid to: 2009-05-28 10:26:08
Router(config)# no ca category local pkcs12request
```

# 37

# ISP Accounts

Use ISP accounts to manage Internet Service Provider (ISP) account information for PPPoE, PPTP and cellular interfaces.

## 37.1 ISP Accounts Overview

An ISP account is a profile of settings for Internet access using PPPoE, PPTP, or cellular.

### 37.1.1 PPPoE and PPTP Account Commands

The following table lists the PPPoE and PPTP ISP account commands.

**Table 175** PPPoE and PPTP ISP Account Commands

| COMMAND | DESCRIPTION |
|---|---|
| `show account [pppoe` *`profile_name`* `\| pptp` *`profile_name`*`]` | Displays information about the specified account(s). |
| `[no] account {pppoe \| pptp}` *`profile_name`* | Creates a new ISP account with name *`profile_name`* if necessary and enters sub-command mode. The `no` command deletes the specified ISP account.<br><br>*`profile_name`*: use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| `[no] user` *`username`* | Sets the username for the specified ISP account. The `no` command clears the username.<br><br>*`username`*: You can use alphanumeric, underscores (_), dashes (-), commas (,), and `/@$` characters, and it can be up to 64 characters long. |
| `[no] password` *`password`* | Sets the password for the specified ISP account. The `no` command clears the password.<br><br>*`password`*: You can use up to 63 printable ASCII characters. Spaces are not allowed. |
| `[no] authentication {chap-pap \| chap \| pap \| mschap \| mschap-v2}` | Sets the authentication for the specified ISP account. The `no` command sets the authentication to chap-pap. |
| `[no] compression {yes \| no}` | Turns compression on or off for the specified ISP account. The `no` command turns off compression. |
| `[no] idle <0..360>` | Sets the idle timeout for the specified ISP account. The `no` command sets the idle timeout to zero. |
| `[no] service-name {`*`ip`* `\|` *`hostname`* `\|` *`service_name`*`}` | Sets the service name for the specified PPPoE ISP account. The `no` command clears the service name.<br><br>*`hostname`*: You may up to 63 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.<br><br>*`service_name`*: You can use up to 63 alphanumeric characters, underscores (_), dashes (-), and `@$./` characters. |

**Table 175** PPPoE and PPTP ISP Account Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] server *ip* | Sets the PPTP server for the specified PPTP ISP account. The no command clears the server name. |
| [no] encryption {nomppe \| mppe-40 \| mppe-128} | Sets the encryption for the specified PPTP ISP account. The no command sets the encryption to nomppe. |
| [no] connection-id *connection_id* | Sets the connection ID for the specified PPTP ISP account. The no command clears the connection ID.<br>*connection_id*: You can use up to 31 alphanumeric characters, underscores (_), dashes (-), and colons (:). |

## 37.1.2 Cellular Account Commands

The following table lists the cellular ISP account commands.

**Table 176** Cellular Account Commands

| COMMAND | DESCRIPTION |
|---|---|
| show account cellular *profile_name* | Displays information about the specified account. |
| [no] account cellular *profile_name* | Creates a new cellular ISP account with name *profile_name* if necessary and enters sub-command mode. The no command deletes the specified ISP account.<br>*profile_name*: the cellular ISP account name format is "cellularx" where "x" is a number. For example, cellular1. |
| [no] apn *access_point_name* | Sets the Access Point Name (APN) for the cellular ISP account. The no command clears the APN.<br>*access_point_name*: Use up to 63 alphanumeric characters and underscores (_), dashes (-), periods (.), and /@\$#. |
| [no] dial-string *isp_dial_string* | Sets the dial string for the specified ISP account. The no command clears the dial-string.<br>*username*: Use up to 63 alphanumeric characters and underscores (_), dashes (-), periods (.), and /@\$#. |
| [no] user *username* | Sets the username for the specified ISP account. The no command clears the username.<br>*username*: Use up to 64 alphanumeric characters and underscores (_), dashes (-), periods (.), and /@\$#. |
| [no] password *password* | Sets the password for the specified ISP account. The no command clears the password.<br>*password*: Use up to 63 printable ASCII characters. Spaces are not allowed. |
| [no] authentication {none \| pap \| chap} | Sets the authentication for the cellular account. The no command sets the authentication to none. |
| [no] idle <0..360> | Sets the idle timeout for the cellular account. Zero disables the idle timeout. The no command sets the idle timeout to zero. |

# 38

# SSL Application

This chapter describes how to configure SSL application objects for use in SSL VPN.

## 38.1 SSL Application Overview

Configure an SSL application object to specify a service and a corresponding IP address of the server on the local network. You can apply one or more SSL application objects in the **VPN > SSL VPN** screen for a user account/user group.

### 38.1.1 SSL Application Object Commands

This table lists the commands for creating SSL application objects. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 177** SSL Application Object Commands

| COMMAND | DESCRIPTION |
|---|---|
| `show sslvpn application [application_object]` | Displays SSL VPN application objects. |
| `[no] sslvpn application application_object` | Enters the sub-command mode to create an SSL VPN application object. |
| `server-type {file-sharing \| owa \| web-server} url URL [entry-point entry_point]` | Specify the type of service for this SSL application.<br>`file-sharing`: create a file share application for VPN SSL.<br>`owa`: (Outlook Web Access) to allow users to access e-mails, contacts, calenders via an Microsoft Outlook-like interface using supported web browsers. The ZyWALL / USG supports one OWA object.<br>`web-server`: to allow access to the specified web site hosted on the local network.<br>`url`: Enter the fully qualified domain name (FQDN) or IP address of the application server. You must enter the “http://” or “https://” prefix. Remote users are restricted to access only files in this directory. For example, if you enter “\remote\” in this field, emote users can only access files in the “remote” directory.<br>*`entry-point`*: optional. Specify the name of the directory or file on the local server as the home page or home directory on the user screen. |

**Table 177** SSL Application Object Commands

| COMMAND | DESCRIPTION |
|---|---|
| server-type file-sharing share-path *share-path* | Specifies the IP address, domain name or NetBIOS name (computer name) of the file server and the name of the share to which you want to allow user access. Enter the path in one of the following formats.<br>"\\<IP address>\<share name>"<br>"\\<domain name>\<share name>"<br>"\\<computer name>\<share name>"<br>For example, if you enter "\\my-server\Tmp", this allows remote users to access all files and/or folders in the "\Tmp" share on the "my-server" computer. |
| server-type rdp server-address *server-address* [starting-port <1..65535> ending-port <1..65535>] [program-path *program-path*] | Creates an SSL application object to allow users to manage LAN computers that have Remote Desktop Protocol remote desktop server software installed.<br>Specify the listening ports of the LAN computer(s) running remote desktop server software. The ZyWALL / USG uses a port number from this range to send traffic to the LAN computer that is being remotely managed.<br>*program-path*: specify an application to open when a remote user logs into the remote desktop application. |
| server-type vnc server-address *server-address* [starting-port <1..65535> ending-port <1..65535>] | Creates an SSL application object to allow users to manage LAN computers that have Virtual Network Computing remote desktop server software installed.<br>Specify the listening ports of the LAN computer(s) running remote desktop server software. The ZyWALL / USG uses a port number from this range to send traffic to the LAN computer that is being remotely managed. |
| server-type weblink url *url* | Sets this to create a link to a web site you specified that you expect the SSL VPN users to commonly use.<br>*url*: Enter the fully qualified domain name (FQDN) or IP address of the application server. You must enter the "http://" or "https://" prefix. For example, https://1.2.3.4. SSL VPN users are restricted to access only web pages or files in this directory. For example, if you enter "\remote\" in this field, emote users can only access web pages or files in the "remote" directory.<br>If a link contains a file that is not within this domain, then SSL VPN users cannot access it. |
| no server-type | Remove the type of service configuration for this SSL application. |
| [no] webpage-encrypt | Turn on web encrypt to prevent users from saving the web content. |

## 38.1.2 SSL Application Command Examples

The following commands create and display a server-type SSL application object named ZW5 for a web server at IP address 192.168.1.12.

```
Router(config)# sslvpn application ZW5
Router(sslvpn application)# server-type web-server url http://192.168.1.12
Router(sslvpn application)# exit
Router(config)# show sslvpn application
SSL Application: ZW5
  Server Type: web-server
  URL: http://192.168.1.12
  Entry Point:
  Encrypted URL: ~aHR0cDovLzE5Mi4xNjguMS4xMi8=/
  Web Page Encryption: yes
  Reference: 1
```

# 39

# Endpoint Security

This chapter describes how to configure endpoint security objects for use in authentication policy and SSL VPN.

## 39.1 Endpoint Security Overview

Use Endpoint Security (EPS), also known as endpoint control, to make sure users' computers comply with defined corporate policies before they can access the network or an SSL VPN tunnel. After a successful user authentication, a user's computer must meet the endpoint security object's Operating System (OS) option and security requirements to gain access. You can configure the endpoint security object to require a user's computer to match just one of the endpoint security object's checking criteria or all of them. Configure endpoint security objects to use with the authentication policy and SSL VPN features.

### What Endpoint Security Can Check

The settings endpoint security can check vary depending on the OS of the user's computer. Depending on the OS, EPS can check user computers for the following:

- Operating System (Windows, Linux, Mac OSX, or others)
- Windows version and service pack version
- Windows Auto Update setting and installed security patches
- Personal firewall installation and activation
- Anti-virus installation and activation
- Windows registry settings
- Processes that the endpoint must execute
- Processes that the endpoint cannot execute
- The size and version of specific files

### Multiple Endpoint Security Objects

You can configure an authentication policy or SSL VPN policy to use multiple endpoint security objects. This allows checking of computers with different OSs or security settings. When a client attempts to log in, the ~~ZyWALL~~ZyWALL / USG checks the client's computer against the endpoint security objects one-by-one. The client's computer must match one of the force authentication or SSL VPN policy's endpoint security policies in order to gain access.

### Requirements

User computers must have Sun's Java (Java Runtime Environment or 'JRE') installed and enabled with a minimum version of 1.4.

## 39.1.1 Endpoint Security Commands Summary

The following table describes the values required for many endpoint security object commands. Other values are discussed with the corresponding commands.

**Table 178** Input Values for Endpoint Security Commands

| LABEL | DESCRIPTION |
|---|---|
| *profile_name* | The name of the endpoint security object. You may use 1-31 characters ("0-9", "a-z", "A-Z", "-", "_" with no spaces allowed). |
| *file_path* | This is a file with the full directory path in quotation marks "". For example, "C:\Program Files\Internet Explorer\iexplore.exe". |

The following sections list the endpoint security object commands.

## 39.1.2 Endpoint Security Object Commands

This table lists the commands for creating endpoint security objects. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 179** Endpoint Security Object Commands

| COMMAND | DESCRIPTION |
|---|---|
| `[no] eps failure-messages` *failure_messages* | Specify a message to display when a user's computer fails the endpoint security check. Use up to 1023 characters (0-9a-zA-Z;/?:@=+$\.-_!*'()%,"). For example, "Endpoint Security checking failed. Please contact your network administrator for help.". The `no` command removes the setting. |
| `show eps failure-messages` | Displays the message to display when a user's computer fails the endpoint security check. |
| `[no] eps profile` *profile_name* | Enters the sub-command mode. The `no` command removes an endpoint security object. |
| `[no] {anti-virus \| personal-firewall} activate` | If you set `windows` as the operating system (using the `os-type` command), you can set whether or not the user's computer is required to have anti-virus or personal firewall software installed. |
| `[no] anti-virus` *anti_virus_software_name* `detect-auto-protection {enable \| disable \| ignore}` | Sets a permitted anti-virus software package. If you want to enter multiple anti-virus software packages, use this command for each of them. Use the `list signature anti-virus` command to view the available anti-virus software package options.<br>`detect-auto-protection`: Set this to `enable` if the specified anti-virus software is not only detectable for the installation but also detectable for the activation status. You can check the settings for each anti-virus software by using the `show eps signature anti-virus` command.<br>The user's computer must have one of the listed anti-virus software packages to pass this checking item. For some anti-virus software the ZyWALL / USG can also detect whether or not the anti-virus software is activated; in those cases it must also be activated. |

**Table 179** Endpoint Security Object Commands

| COMMAND | DESCRIPTION |
|---|---|
| [no] personal-firewall *personal_firewall_software_name* detect-auto-protection {enable \| disable \| ignore} | Sets a permitted personal firewall. If you want to enter multiple personal firewalls, use this command for each of them. Use the list signature personal-firewall command to view the available personal firewall software package options.<br>detect-auto-protection: Set this to enable if the specified firewall software is not only detectable for the installation but also detectable for the activation status. You can check the settings for each firewall software by using the show eps signature personal-firewall command.<br>The user's computer must have one of the listed personal firewalls to pass this checking item. For some personal firewalls the ZyWALL / USG can also detect whether or not the firewall is activated; in those cases it must also be activated. |
| [no] application forbidden-process *process_name* | If you selected windows or linux as the operating system (using the os-type command), you can use this command to set an application that a user's computer is not permitted to have running. If you want to enter multiple applications, use this command for each of them.<br>The user's computer must not have any of the forbidden applications running to pass this checking item.<br>Include the filename extension for Linux operating systems. |
| [no] application trusted-process *process_name* | If you selected windows or linux as the operating system (using the os-type command), you can use this command to set an application that a user's computer must be running.<br>The user's computer must have all of the trusted applications running to pass this checking item.<br>Include the filename extension for Linux operating systems. |
| [no] description *description* | Type a description for this endpoint security object. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long. |
| [no] file-info file-path *file_path* | If you selected windows or linux as the operating system (using the os-type command), you can use this command to check details of specific files on the user's computer.<br>The user's computer must pass one of the file information checks to pass this checking item. |
| [no] file-info file-path *file_path* {eq \| gt \| lt \| ge \| le \| neq} file-size <1..1073741824> | Sets whether the size of the file on the user's computer has to be equal to (eq), greater than (gt), less than (lt), greater than or equal to (ge), less than or equal to (le), or not equal to (neq) the size of the file specified. |
| [no] file-info file-path *file_path* {eq \| gt \| lt \| ge \| le \| neq} file-version *file_version* | Sets whether the version of the file on the user's computer has to be equal to (eq), greater than (gt), less than (lt), greater than or equal to (ge), less than or equal to (le), or not equal to (neq) the version of the file specified. |
| [no] file-info file-path *file_path* {eq \| gt \| lt \| ge \| le \| neq} file-size <1..1073741824> {eq \| gt \| lt \| ge \| le \| neq} file-version *file_version* | Sets whether the size and version of the file on the user's computer has to be equal to (eq), greater than (gt), less than (lt), greater than or equal to (ge), less than or equal to (le), or not equal to (neq) the size and version of the file specified. |
| os-type {windows \| linux \| mac-osx \| others} | Select the type of operating system the user's computer must be using. Use the windows-version command to configure the checking items according to the set operating system. If you set this to mac-osx, there are no other checking items.<br>others allows access for computers not using Windows, Linux, or Mac OSX operating systems. For example you create Windows, Linux, and Mac OSX endpoint security objects to apply to your LAN users. An "others" policy allows access for LAN computers using Solaris, HP, Android, or other operating systems. |

**Table 179** Endpoint Security Object Commands

| COMMAND | DESCRIPTION |
|---|---|
| windows-version {windows-2000 \| windows-xp \| windows-2003 \| windows-2008 \| windows-vista \| windows-7 \| windows-2008r2} | If you set windows as the operating system (using the os-type command), use this command to set the version of Windows. |
| matching-criteria {any \| all} | Select whether the user's computer has to match just one of the endpoint security object's checking criteria or all of them. |
| list signature {anti-virus \| personal-firewall \| status} | Displays all the anti-virus software packages, personal firewall software packages or EPS signature information respectively.<br>The status command displays the EPS signature version, release date and the total number of software packages for which the ZyWALL / USG's endpoint security can check. |
| [no] windows-auto-update {enable \| disable \| ignore} | If you set windows as the operating system (using the os-type command), you can use enable with this command if the user's computer must have the Windows Auto Update feature installed and activated; use disable if the Windows Auto Update feature must be installed but deactivated; use ignore if the Windows Auto Update feature must be installed but does not matter if it is activated or not.<br>The no command does not check the Windows Auto Update feature. |
| [no] windows-service-pack <1..10> | If you set windows as the operating system (using the os-type command), you can enter the minimum Windows service pack number the user's computer must have installed. The user's computer must have this service pack or higher. For example, "2" means service pack 2. The no command means to have the ZyWALL / USG ignore the Windows service pack number. |
| [no] windows-security-patch *security_patch* | If you set windows as the operating system (using the os-type command), you can use this command to set a Windows security patch that the user's computer must have installed. If you want to enter multiple security patches, use this command for each of them.<br>The user's computer must have all of the set Windows security patches installed to pass the checking item. |
| [no] windows-registry *registry_key* {eq \| gt \| lt \| ge \| le \| neq} *registry_value* | If you set windows as the operating system (using the os-type command), you can use this command to set a Windows registry value to check on the user's computer. If you want to enter multiple registry values, use this command for each of them.<br>Set whether the value for the registry item in the user's computer has to be equal to (eq), greater than (gt), less than (lt), greater than or equal to (ge), less than or equal to (le), or not equal to (neq) the value specified.<br>The user's computer must pass all of the set Windows registry value checks to pass the checking item. |
| show eps profile [*profile_name*] | Displays the settings of all or the specified endpoint security object. |
| show eps profile *profile_name* signature {anti-virus \| personal-firewall} | Displays Anti-Virus or personal firewall signatures that have been added to the specified endpoint security object. |
| show eps signature {anti-virus \| personal-firewall \| status} | Displays all the anti-virus software packages, personal firewall software packages or EPS signature information respectively.<br>The status command displays the EPS signature version, release date and the total number of software packages for which the ZyWALL / USG's endpoint security can check. |

**Table 179** Endpoint Security Object Commands

| COMMAND | DESCRIPTION |
|---|---|
| show eps warning-message {windows-auto-update \| windows-security-patch \| anti-virus \| personal-firewall \| windows-registry \| process \| file-path} | Shows the warning messages displayed when a network client's computer fails an EPS check. |
| eps warning-message {windows-auto-update \| windows-security-patch \| anti-virus \| personal-firewall \| windows-registry \| process \| file-path} | Enters the sub-command mode for configuring the EPS warning message to show to network clients whose computers fail the related EPS check. |
| [no] enable | Enables or disables showing the related EPS warning message to network clients whose computers fail the related EPS check. |
| exit | Leaves the sub-command mode. |
| [no] message *eps_warning_message* | Specify a warning message to display when a user's computer fails the endpoint security check. Use up to 1023 characters (0-9a-zA-Z;/?:@=+$\.-_!*'()%,"). For example, "Endpoint Security anti-virus checking failed. Please contact your network administrator for help.". The no command removes the setting. |
| [no] eps rename *profile_name new_profile_name* | Changes an endpoint security object name. |

## 39.1.3 Endpoint Security Object Command Example

Peter wants to create and display an endpoint security object named EPS-Example. Only the computers that match the following criteria can access the company's SSL VPN:

- Operating system: Windows XP
- Windows auto update: enabled
- Windows service pack: 2 or above
- Personal firewall: Windows firewall installed and enabled
- Anti-Virus: Kaspersky Anti-Virus v2011 installed and enabled

However, he needs to check the Anti-Virus software name defined on the ZyWALL / USG. The following example shows how to check all available Anti-Virus software packages for which the

ZyWALL / USG's endpoint security can check. Copy and paste the name of the output item 17 for the setting later.

```
Router> configure terminal
Router(config)# show eps signature anti-virus
No.  Name                                                                    Detection
================================================================================
1    Norton_Anti-Virus_v2010                                                 no
2    Norton_Internet_Security_v2010                                          no
3    Norton_360_v3                                                           no
4    Microsoft_Security_Center                                               yes
5    TrendMicro_PC-cillin_AntiVirus_v2010                                    yes
6    TrendMicro_PC-cillin_Internet_Security_v2010                            yes
7    TrendMicro_PC-cillin_Internet_Security_Pro_v2010                        yes
8    Avira_Antivir_Personal_v2009                                            no
9    Kaspersky_Anti-Virus_v2010                                              yes
10   Kaspersky_Internet_Security_v2010                                       yes
11   Kaspersky_Anti-Virus_v2009                                              yes
12   Kaspersky_Internet_Security_v2009                                       yes
13   Norton_Anti-Virus_v2011                                                 no
14   Norton_Internet_Security_v2011                                          no
15   Norton_360_v4                                                           no
16   Norton_360_v5                                                           no
17   Kaspersky_Anti-Virus_v2011                                              yes
18   Kaspersky_Anti-Virus_v2012                                              no
19   Kaspersky_Internet_Security_v2011                                       yes
20   Kaspersky_Internet_Security_v2012                                       no
21   TrendMicro_PC-cillin_v2011_Cloud                                        yes
22   Avira_Antivir_Personal_v2010                                            no
23   Avira_Antivir_Premium_2009                                              no
24   Avira_Antivir_Premium_v10                                               no
Router(config)#
```

Then he also needs to check the personal firewall software name defined on the ZyWALL / USG. Copy and paste the name of the output item 4 for the setting later.

```
Router(config)# show eps signature personal-firewall
No.  Name                                                                    Detection
================================================================================
1    Kaspersky_Internet_Security_v2009                                       yes
2    Kaspersky_Internet_Security_v2010                                       yes
3    Microsoft_Security_Center                                               yes
4    Windows_Firewall                                                        yes
5    TrendMicro_PC-cillin_Internet_Security_v2010                            yes
6    TrendMicro_PC-cillin_Internet_Security_Pro_v2010                        yes
7    Windows_Firewall_Public                                                 yes
8    Kaspersky_Internet_Security_v2011                                       yes
9    Kaspersky_Internet_Security_v2012                                       no
Router(config)#
```

Now Peter can create the EPS object profile as the example shown next. Note that he uses the `matching-criteria all` command to make sure all users' computers have the required software installed and settings being configured before they access the company's SSL VPN.

```
Router(config)# eps profile EPS-Example
Router(eps EPS-Example)# windows-version windows-xp
Router(eps EPS-Example)# personal-firewall activate
Router(eps EPS-Example)# anti-virus activate
Router(eps EPS-Example)# windows-auto-update enable
Router(eps EPS-Example)# windows-service-pack 2
Router(eps EPS-Example)# personal-firewall Windows_Firewall detect-auto-protection
enable
Router(eps EPS-Example)# anti-virus Kaspersky_Anti-Virus_v2011 detect-auto-
protection enable
Router(eps EPS-Example)# matching-criteria all
Router(eps EPS-Example)# exit
Router(config)#
```

Then he leaves the sub-command mode and uses the `show` command to view the EPS object settings.

```
Router(eps EPS-Example)# exit
Router(config)# show eps profile
name: EPS-Example
  description:
  os type: windows
  windows version: windows-xp
  matching criteria: all
  anti-virus activation: yes
  anti-virus: 1
    name: Kaspersky_Anti-Virus_v2011
    detect auto-protection: enable
  personal firewall activation: yes
  personal firewall: 1
    name: Windows_Firewall
    detect auto-protection: enable
  windows update: enable
  windows service pack: 2
  windows security patch:
  windows registry:
  trusted application:
  forbidden application:
  file information:
  reference count: 1
Router(config)#
```

See Chapter 22 on page 187 for how to configure an SSL VPN using this EPS object .

For users who fail the endpoint security checking, Peter decides to show them an error message of "Endpoint Security checking failed. Contact helpdesk at #7777 if you have any questions." The following shows how to configure the error message.

```
Router(config)# eps failure-messages "Endpoint Security checking failed. Contact
helpdesk at #7777 if you have any questions."
Router(config)#
```

# 40

# DHCPv6 Objects

This chapter describes how to configure and view DHCPv6 request and lease objects.

## 40.1 DHCPv6 Object Commands Summary

The following table identifies the values required for many DHCPv6 object commands. Other input values are discussed with the corresponding commands.

**Table 180** DHCPv6 Object Command Input Values

| LABEL | DESCRIPTION |
|---|---|
| *dhcp6_profile* | The name of a DHCPv6 request object. Use a string of less than 31 characters. |
| *interface_name* | The name of the interface. This depends on the ZyWALL / USG model.<br>~~For the USG 300 and above~~For some models, use ge*x*, *x* = 1 ~ N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model.<br>~~For the ZyWALL USG 200 and below~~For other models, use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. |

The following sections list the DHCPv6 object commands.

### 40.1.1 DHCPv6 Object Commands

This table lists the commands for creating endpoint security objects. Use the `configure terminal` command to enter the configuration mode to be able to use the commands that configure settings.

**Table 181** DHCPv6 Object Commands

| COMMAND | DESCRIPTION |
|---|---|
| `show ipv6 dhcp6 binding` | Displays the server side IPv6/DUID binding lease. |
| `show dhcp6 interface` | Displays all DHCPv6 server, client and relay interfaces. |
| `show dhcp6-lease-object [dhcp6_profile]` | Displays the specified DHCPv6 lease object or all of them. |
| `show dhcp6 object-binding interface_name` | Displays the DHCPv6 object bound to the specified interface. |
| `show dhcp6-request-object [dhcp6_profile]` | Displays the specified DHCPv6 request object or all of them. |
| `dhcp6-lease-object dhcp6_profile address ipv6_addr duid duid` | Creates or edits the specified DHCP lease object with the specified IPv6 address and DHCP Unique IDentifier (DUID). |
| `dhcp6-lease-object dhcp6_profile prefix-delegation ipv6_addr_prefix duid duid` | Creates or edits the specified pre-fix delegation DHCP lease object with the specified IPv6 address prefix and DUID. |
| `dhcp6-lease-object dhcp6_profile address-pool ipv6_addr ipv6_addr` | Creates or edits the specified DHCP lease object address pool with the specified IPv6 address range. |

**Table 181** DHCPv6 Object Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| dhcp6-lease-object *dhcp6_profile* { sip-server \| ntp-server \| dns-server } { *ipv6_addr* \| *dhcp6_profile* } | Creates or edits the specified SIP server, NTP server, or DNS server DHCP lease object with the specified IPv6 address. When you assign a request object, the lease object value will be the request object value retrieved from the DHCPv6 server. |
| dhcp6-lease-object rename *dhcp6_profile dhcp6_profile* | Renames the specified DHCPv6 lease object to the specified name. |
| no dhcp6-lease-object *dhcp6_profile* | Deletes the specified DHCPv6 lease object. |
| dhcp6-request-object *dhcp6_profile* { dns-server \| ntp-server \| prefix-delegation \| sip-server } | Creates or edits the specified SIP server, DNS server, NTP server, prefix-delegation, or SIP server DHCP request object. |
| dhcp6-request-object rename *dhcp6_profile dhcp6_profile* | Renames the specified DHCPv6 request object to the specified name. |
| no dhcp6-request-object *dhcp6_profile* | Deletes the specified DHCPv6 request object. |

## 40.1.2 DHCPv6 Object Command Examples

This example creates and displays a DHCPv6 lease object named “test1” for IPv6 address 2003::1 with DUID 00:01:02:03:04:05:06:07.

```
Router(config)# dhcp6-lease-object test1 address 2003::1 duid
00:01:02:03:04:05:06:07
Router(config)# show dhcp6 lease-object
DHCP6 Lease Object: test1
  Object Type: address
  Object Value: 2003::1
  DUID: 00:01:02:03:04:05:06:07
  Bind Iface:
  REFERENCE: 0
```

This example makes “test1” into a DHCPv6 address pool lease object for IPv6 addresses 2004::10 to 2004::40.

```
Router(config)# dhcp6-lease-object test1 address-pool 2004::10 2004::40
Router(config)# show dhcp6 lease-object
DHCP6 Lease Object: test1
  Object Type: address-pool
  Object Value: 2004::10
  Ext Object Value: 2004::40
  Bind Iface:
  REFERENCE: 0
```

This example creates and displays a DHCPv6 pre-fix delegation lease object named “pfx” for IPv6 address prefix 2005::/64 and DUID 00:01:02:03:04:05:06:07, then renames it to “pd”.

```
Router(config)# dhcp6-lease-object pfx prefix-delegation 2005::/64 duid
00:01:02:03:04:05:06:07
Router(config)# show dhcp6 lease-object pfx
DHCP6 Lease Object: pfx
  Object Type: prefix-delegation
  Object Value: 2005::/64
  DUID: 00:01:02:03:04:05:06:07
  Bind Iface:
  REFERENCE: 0
Router(config)# dhcp6-lease-object rename pfx pd
Router(config)# show dhcp6 lease-object pd
DHCP6 Lease Object: pd
  Object Type: prefix-delegation
  Object Value: 2005::/64
  DUID: 00:01:02:03:04:05:06:07
  Bind Iface:
  REFERENCE: 0
```

This example deletes the “test1” DHCPv6 lease object.

```
Router(config)# no dhcp6-lease-object test1
```

This example creates a DHCPv6 pre-fix delegation request object named “pfx” and displays its settings.

```
Router(config)# dhcp6-request-object pfx prefix-delegation
Router(config)# show dhcp6 request-object
DHCP6 Request Object: pfx
  Object Type: prefix-delegation
  Object Value: 2089:3::/48
  Bind Iface: ge2
  REFERENCE: 1
```

# 41

# System

This chapter provides information on the commands that correspond to what you can configure in the system screens.

## 41.1 System Overview

Use these commands to configure general ZyWALL / USG information, the system time and the console port connection speed for a terminal emulation program. They also allow you to configure DNS settings and determine which services/protocols can access which ZyWALL / USG zones (if any) from which computers.

## 41.2 Customizing the WWW Login Page

Use these commands to customize the Web Configurator login screen. You can also customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet. See Chapter 30 on page 265 for more on access user accounts.

The following figures identify the parts you can customize in the login and access pages.

**Figure 26** Login Page Customization

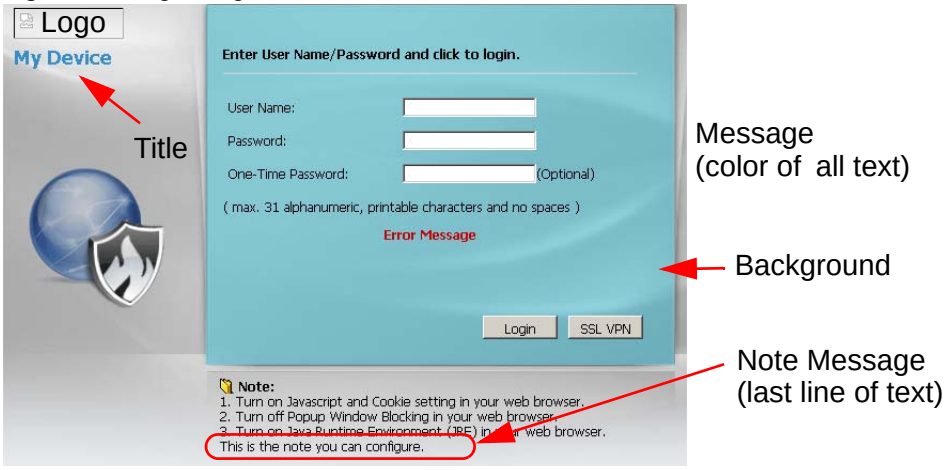
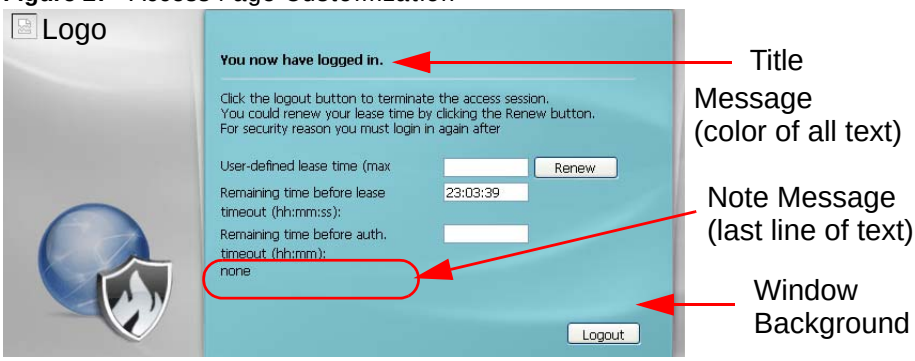


**Figure 27** Access Page Customization




You can specify colors in one of the following ways:

- *color-rgb*: Enter red, green, and blue values in parenthesis and separate by commas. For example, use “rgb(0,0,0)” for black.
- *color-name*: Enter the name of the desired color.
- *color-number*: Enter a pound sign (#) followed by the six-digit hexadecimal number that represents the desired color. For example, use “#000000” for black.

The following table describes the commands available for customizing the Web Configurator login screen and the page that displays after an access user logs into the Web Configurator to access network services like the Internet. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 182** Command Summary: Customization

| COMMAND | DESCRIPTION |
|---|---|
| `[no] access-page color-window-background` | Sets whether or not the access page uses a colored background. |
| `access-page message-color {`*color-rgb* `|` *color-name* `|` *color-number*`}` | Sets the color of the message text on the access page. |
| `[no] access-page message-text` *message* | Sets a note to display below the access page’s title. Use up to 64 printable ASCII characters. Spaces are allowed. |
| `access-page title` *title* | Sets the title for the top of the access page. Use up to 64 printable ASCII characters. Spaces are allowed. |
| `access-page window-color {`*color-rgb* `|` *color-name* `|` *color-number*`}` | Sets the color of the access page’s colored background. |
| `login-page background-color {`*color-rgb* `|` *color-name* `|` *color-number*`}` | Sets the color of the login page’s background. |
| `[no] login-page color-background` | Sets the login page to use a solid colored background. |
| `[no] login-page color-window-background` | Sets the login page’s window to use a solid colored background. |
| `login-page message-color {`*color-rgb* `|` *color-name* `|` *color-number*`}` | Sets the color of the message text on the login page. |
| `[no] login-page message-text %` *message* | Sets a note to display at the bottom of the login screen. Use up to 64 printable ASCII characters. Spaces are allowed. |
| `login-page title` *title* | Sets the title for the top of the login screen. Use up to 64 printable ASCII characters. Spaces are allowed. |
| `login-page title-color {`*color-rgb* `|` *color-name* `|` *color-number*`}` | Sets the title text color of the login page. |

**Table 182** Command Summary: Customization (continued)

| COMMAND | DESCRIPTION |
|---|---|
| `login-page window-color {color-rgb \| color-name \| color-number}` | Sets the color of the login page's window border. |
| `logo background-color {color-rgb \| color-name \| color-number}` | Sets the color of the logo banner across the top of the login screen and access page. |
| `show access-page settings` | Lists the current access page settings. |
| `show login-page default-title` | Lists the factory default title for the login page. |
| `show login-page settings` | Lists the current login page settings. |
| `show logo settings` | Lists the current logo background (banner) and floor (line below the banner) settings. |
| `show page-customization` | Lists whether the ZyWALL / USG is set to use custom login and access pages or the default ones. |

# 41.3 Host Name Commands

The following table describes the commands available for the hostname and domain name. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 183** Command Summary: Host Name

| COMMAND | DESCRIPTION |
|---|---|
| `[no] domainname domain_name` | Sets the domain name. The `no` command removes the domain name.<br>*domain_name*: This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. |
| `[no] hostname hostname` | Sets a descriptive name to identify your ZyWALL / USG. The `no` command removes the host name. |
| `show fqdn` | Displays the fully qualified domain name. |

# 41.4 Time and Date

For effective scheduling and logging, the ZyWALL / USG system time must be accurate. The ZyWALL / USG's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server.

### 41.4.1 Date/Time Commands

The following table describes the commands available for date and time setup. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 184** Command Summary: Date/Time

| COMMAND | DESCRIPTION |
|---|---|
| `clock date yyyy-mm-dd time hh:mm:ss` | Sets the new date in year, month and day format manually and the new time in hour, minute and second format. |
| `[no] clock daylight-saving` | Enables daylight saving. The `no` command disables daylight saving. |
| `[no] clock saving-interval begin {apr\|aug\|dec\|feb\|jan\|jul\|jun\|mar\|may\|nov\|oct\|sep} {1\|2\|3\|4\|last} {fri\|mon\|sat\|sun\|thu\|tue\|wed} hh:mm end {apr\|aug\|dec\|feb\|jan\|jul\|jun\|mar\|may\|nov\|oct\|sep} {1\|2\|3\|4\|last} {fri\|mon\|sat\|sun\|thu\|tue\|wed} hh:mm offset` | Configures the day and time when Daylight Saving Time starts and ends. The `no` command removes the day and time when Daylight Saving Time starts and ends.<br>offset: a number from 1 to 5.5 (by 0.5 increments) |
| `clock time hh:mm:ss` | Sets the new time in hour, minute and second format. |
| `[no] clock time-zone {-\|+hh}` | Sets your time zone. The `no` command removes time zone settings. |
| `[no] ntp` | Saves your date and time and time zone settings and updates the data and time every 24 hours. The `no` command stops updating the data and time every 24 hours. |
| `[no] ntp server {fqdn\|w.x.y.z}` | Sets the IP address or URL of your NTP time server. The `no` command removes time server information. |
| `ntp sync` | Gets the time and date from a NTP time server. |
| `show clock date` | Displays the current date of your ZyWALL / USG. |
| `show clock status` | Displays your time zone and daylight saving settings. |
| `show clock time` | Displays the current time of your ZyWALL / USG. |
| `show ntp server` | Displays time server settings. |

## 41.5 Console Port Speed

This section shows you how to set the console port speed when you connect to the ~~ZyWALL~~ZyWALL / USG via the console port using a terminal emulation program. The following table describes the console port commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 185** Command Summary: Console Port Speed

| COMMAND | DESCRIPTION |
|---|---|
| `[no] console baud baud_rate` | Sets the speed of the console port. The no command resets the console port speed to the default (115200).<br>`baud_rate`: 9600, 19200, 38400, 57600 or 115200. |
| `show console` | Displays console port speed. |

# 41.6 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

## 41.6.1 Domain Zone Forwarder

A domain zone forwarder contains a DNS server's IP address. The ZyWALL / USG can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

## 41.6.2 DNS Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 186** Input Values for General DNS Commands

| LABEL | DESCRIPTION |
|---|---|
| *address_object* | The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *interface_name* | The name of the interface.<br>Ethernet interface: For the ZyWALL / USG USG 300 and above, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model.<br>The ZyWALL / USG USG 200 and lower models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.<br>virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4<br>VLAN interface: vlan*x*, *x* = 0 - 4094<br>virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 12<br>bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ZyWALL / USG model supports.<br>virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4<br>PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL / USG model supports. |

The following table describes the commands available for DNS. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 187** Command Summary: DNS

| COMMAND | DESCRIPTION |
|---|---|
| `[no] ip dns server a-record` *`fqdn w.x.y.z`* | Sets an A record that specifies the mapping of a fully qualified domain name (FQDN) to an IP address. The `no` command deletes an A record. |
| `ip dns server cache-flush` | Clears the DNS. |

**Table 187** Command Summary: DNS (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] ip dns server mx-record *domain_name* {*w.x.y.z*\|*fqdn*} | Sets a MX record that specifies a mail server that is responsible for handling the mail for a particular domain. The no command deletes a MX record. |
| ip dns server rule {<1..32>\|append\|insert <1..32>} access-group {ALL\|*address_object*} zone {ALL\|*address_object*} action {accept\|deny} | Sets a service control rule for DNS requests. |
| ip dns server rule move <1..32> to <1..32> | Changes the number of a service control rule. |
| [no] ip dns server zone-forwarder {<1..32>\|append\|insert <1..32>} {*domain_zone_name*\|*} interface *interface_name* | Sets a domain zone forwarder record that specifies a fully qualified domain name. You can also use a star (*) if all domain zones are served by the specified DNS server(s).<br>*domain_zone_name*: This is a domain zone, not a host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the ZyWALL / USG receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address.<br>*interface_name*: This is the interface through which the ISP provides a DNS server. The interface should be activated and set to be a DHCP client.<br>The no command deletes a zone forwarder record. |
| ip dns server zone-forwarder {<1..32>\|append\|insert <1..32>} {*domain_zone_name*\|*} user-defined *w.x.y.z* [private \| interface {*interface_name* \| auto}] | Sets a domain zone forwarder record that specifies a DNS server's IP address.<br>private \| interface: Use private if the ZyWALL / USG connects to the DNS server through a VPN tunnel. Otherwise, use the interface command to set the interface through which the ZyWALL / USG sends DNS queries to a DNS server. The auto means any interface that the ZyWALL / USG uses to send DNS queries to a DNS server according to the routing rule. |
| ip dns server zone-forwarder move <1..32> to <1..32> | Changes the index number of a zone forwarder record. |
| no ip dns server rule <1..32> | Deletes a service control rule. |
| show ip dns server | Displays all DNS entries. |
| show ip dns server database | Displays all configured records. |
| show ip dns server status | Displays whether this service is enabled or not. |

## 41.6.3 DNS Command Example

This command sets an A record that specifies the mapping of a fully qualified domain name (www.abc.com) to an IP address (210.17.2.13).

```
Router# configure terminal
Router(config)# ip dns server a-record www.abc.com 210.17.2.13
```

# 42

# System Remote Management

This chapter shows you how to determine which services/protocols can access which ZyWALL / USG zones (if any) from which computers.

Note: To access the ZyWALL / USG from a specified computer using a service, make sure no service control rules or to-ZyWALL / USG firewall rules block that traffic.

## 42.1 Remote Management Overview

You may manage your ZyWALL / USG from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (LAN&WAN&DMZ)
- DMZ only

To disable remote management of a service, deselect **Enable** in the corresponding service screen.

### 42.1.1 Remote Management Limitations

Remote management will not work when:

1. You have disabled that service in the corresponding screen.
2. The accepted IP address in the **Service Control** table does not match the client IP address. If it does not match, the ZyWALL / USG will disconnect the session immediately.
3. There is a firewall rule that blocks it.

### 42.1.2 System Timeout

There is a lease timeout for administrators. The ZyWALL / USG automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the ZyWALL / USG for authentication again when the reauthentication time expires.

# 42.2 Common System Command Input Values

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 188** Input Values for General System Commands

| LABEL | DESCRIPTION |
|---|---|
| *address_object* | The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| *rule_number* | The number of a service control rule. 1 - *X* where *X* is the highest number of rules the ZyWALL / USG model supports. |
| *zone_object* | The name of the zone. For the ZyWALL / USG USG 300 and above, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.<br><br>The ZyWALL / USG USG 200 and lower models use pre-defined zone names like DMZ, LAN1, SSL VPN, WLAN, IPSec VPN, OPT, and WAN. |

# 42.3 HTTP/HTTPS Commands

The following table describes the commands available for HTTP/HTTPS. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 189** Command Summary: HTTP/HTTPS

| COMMAND | DESCRIPTION |
|---|---|
| `[no] ip http authentication` *auth_method* | Sets an authentication method used by the HTTP/HTTPS server. The `no` command resets the authentication method used by the HTTP/HTTPS server to the factory default (`default`).<br><br>*auth_method*: The name of the authentication method. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| `[no] ip http port <1..65535>` | Sets the HTTP service port number. The `no` command resets the HTTP service port number to the factory default (80). |
| `[no] ip http secure-port <1..65535>` | Sets the HTTPS service port number. The `no` command resets the HTTPS service port number to the factory default (443). |
| `[no] ip http secure-server` | Enables HTTPS access to the ZyWALL / USG web configurator. The `no` command disables HTTPS access to the ZyWALL / USG web configurator. |
| `[no] ip http secure-server auth-client` | Sets the client to authenticate itself to the HTTPS server. The `no` command sets the client not to authenticate itself to the HTTPS server. |

**Table 189** Command Summary: HTTP/HTTPS (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] ip http secure-server cert *certificate_name* | Specifies a certificate used by the HTTPS server. The no command resets the certificate used by the HTTPS server to the factory default (default).<br>*certificate_name*: The name of the certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters. |
| [no] ip http secure-server force-redirect | Redirects all HTTP connection requests to a HTTPS URL. The no command disables forwarding HTTP connection requests to a HTTPS URL. |
| ip http secure-server table {admin\|user} rule {*rule_number*\|append\|insert *rule_number*} access-group {ALL\|*address_object*} zone {ALL\|*zone_object*} action {accept\|deny} | Sets a service control rule for HTTPS service. |
| ip http secure-server table {admin\|user} rule move *rule_number* to *rule_number* | Changes the index number of a HTTPS service control rule. |
| ip http secure-server cipher-suite {*cipher_algorithm*} [*cipher_algorithm*] [*cipher_algorithm*] [*cipher_algorithm*] | Sets the encryption algorithms (up to four) that the ZyWALL / USG uses for the SSL in HTTPS connections and the sequence in which it uses them. The *cipher_algorithm* can be any of the following.<br>rc4: RC4 (RC4 may impact the ZyWALL / USG's CPU performance since the ZyWALL / USG's encryption accelerator does not support it).<br>aes: AES<br>des: DES<br>3des: Triple DES. |
| no ip http secure-server cipher-suite {*cipher_algorithm*} | Has the ZyWALL / USG not use the specified encryption algorithm for the SSL in HTTPS connections. |
| [no] ip http server | Allows HTTP access to the ZyWALL / USG web configurator. The no command disables HTTP access to the ZyWALL / USG web configurator. |
| ip http server table {admin\|user} rule {*rule_number*\|append\|insert *rule_number*} access-group {ALL\|*address_object*} zone {ALL\|*zone_object*} action {accept\|deny} | Sets a service control rule for HTTP service. |
| ip http server table {admin\|user} rule move *rule_number* to *rule_number* | Changes the number of a HTTP service control rule. |
| no ip http secure-server table {admin\|user} rule *rule_number* | Deletes a service control rule for HTTPS service. |
| no ip http server table {admin\|user} rule *rule_number* | Deletes a service control rule for HTTP service. |
| show ip http server status | Displays HTTP settings. |
| show ip http server secure status | Displays HTTPS settings. |

### 42.3.1 HTTP/HTTPS Command Examples

This following example adds a service control rule that allowed an administrator from the computers with the IP addresses matching the Marketing address object to access the WAN zone using HTTP service.

```
Router# configure terminal
Router(config)# ip http server table admin rule append access-group Marketing zone WAN
action accept
```

This command sets an authentication method used by the HTTP/HTTPS server to authenticate the client(s).

```
Router# configure terminal
Router(config)# ip http authentication Example
```

This following example sets a certificate named MyCert used by the HTTPS server to authenticate itself to the SSL client.

```
Router# configure terminal
Router(config)# ip http secure-server cert MyCert
```

## 42.4 SSH

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

### 42.4.1 SSH Implementation on the ZyWALL / USG

Your ZyWALL / USG supports SSH versions 1 and 2 using RSA authentication and four encryption methods (AES, 3DES, Archfour, and Blowfish). The SSH server is implemented on the ZyWALL / USG for remote management on port 22 (by default).

### 42.4.2 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ZyWALL / USG over SSH.

## 42.4.3 SSH Commands

The following table describes the commands available for SSH. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 190** Command Summary: SSH

| COMMAND | DESCRIPTION |
|---|---|
| `[no] ip ssh server` | Allows SSH access to the ZyWALL / USG CLI. The `no` command disables SSH access to the ZyWALL / USG CLI. |
| `[no] ip ssh server cert` *certificate_name* | Sets a certificate whose corresponding private key is to be used to identify the ZyWALL / USG for SSH connections. The `no` command resets the certificate used by the SSH server to the factory default (`default`).<br>*certificate_name*: The name of the certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters. |
| `[no] ip ssh server port <1..65535>` | Sets the SSH service port number. The `no` command resets the SSH service port number to the factory default (22). |
| `ip ssh server rule {`*rule_number*`|append|insert` *rule_number*`} access-group {ALL|`*address_object*`} zone {ALL|`*zone_object*`} action {accept|deny}` | Sets a service control rule for SSH service.<br>*address_object*: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.<br>*zone_object*: The name of the zone. For the ZyWALL / USG USG 300 and above, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.<br>The ZyWALL / USG USG 200 and lower models use pre-defined zone names like DMZ, LAN1, SSL VPN, WLAN, IPSec VPN, OPT, and WAN. |
| `ip ssh server rule move` *rule_number* `to` *rule_number* | Changes the index number of a SSH service control rule. |
| `[no] ip ssh server v1` | Enables remote management using SSH v1. The `no` command stops the ZyWALL / USG from using SSH v1. |
| `no ip ssh server rule` *rule_number* | Deletes a service control rule for SSH service. |
| `show ip ssh server status` | Displays SSH settings. |

## 42.4.4 SSH Command Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using SSH service.

```
Router# configure terminal
Router(config)# ip ssh server rule 2 access-group Marketing zone WAN action accept
```

This command sets a certificate (Default) to be used to identify the ZyWALL / USG.

```
Router# configure terminal
Router(config)# ip ssh server cert Default
```

# 42.5 Telnet

You can configure your ZyWALL / USG for remote Telnet access.

# 42.6 Telnet Commands

The following table describes the commands available for Telnet. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 191** Command Summary: Telnet

| COMMAND | DESCRIPTION |
|---|---|
| `[no] ip telnet server` | Allows Telnet access to the ZyWALL / USG CLI. The `no` command disables Telnet access to the ZyWALL / USG CLI. |
| `[no] ip telnet server port <1..65535>` | Sets the Telnet service port number. The `no` command resets the Telnet service port number back to the factory default (23). |
| `ip telnet server rule {`*`rule_number`*`\|append\|insert` *`rule_number`*`} access-group {ALL\|`*`address_object`*`} zone {ALL\|`*`zone_object`*`} action {accept\|deny}` | Sets a service control rule for Telnet service.<br>*address_object*: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.<br>*zone_object*: The name of the zone. For the ZyWALL / USG USG 300 and above, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.<br>The ZyWALL / USG USG 200 and lower models use pre-defined zone names like DMZ, LAN1, SSL VPN, WLAN, IPSec VPN, OPT, and WAN. |
| `ip telnet server rule move` *`rule_number`* `to` *`rule_number`* | Changes the index number of a service control rule. |
| `no ip telnet server rule` *`rule_number`* | Deletes a service control rule for Telnet service. |
| `show ip telnet server status` | Displays Telnet settings. |

## 42.6.1 Telnet Commands Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using Telnet service.

```
Router# configure terminal
Router(config)# ip telnet server rule 11 access-group RD zone LAN action
-> accept
```

This command displays Telnet settings.

```
Router# configure terminal
Router(config)# show ip telnet server status
active     : yes
port       : 23
service control:
No.  Zone                        Address                     Action
============================================================================
Router(config)#
```

# 42.7 Configuring FTP

You can upload and download the ZyWALL / USG's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

## 42.7.1 FTP Commands

The following table describes the commands available for FTP. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 192** Command Summary: FTP

| COMMAND | DESCRIPTION |
|---|---|
| `[no] ip ftp server` | Allows FTP access to the ZyWALL / USG. The `no` command disables FTP access to the ZyWALL / USG. |
| `[no] ip ftp server cert` *certificate_name* | Sets a certificate to be used to identify the ZyWALL / USG. The `no` command resets the certificate used by the FTP server to the factory default. |
| `[no] ip ftp server port <1..65535>` | Sets the FTP service port number. The `no` command resets the FTP service port number to the factory default (21). |
| `[no] ip ftp server tls-required` | Allows FTP access over TLS. The `no` command disables FTP access over TLS. |
| `ip ftp server rule` {*rule_number*\|`append`\|`insert` *rule_number*} `access-group` {`ALL`\|*address_object*} `zone` {`ALL`\|*zone_object*} `action` {`accept`\|`deny`} | Sets a service control rule for FTP service.<br>*address_object*: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.<br>*zone_object*: The name of the zone. For the ZyWALL / USG USG 300 and above, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.<br>The ZyWALL / USG USG 200 and lower models use pre-defined zone names like DMZ, LAN1, SSL VPN, WLAN, IPSec VPN, OPT, and WAN. |
| `ip ftp server rule move` *rule_number* `to` *rule_number* | Changes the index number of a service control rule. |
| `no ip ftp server rule` *rule_number* | Deletes a service control rule for FTP service. |
| `show ip ftp server status` | Displays FTP settings. |

### 42.7.2 FTP Commands Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using FTP service.

```
Router# configure terminal
Router(config)# ip ftp server rule 4 access-group Sales zone WAN action accept
```

This command displays FTP settings.

```
Router# configure terminal
Router(config)# show ip ftp server status
active     : yes
port       : 21
certificate: default
TLS        : no
service control:
No.  Zone                     Address                     Action
=========================================================================
```

## 42.8 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your ZyWALL / USG supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL / USG through the network. The ZyWALL / USG supports SNMP version one (SNMPv1) and version two (SNMPv2c).

### 42.8.1 Supported MIBs

The ZyWALL / USG supports MIB II that is defined in RFC-1213 and RFC-1215. The ZyWALL / USG also supports private MIBs (zywall.mib and zyxel-zywall-ZLD-Common.mib) to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the ZyWALL / USG's MIBs from www.zyxel.com.

### 42.8.2 SNMP Traps

The ZyWALL / USG will send traps to the SNMP manager when any one of the following events occurs:

**Table 193** SNMP Traps

| OBJECT LABEL | OBJECT ID | DESCRIPTION |
|---|---|---|
| Cold Start | 1.3.6.1.6.3.1.1.5.1 | This trap is sent when the ZyWALL / USG is turned on or an agent restarts. |
| linkDown | 1.3.6.1.6.3.1.1.5.3 | This trap is sent when the Ethernet link is down. |

**Table 193** SNMP Traps (continued)

| OBJECT LABEL | OBJECT ID | DESCRIPTION |
|---|---|---|
| linkUp | 1.3.6.1.6.3.1.1.5.4 | This trap is sent when the Ethernet link is up. |
| authenticationFailure | 1.3.6.1.6.3.1.1.5.5 | This trap is sent when an SNMP request comes from non-authenticated hosts. |

## 42.8.3 SNMP Commands

The following table describes the commands available for SNMP. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 194** Command Summary: SNMP

| COMMAND | DESCRIPTION |
|---|---|
| `[no] snmp-server` | Allows SNMP access to the ZyWALL / USG. The `no` command disables SNMP access to the ZyWALL / USG. |
| `[no] snmp-server community` *`community_string`* `{ro\|rw}` | Enters up to 64 characters to set the password for read-only (ro) or read-write (rw) access. The `no` command resets the password for read-only (`ro`) or read-write (`rw`) access to the default. |
| `[no] snmp-server contact` *`description`* | Sets the contact information (of up to 60 characters) for the person in charge of the ZyWALL / USG. The `no` command removes the contact information for the person in charge of the ZyWALL / USG. |
| `[no] snmp-server enable {informs\|traps}` | Enables all SNMP notifications (informs or traps). The `no` command disables all SNMP notifications (informs or traps). |
| `[no] snmp-server host {`*`w.x.y.z`*`}` [*`community_string`*] | Sets the IPv4 or IPv6 address of the host that receives the SNMP notifications. The `no` command removes the host that receives the SNMP notifications. |
| `[no] snmp-server location` *`description`* | Sets the geographic location (of up to 60 characters) for the ZyWALL / USG. The `no` command removes the geographic location for the ZyWALL / USG. |
| `[no] snmp-server port <1..65535>` | Sets the SNMP service port number. The `no` command resets the SNMP service port number to the factory default (`161`). |
| `snmp-server rule {`*`rule_number`*`\|append\|insert` *`rule_number`*`} access-group {ALL\|`*`address_object`*`} zone {ALL\|`*`zone_object`*`} action {accept\|deny}` | Sets a service control rule for SNMP service.<br>*`address_object`*: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.<br>*`zone_object`*: The name of the zone. For the ZyWALL / USG USG 300 and above, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.<br>The ZyWALL / USG USG 200 and lower models use pre-defined zone names like DMZ, LAN1, SSL VPN, WLAN, IPSec VPN, OPT, and WAN. |
| `snmp-server rule move` *`rule_number`* `to` *`rule_number`* | Changes the index number of a service control rule. |
| `no snmp-server rule` *`rule_number`* | Deletes a service control rule for SNMP service. |
| `show snmp status` | Displays SNMP Settings. |

### 42.8.4 SNMP Commands Examples

The following command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using SNMP service.

```
Router# configure terminal
Router(config)# snmp-server rule 11 access-group Example zone WAN action accept
```

The following command sets the password (secret) for read-write (`rw`) access.

```
Router# configure terminal
Router(config)# snmp-server community secret rw
```

The following command sets the IP address of the host that receives the SNMP notifications to 172.23.15.84 and the password (sent with each trap) to qwerty.

```
Router# configure terminal
Router(config)# snmp-server host 172.23.15.84 qwerty
```

## 42.9 ICMP Filter

The `ip icmp-filter` commands are obsolete. See Chapter 19 on page 159 to configure firewall rules for ICMP traffic going to the ZyWALL / USG to discard or reject ICMP packets destined for the ZyWALL / USG.

Configure the ICMP filter to help keep the ZyWALL / USG hidden from probing attempts. You can specify whether or not the ZyWALL / USG is to respond to probing for unused ports.

You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 195** Command Summary: ICMP Filter

| COMMAND | DESCRIPTION |
|---|---|
| `[no] ip icmp-filter activate` | Turns the ICMP filter on or off. |
| `ip icmp-filter rule {<1..32>\|append\|insert <1..32>} access-group {ALL\|ADDRESS_OBJECT} zone {ALL\|ZONE_OBJECT} icmp-type {ALL \|echo-reply \|destination-unreachable \|source-quench\|redirect\|echo-request\| router-advertisement\|router-solicitation \|time-exceeded \| parameter-problem\| timestamp-request\|timestamp-reply\| address-mask-request\| address-mask-reply} action {accept\|deny}` | Sets an ICMP filter rule.<br>ADDRESS_OBJECT: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.<br>ZONE_OBJECT: The name of the zone. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| `no ip icmp-filter rule <1..64>` | Deletes an ICMP filter rule. |
| `ip icmp-filter rule move <1..64> to <1..64>` | Changes the index number of an ICMP filter rule. |
| `show ip icmp-filter status` | Displays ICMP filter settings. |

# 42.10 Dial-in Management

Connect an external serial modem to the **DIAL BACKUP** port (or **AUX** port depending on your model) to provide a remote management connection in case the ZyWALL / USG's other WAN connections are down. This is like an auxiliary interface, except it is used for management connections coming into the ZyWALL / USG instead of as a backup WAN connection.

## 42.10.1 AT Command Strings

For regular telephone lines, the default Dial string tells the modem that the line uses tone dialing. `ATDT` is the command for a switch that requires tone dialing. If your switch requires pulse dialing, change the string to `ATDP`.

## 42.10.2 DTR Signal

The majority of WAN devices default to hanging up the current call when the DTR (Data Terminal Ready) signal is dropped by the DTE. When the Drop DTR When Hang Up check box is selected, the ZyWALL / USG uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command `ATH`.

## 42.10.3 Response Strings

The response strings tell the ZyWALL / USG the tags, or labels, immediately preceding the various call parameters sent from the serial modem. The response strings have not been standardized; please consult the documentation of your serial modem to find the correct tags.

## 42.10.4 Dial-in Management Commands

The following table describes the commands available for dial-in management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 196** Command Summary: Dial-in Management

| COMMAND | DESCRIPTION |
|---|---|
| `dial-in` | Enters sub-command mode. |
| `[no] activate` | Turns dial-in management on. The `no` command turns it off. |
| `[no] answer-rings` | Sets how many times the ZyWALL / USG lets the incoming dial-in management session ring before processing it. The `no` command sets it to one. |
| `[no] description` *description* | Specifies the description for the dial-in management connection. The `no` command clears the description.<br>*description*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long. |
| `[no] initial-string` *initial_string* | Specifies the initial string of the auxiliary interface. The `no` command removes the initial string.<br>*initial_string*: You can use up to 64 characters. Semicolons (;) and backslashes (\) are not allowed. |
| `[no] mute` | Stops the external serial modem from making audible sounds during a dial-in management session. The `no` command turns the sounds back on. |

**Table 196** Command Summary: Dial-in Management

| COMMAND | DESCRIPTION |
|---|---|
| [no] port-speed {9600 \| 19200 \| 38400 \| 57600 \| 115200} | Specifies the baud rate of the auxiliary interface. The no command sets the baud rate to 115200. |
| show dial-in | Displays dial-in management settings. |

### 42.10.4.1 Dial-in Management Command Examples

The following commands show you how to set up dial-in management with the following parameters: active, port speed 57600, initial-string ATDT, and description “I am dial-in management”.

```
Router# configure terminal
Router(config)# dial-in
Router(config-dial-in)# activate
Router(config-dial-in)# port-speed 57600
Router(config-dial-in)# initial-string ATDT
Router(config-dial-in)# description I am dial-in management
Router(config-dial-in)# exit
```

# 42.11 Vantage CNM

Vantage CNM (Centralized Network Management) is a browser-based global management solution that allows an administrator from any location to easily configure, manage, monitor and troubleshoot ZyXEL devices located worldwide. See the Vantage CNM User's Guide for details.

If you allow your ZyWALL / USG to be managed by the Vantage CNM server, then you should not do any configurations directly to the ZyWALL / USG (using either the web configurator or commands) without notifying the Vantage CNM administrator.

## 42.11.1 Vantage CNM Commands

The following table describes the commands available for dial-in management. You must use the configure terminal command to enter the configuration mode before you can use these commands.

**Table 197** Command Summary: Vantage CNM

| COMMAND | DESCRIPTION |
|---|---|
| [no] cnm-agent manager *url* | Sets up the URL of the Vantage server that the ZyWALL / USG registers with. Include the full HTTPS or HTTP URL. For example, https://1.2.3.4/vantage/TR069. |
| [no] cnm-agent activate | Turns management through Vantage CNM on or off. |
| cnm-agent keepalive interval <10..90> | Sets the keepalive interval. |
| [no] cnm-agent periodic-inform activate | Turns the periodic inform on or off. |
| cnm-agent periodic-inform interval <10..86400> | Sets the periodic inform interval. |
| cnm-agent trigger-inform [interval] | initiates a TR069 connection to the server. You can also specify the interval for the inform messages. |

**Table 197** Command Summary: Vantage CNM

| COMMAND | DESCRIPTION |
|---|---|
| [no] cnm-agent auth activate | Enables or disables authentication of the server when using HTTPS. |
| show cnm-agent configuration | Displays the Vantage CNM configuration. |
| [no] cnm-agent acs username <username for ACS connection request> | Configure the username of the ACS (Auto-Configuration Server) connection request for the ZyWALL / USG to authenticate the server using HTTP digest authentication.<br>No removes the username of the ACS connection request. |
| [no] cnm-agent acs password <password for ACS connection request> | Configure the password of the ACS (Auto-Configuration Server) connection request for the ZyWALL / USG to authenticate the server using HTTP digest authentication.<br>No removes the password of the ACS connection request. |
| [no] cnm-agent username <TR-069 username> | Configure the username of the ZyWALL / USGfor the ACS server to authenticate the ZyWALL / USG using HTTP digest authentication.<br>No removes the password of the ACS server authentication request. |
| [no] cnm-agent password <TR-069 password> | Configure the password of the ZyWALL / USG for the ACS server to authenticate the ZyWALL / USG using HTTP digest authentication.<br>No removes the password of the ACS server authentication request. |
| cnm-agent server-type {vantage \| tr069} | Configure the server type of the management server as either a Vantage CNM server or a TR069 ACS server. |

### 42.11.1.1 Vantage CNM Command Examples

The following example turns on Vantage CNM management and sets the ZyWALL / USG to register with a server at https://1.2.3.4/vantage/TR069.

```
Router# configure terminal
Router(config)# cnm-agent activate
Router(config)# cnm-agent manager https://1.2.3.4/vantage/TR069
Router(config)# show cnm-agent configuration
Activate: YES
ACS URL: https://1.2.3.4/vantage/TR069
Keepalive: ENABLE
Keepalive Interval: 60
Periodic Inform: DISABLE
Periodic Inform Interval: 3600
Custom IP: NO
HTTPS Authentication: NO
Vantage Certificate: zw1050.cer456
```

# 42.12 Language Commands

Use the `language` commands to display what language the web configurator is using or change it. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 198** Command Summary: Language

| COMMAND | DESCRIPTION |
|---|---|
| `language <English \| Simplified_Chinese \| Traditional_Chinese>` | Specifies the language used in the web configurator screens. |
| `show language {setting \| all}` | `setting` displays the current display language in the web configurator screens.<br>`all` displays the available languages. |

# 42.13 IPv6 Commands

Use the `ipv6` commands to enable or disable IPv6 support. You must use the `configure terminal` command to enter the configuration mode before you can use the commands that configure settings.

**Table 199** Command Summary: IPv6

| COMMAND | DESCRIPTION |
|---|---|
| `[no] ipv6 activate` | Enables or disables IPv6 support. |
| `show ipv6 status` | Displays whether IPv6 support is enabled or disabled. |

# 43

# File Manager

This chapter covers how to work with the ZyWALL / USG's firmware, certificates, configuration files, custom IDP signatures, packet trace results, shell scripts and temporary files.

## 43.1 File Directories

The ZyWALL / USG stores files in the following directories.

**Table 200** FTP File Transfer Notes

| DIRECTORY | FILE TYPE | FILE NAME EXTENSION |
|---|---|---|
| A | Firmware (upload only) | bin |
| cert | Non-PKCS#12 certificates | cer |
| conf | Configuration files | conf |
| idp | IDP custom signatures | rules |
| packet_trace | Packet trace results (download only) | |
| script | Shell scripts | .zysh |
| tmp | Temporary system maintenance files and crash dumps for technical support use (download only) | |

A. After you log in through FTP, you do not need to change directories in order to upload the firmware.

## 43.2 Configuration Files and Shell Scripts Overview

You can store multiple configuration files and shell script files on the ZyWALL / USG.

When you apply a configuration file, the ZyWALL / USG uses the factory default settings for any features that the configuration file does not include. Shell scripts are files of commands that you can store on the ZyWALL / USG and run when you need them. When you run a shell script, the ZyWALL / USG only applies the commands that it contains. Other settings do not change.

You can edit configuration files or shell scripts in a text editor and upload them to the ZyWALL / USG. Configuration files use a .conf extension and shell scripts use a .zysh extension.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

**Figure 28** Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
# configure ge3
interface ge3
ip address 172.23.37.240 255.255.255.0
ip gateway 172.23.37.254 metric 1
exit
# create address objects for remote management / to-ZyWALL firewall rules
# use the address group in case we want to open up remote management later
address-object TW_SUBNET 172.23.37.0/24
object-group address TW_TEAM
address-object TW_SUBNET
exit
# enable Telnet access (not enabled by default, unlike other services)
ip telnet server
# open WAN-to-ZyWALL firewall for TW_TEAM for remote management
firewall WAN ZyWALL insert 4
sourceip TW_TEAM
service TELNET
action allow
exit
write
```

While configuration files and shell scripts have the same syntax, the ZyWALL / USG applies configuration files differently than it runs shell scripts. This is explained below.

**Table 201** Configuration Files and Shell Scripts in the ZyWALL / USG

| Configuration Files (.conf) | Shell Scripts (.zysh) |
|---|---|
| • Resets to default configuration.<br>• Goes into CLI **Configuration** mode.<br>• Runs the commands in the configuration file. | • Goes into CLI **Privilege** mode.<br>• Runs the commands in the shell script. |

You have to run the example in Table 28 on page 336 as a shell script because the first command is run in **Privilege** mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in **Configuration** mode. (See Section 1.5 on page 27 for more information about CLI modes.)

## 43.2.1 Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use “#” or “!” as the first character of a command line to have the ZyWALL / USG treat the line as a comment.

Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the ZyWALL / USG exit sub command mode.

Note: “exit” or “!'” must follow sub commands if it is to make the ZyWALL / USG exit sub command mode.

Line 3 in the following example exits sub command mode.

```
interface ge1
ip address dhcp
!
```

Lines 1 and 3 in the following example are comments and line 4 exits sub command mode.

```
!
interface ge1
# this interface is a DHCP client
!
```

Lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2006/06/05
interface ge1
ip address dhcp
!
```

## 43.2.2 Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the ZyWALL / USG processes the file line-by-line. The ZyWALL / USG checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the ZyWALL / USG finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The ZyWALL / USG ignores any errors in the configuration file or shell script and applies all of the valid commands. The ZyWALL / USG still generates a log for any errors.

## 43.2.3 ZyWALL / USG Configuration File Details

You can store multiple configuration files on the ZyWALL / USG. You can also have the ZyWALL / USG use a different configuration file without the ZyWALL / USG restarting.

- When you first receive the ZyWALL / USG, it uses the **system-default.conf** configuration file of default settings.
- When you change the configuration, the ZyWALL / USG creates a **startup-config.conf** file of the current configuration.
- The ZyWALL / USG checks the **startup-config.conf** file for errors when it restarts. If there is an error in the **startup-config.conf** file, the ZyWALL / USG copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file.

- When the ZyWALL / USG reboots, if the **startup-config.conf** file passes the error check, the ZyWALL / USG keeps a copy of the **startup-config.conf** file as the **lastgood.conf** configuration file for you as a back up file. If you upload and apply a configuration file with an error, you can apply **lastgood.conf** to return to a valid configuration.

### 43.2.4 Configuration File Flow at Restart

If there is not a **startup-config.conf** when you restart the ZyWALL / USG (whether through a management interface or by physically turning the power off and back on), the ZyWALL / USG uses the **system-default.conf** configuration file with the ZyWALL / USG's default settings.

If there is a **startup-config.conf**, the ZyWALL / USG checks it for errors and applies it. If there are no errors, the ZyWALL / USG uses it and copies it to the **lastgood.conf** configuration file. If there is an error, the ZyWALL / USG generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the ZyWALL / USG applies the **system-default.conf** configuration file.

You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The ZyWALL / USG ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The ZyWALL / USG still generates a log for any errors.

## 43.3 File Manager Commands Input Values

The following table explains the values you can input with the file manager commands.

**Table 202** File Manager Command Input Values

| LABEL | DESCRIPTION |
|---|---|
| *file_name* | The name of a file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). |

# 43.4 File Manager Commands Summary

The following table lists the commands that you can use for file management.

**Table 203** File Manager Commands Summary

| COMMAND | DESCRIPTION |
|---|---|
| apply /conf/*file_name.conf* [ignore-error] [rollback] | Has the ZyWALL / USG use a specific configuration file. You must still use the write command to save your configuration changes to the flash ("non-volatile" or "long term") memory.<br><br>Use this command without specify both ignore-error and rollback: this is not recommended because it would leave the rest of the configuration blank. If the interfaces were not configured before the first error, the console port may be the only way to access the device.<br><br>Use ignore-error without rollback: this applies the valid parts of the configuration file and generates error logs for all of the configuration file's errors. This lets the ZyWALL / USG apply most of your configuration and you can refer to the logs for what to fix.<br><br>Use both ignore-error and rollback: this applies the valid parts of the configuration file, generates error logs for all of the configuration file's errors, and starts the ZyWALL / USG with a fully valid configuration file.<br><br>Use rollback without ignore-error: this gets the ZyWALL / USG started with a fully valid configuration file as quickly as possible.<br><br>You can use the "apply /conf/system-default.conf" command to reset the ZyWALL / USG to go back to its system defaults. |
| copy {/cert \| /conf \| /idp \| / packet_trace \| /script \| /tmp}*file_name-a.conf* {/cert \| /conf \| /idp \| / packet_trace \| /script \| /tmp}/ *file_name-b.conf* | Saves a duplicate of a file on the ZyWALL / USG from the source file name to the target file name.<br><br>Specify the directory and file name of the file that you want to copy and the directory and file name to use for the duplicate. Always copy the file into the same directory. |
| copy running-config startup-config | Saves your configuration changes to the flash ("non-volatile" or "long term") memory. The ZyWALL / USG immediately uses configuration changes made via commands, but if you do not use this command or the write command, the changes will be lost when the ZyWALL / USG restarts. |
| copy running-config /conf/*file_name.conf* | Saves a duplicate of the configuration file that the ZyWALL / USG is currently using. You specify the file name to which to copy. |
| delete {/cert \| /conf \| /idp \| / packet_trace \| /script \| /tmp}/*file_name* | Removes a file. Specify the directory and file name of the file that you want to delete. |
| dir {/cert \| /conf \| /idp \| / packet_trace \| /script \| /tmp} | Displays the list of files saved in the specified directory. |
| rename {/cert \| /conf \| /idp \| / packet_trace \| /script \| /tmp}/*old-file_name* {/cert \| /conf \| /idp \| / packet_trace \| /script \| /tmp}/*new-file_name* | Changes the name of a file.<br><br>Specify the directory and file name of the file that you want to rename. Then specify the directory again followed by the new file name. |
| rename /script/*old-file_name* /script/ *new-file_name* | Changes the name of a shell script. |
| run /script/*file_name.zysh* | Has the ZyWALL / USG execute a specific shell script file. You must still use the write command to save your configuration changes to the flash ("non-volatile" or "long term") memory. |

**Table 203** File Manager Commands Summary (continued)

| COMMAND | DESCRIPTION |
|---|---|
| schedule-run 1 *file_name.zysh* {daily \| monthly \| weekly} time {*date* \| sun \| mon \| tue \| wed \| thu \| fri \| sat} | Has the ZyWALL / USG execute the specified specific shell script file at the the specified time. You must still use the write command to save your configuration changes to the flash (“non-volatile” or “long term”) memory. |
| show running-config | Displays the settings of the configuration file that the system is using. |
| setenv-startup stop-on-error off | Has the ZyWALL / USG ignore any errors in the startup-config.conf file and apply all of the valid commands. |
| show setenv-startup | Displays whether or not the ZyWALL / USG is set to ignore any errors in the startup-config.conf file and apply all of the valid commands. |
| write | Saves your configuration changes to the flash (“non-volatile” or “long term”) memory. The ZyWALL / USG immediately uses configuration changes made via commands, but if you do not use the write command, the changes will be lost when the ZyWALL / USG restarts. |

# 43.5 File Manager Command Examples

This example saves a back up of the current configuration before applying a shell script file.

```
Router(config)# copy running-config /conf/backup.conf
Router(config)# run /script/vpn_setup.zysh
```

These commands run the aaa.zysh script at noon every day, on the first day of every month, and on every Monday, Wednesday, and Friday.

```
Router> configure terminal
Router(config)# schedule-run 1 aaa.zysh daily 12:00
Router(config)# schedule-run 1 aaa.zysh monthly 12:00 01
Router(config)# schedule-run 1 aaa.zysh weekly 12:00 mon wed fri
Router(config)#
```

# 43.6 FTP File Transfer

You can use FTP to transfer files to and from the ZyWALL / USG for advanced maintenance and support.

## 43.6.1 Command Line FTP File Upload

1. Connect to the ZyWALL / USG.
2. Enter “bin” to set the transfer mode to binary.
3. You can upload the firmware after you log in through FTP. To upload other files, use “cd” to change to the corresponding directory.

4 Use “put” to transfer files from the computer to the ZyWALL / USG.[1] For example:

In the conf directory, use "put config.conf today.conf” to upload the configuration file (config.conf) to the ZyWALL / USG and rename it “today.conf”.

"put 1.00(XL.0).bin” transfers the firmware (1.00(XL.0).bin) to the ZyWALL / USG.

**The firmware update can take up to five minutes. Do not turn off or reset the ZyWALL / USG while the firmware update is in progress! If you lose power during the firmware upload, you may need to refer to Section 43.8 on page 343 to recover the firmware.**

## 43.6.2 Command Line FTP Configuration File Upload Example

The following example transfers a configuration file named tomorrow.conf from the computer and saves it on the ZyWALL / USG as next.conf.

Note: Uploading a custom signature file named "custom.rules”, overwrites all custom signatures on the ZyWALL.

**Figure 29** FTP Configuration File Upload Example

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 FTP Server (ZyWALL) [192.168.1.1]
User (192.168.1.1:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> cd conf
250 CWD command successful
ftp> bin
200 Type set to I
ftp> put tomorrow.conf next.conf
200 PORT command successful
150 Opening BINARY mode data connection for next.conf
226-Post action ok!!
226 Transfer complete.
ftp: 20231 bytes sent in 0.00Seconds 20231000.00Kbytes/sec.
```

## 43.6.3 Command Line FTP File Download

1 Connect to the ZyWALL / USG.

2 Enter “bin” to set the transfer mode to binary.

3 Use “cd” to change to the directory that contains the files you want to download.

4 Use “dir” or “ls” if you need to display a list of the files in the directory.

1. When you upload a custom signature, the ZyWALL / USG appends it to the existing custom signatures stored in the "custom.rules” file.

5 Use "get" to download files. For example:

"get vpn_setup.zysh vpn.zysh" transfers the vpn_setup.zysh configuration file on the ZyWALL / USG to your computer and renames it "vpn.zysh."

### 43.6.4 Command Line FTP Configuration File Download Example

The following example gets a configuration file named today.conf from the ZyWALL / USG and saves it on the computer as current.conf.

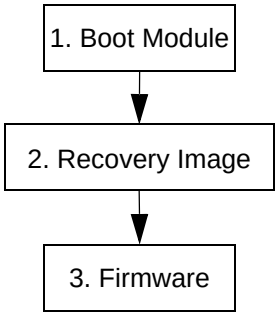
**Figure 30** FTP Configuration File Download Example

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 FTP Server (ZyWALL) [192.168.1.1]
User (192.168.1.1:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> bin
200 Type set to I
ftp> cd conf
250 CWD command successful
ftp> get today.conf current.conf
200 PORT command successful
150 Opening BINARY mode data connection for conf/today.conf (20220
bytes)
226 Transfer complete.
ftp: 20220 bytes received in 0.03Seconds 652.26Kbytes/sec.
```

## 43.7 ZyWALL / USG File Usage at Startup

The ZyWALL / USG uses the following files at system startup.

**Figure 31** ZyWALL / USG File Usage at Startup




1 The boot module performs a basic hardware test. You cannot restore the boot module if it is damaged. The boot module also checks and loads the recovery image. The ZyWALL / USG notifies you if the recovery image is damaged.

2 The recovery image checks and loads the firmware. The ZyWALL / USG notifies you if the firmware is damaged.

# 43.8 Notification of a Damaged Recovery Image or Firmware

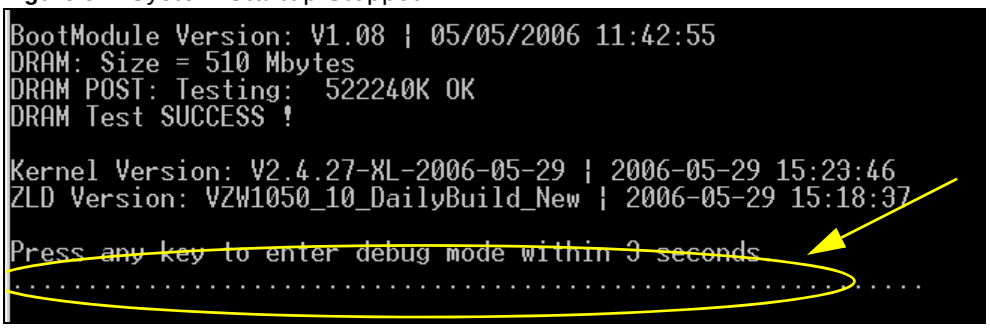
The ZyWALL / USG's recovery image and/or firmware could be damaged, for example by the power going off during a firmware upgrade. This section describes how the ZyWALL / USG notifies you of a damaged recovery image or firmware file. Use this section if your device has stopped responding for an extended period of time and you cannot access or ping it. Note that the ZyWALL / USG does not respond while starting up. It takes less than five minutes to start up with the default configuration, but the start up time increases with the complexity of your configuration.

1 Use a console cable and connect to the ZyWALL / USG via a terminal emulation program (such as HyperTerminal). Your console session displays the ZyWALL / USG's startup messages. If you cannot see any messages, check the terminal emulation program's settings (see Section 1.2.1 on page 22) and restart the ZyWALL / USG.

2 The system startup messages display followed by "Press any key to enter debug mode within 3 seconds."

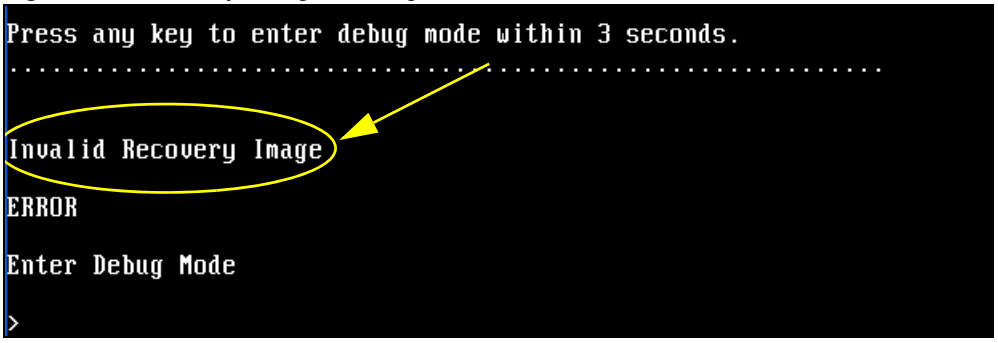
Note: Do not press any keys at this point. Wait to see what displays next.

**Figure 32** System Startup Stopped




3 If the console session displays "Invalid Firmware", or "Invalid Recovery Image", or the console freezes at "Press any key to enter debug mode within 3 seconds" for more than one minute, go to Section 43.9 on page 344 to restore the recovery image.

**Figure 33** Recovery Image Damaged



4 If “Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file” displays on the screen, the firmware file is damaged. Use the procedure in Section 43.10 on page 346 to restore it. If the message does not display, the firmware is OK and you do not need to use the firmware recovery procedure.

**Figure 34** Firmware Damaged

```
Building ...

Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file.
```

# 43.9 Restoring the Recovery Image

This procedure requires the ZyWALL / USG’s recovery image. Download the firmware package from www.zyxel.com and unzip it. The recovery image uses a .ri extension, for example, "1.01(XL.0)C0.ri". Do the following after you have obtained the recovery image file.

Note: You only need to use this section if you need to restore the recovery image.

1 Restart the ZyWALL / USG.

2 When “Press any key to enter debug mode within 3 seconds.” displays, press a key to enter debug mode.

**Figure 35** Enter Debug Mode

```
BootModule Version: V1.011 | 2007-03-30 12:22:57
DRAM: Size = 510 Mbytes
DRAM POST: Testing:  522240K OK
DRAM Test SUCCESS !

Kernel Version: V2.4.27-kernel-2006-08-21 | 2006-08-21 19:54:00
ZLD Version: V1.01(XL.0) | 2006-09-11 17:41:56

Press any key to enter debug mode within 3 seconds.
.............................
Enter Debug Mode

> 
```

3 Enter `atuk` to initialize the recovery process. If the screen displays “ERROR”, enter `atur` to initialize the recovery process.

Note: You only need to use the `atuk` or `atur` command if the recovery image is damaged.

**Figure 36** atuk Command for Restoring the Recovery Image

```
> atuk
This command is for restoring the "recovery image" (xxx.ri).
Use This command only when
1) the console displays "Invalid Recovery Image" or
2) the console freezes at "Press any key to enter debug mode within 3 seconds"
   for more than one minute.

Note:
Please exit this command immediately if you do not need to restore the
"recovery image".

Do you want to start the recovery process (Y/N)? (default N)
```

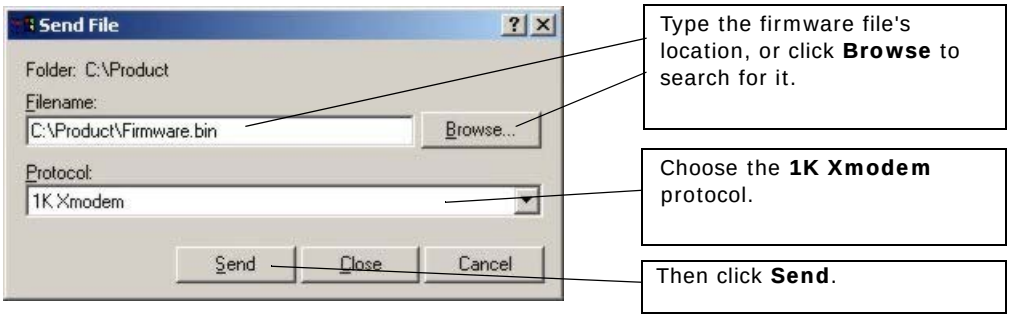
4 Enter `Y` and wait for the "Starting XMODEM upload" message before activating XMODEM upload on your terminal.

**Figure 37** Starting Xmodem Upload

```
Do you want to start the recovery process (Y/N)? (default N)
Starting XMODEM upload (CRC mode)....
C
```

5 This is an example Xmodem configuration upload using HyperTerminal. Click **Transfer**, then **Send File** to display the following screen.

**Figure 38** Example Xmodem Upload




6 Wait for about three and a half minutes for the Xmodem upload to finish.

**Figure 39** Recovery Image Upload Complete

```
Total  1867264 bytes received.
programming ..................................................
..............................................................
..............................................................
..............................................................
..............................................................
..............................................................

OK

>
```

7 Enter `atgo`. The ZyWALL / USG starts up. If “Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file” displays on the screen, the firmware file is damaged and you need to use the procedure in Section 43.10 on page 346 to recover the firmware.

**Figure 40** atgo Debug Command

```
> atgo
Booting...
```

# 43.10 Restoring the Firmware

This procedure requires the ZyWALL / USG’s firmware. Download the firmware package from www.zyxel.com and unzip it. The firmware file uses a .bin extension, for example, "1.01(XL.0)C0.bin". Do the following after you have obtained the firmware file.

Note: This section is not for normal firmware uploads. You only need to use this section if you need to recover the firmware.

1 Connect your computer to the ZyWALL / USG’s port **1** (only port **1** can be used).

2 The ZyWALL / USG’s FTP server IP address for firmware recovery is 192.168.1.1, so set your computer to use a static IP address from 192.168.1.2 ~192.168.1.254.

3 Use an FTP client on your computer to connect to the ZyWALL / USG. For example, in the Windows command prompt, type `ftp 192.168.1.1`. Keep the console session connected in order to see when the firmware recovery finishes.

4 Hit enter to log in anonymously.

5 Set the transfer mode to binary (type `bin`).

6 Transfer the firmware file from your computer to the ZyWALL / USG. Type `put` followed by the path and name of the firmware file. This examples uses `put e:\ftproot\ZLD FW \1.01(XL.0)C0.bin`.

**Figure 41** FTP Firmware Transfer Command

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220-=(<*>)=-.:. (( Welcome to PureFTPd 1.0.11 )) .:.-=(<*>)=-
220-You are user number 1 of 50 allowed
220-Local time is now 21:33 and the load is 0.01. Server port: 21.
220-Only anonymous FTP is allowed here
220 You will be disconnected after 15 minutes of inactivity.
User (192.168.1.1:(none)):
230 Anonymous user logged in
ftp> bi
200 TYPE is now 8-bit binary
ftp> put E:\ftproot\ZLD_FW\100XL0c0\1.00(XL.0)C0.bin_
```

7 Wait for the file transfer to complete.

**Figure 42** FTP Firmware Transfer Complete

```
200 PORT command successful
150 Connecting to port 1564
226-87.0 Mbytes free disk space
226-File successfully transferred
226 3.231 seconds (measured here), 10.83 Mbytes per second
ftp: 36708858 bytes sent in 3.23Seconds 11350.91Kbytes/sec.
ftp> _
```

8 After the transfer is complete, “Firmware received” or “ZLD-current received” displays. Wait (up to four minutes) while the ZyWALL / USG recovers the firmware.

**Figure 43** Firmware Received and Recovery Started

```
Firmware received ...

[Update Filesystem]
       Updating Code
       ..
```

9 The console session displays “done” when the firmware recovery is complete. Then the ZyWALL / USG automatically restarts.

**Figure 44** Firmware Recovery Complete and Restart

```
.....
.....
.....
.....
.....
.....
.....
       done

[Update Kernel]
       Extracting Kernel Image
       ..
       done
       Writing Kernel Image ... done

[Update BootModule]
       Extracting BootModule Image
       .
       done
       Writing BootModule
       .....
.....                                  done
Restarting system.
```

**10** The username prompt displays after the ZyWALL / USG starts up successfully. The firmware recovery process is now complete and the ZyWALL / USG is ready to use.

**Figure 45** Restart Complete

```
Setting the System Clock using the Hardware Clock as reference...
System Clock set. Local time: Sun Jan 26 21:40:24 UTC 2003

Cleaning: /tmp /var/lock /var/run.
Initializing random number generator... done.
Initializing Debug Account Authentication Seed (DAAS)... done.
Lionic device init successfully
cavium nitrox device CN1005 init complete
INIT: Entering runlevel: 3
Starting zylog daemon: zylogd zylog starts.
Starting syslog-ng.
Starting uam daemon.
Starting app patrol daemon.
Starting periodic command scheduler: cron.
Start ZyWALL system daemon....
Got LINK_CHANGE
Port [0] is up --> Group [0] is up
Applying system configuration file, please wait...
ZyWALL system is configured successfully with startup-config.conf

Welcome to ZyWALL 1050

Username:
```

# 43.11 Restoring the Default System Database

The default system database stores information such as the default anti-virus or IDP signatures. The ZyWALL / USG can still operate if the default system database is damaged or missing, but related features (like anti-virus or IDP) may not function properly.

If the default system database file is not valid, the ZyWALL / USG displays a warning message in your console session at startup or when reloading the anti-virus or IDP signatures. It also generates

a log. Here are some examples. Use this section to restore the ZyWALL / USG's default system database.

**Figure 46** Default System Database Console Session Warning at Startup: Anti-virus

```
Hostname: localhost.

Setting the System Clock using the Hardware Clock as reference...
System Clock set. Local time: Fri May 11 09:31:55 GMT 2007

Cleaning: /tmp /var/lock /var/run.
Initializing random number generator... done.
Initializing Debug Account Authentication Seed (DAAS)... done.
INIT: Entering runlevel: 3
Starting zylog daemon: zylogd zylog starts.
Starting syslog-ng.
Starting uam daemon.
Starting app patrol daemon.
Starting periodic command scheduler: cron.
Start ZyWALL system daemon....
Got LINK_CHANGE
Port [1] is up --> Group [1] is up
% Anti-Virus signatures misssing, refer to your user documentation to recover th
e default database file.
% Loading AV signature database has failed.
Applying system configuration file, please wait...
ZyWALL system is configured successfully with startup-config.conf

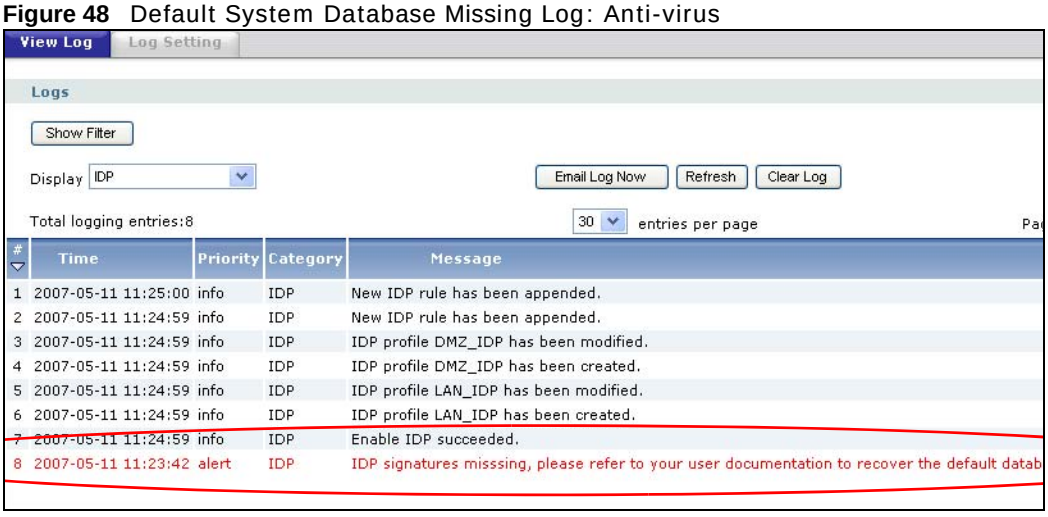
Welcome to ZyWALL USG 300

Username:
```

**Figure 47** Default System Database Console Session Warning When Reloading IDP

```
Router(config)# idp reload
IDP signatures misssing, please refer to your user documentation to recover the
default database file.
retval = -32056
ERROR: Enable IDP engine failed.
Router(config)#
```

**Figure 48** Default System Database Missing Log: Anti-virus




This procedure requires the ZyWALL / USG's default system database file. Download the firmware package from www.zyxel.com and unzip it. The default system database file uses a .db extension,

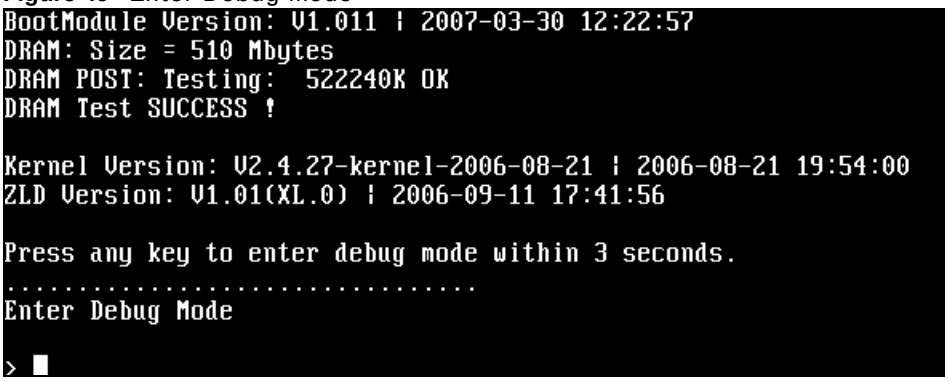
for example, "1.01(XL.0)C0.db". Do the following after you have obtained the default system database file.

## 43.11.1 Using the atkz -u Debug Command

Note: You only need to use the `atkz -u` command if the default system database is damaged.

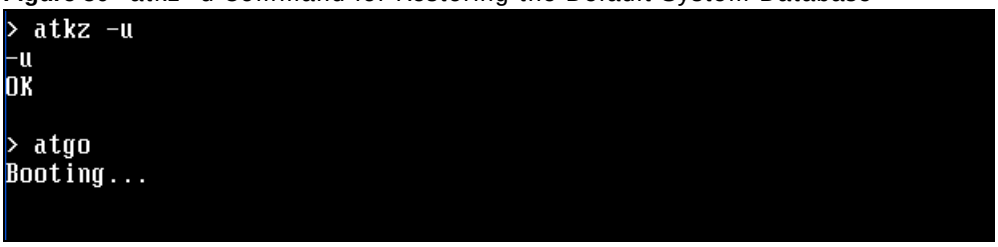
1. Restart the ZyWALL / USG.
2. When “Press any key to enter debug mode within 3 seconds.” displays, press a key to enter debug mode.

**Figure 49** Enter Debug Mode



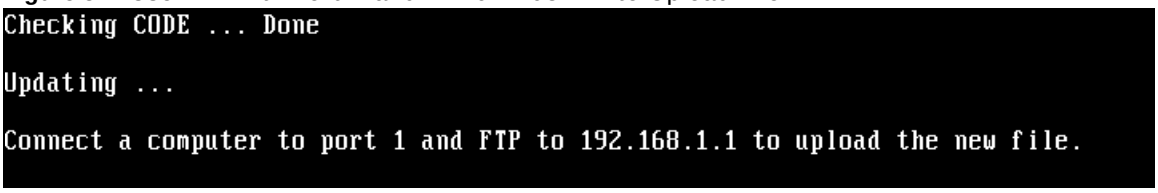

3. Enter `atkz -u` to start the recovery process.

**Figure 50** atkz -u Command for Restoring the Default System Database




4. “Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file” displays on the screen. Connect your computer to the ZyWALL / USG’s port **1** (only port **1** can be used).

**Figure 51** Use FTP with Port 1 and IP 192.168.1.1 to Upload File




5. The ZyWALL / USG’s FTP server IP address for firmware recovery is 192.168.1.1, so set your computer to use a static IP address from 192.168.1.2 ~192.168.1.254.
6. Use an FTP client on your computer to connect to the ZyWALL / USG. For example, in the Windows command prompt, type `ftp 192.168.1.1`. Keep the console session connected in order to see when the default system database recovery finishes.

7 Hit enter to log in anonymously.

8 Set the transfer mode to binary (type `bin`).

9 Transfer the firmware file from your computer to the ZyWALL / USG. Type `put` followed by the path and name of the firmware file. This examples uses `put e:\ftproot\ZLD FW \1.01(XL.0)C0.db`.

**Figure 52** FTP Default System Database Transfer Command

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220-=(<*>)=-.:. (( Welcome to PureFTPd 1.0.11 )) .:.-=(<*>)=-
220-You are user number 1 of 50 allowed
220-Local time is now 03:56 and the load is 0.00. Server port: 21.
220-Only anonymous FTP is allowed here
220 You will be disconnected after 15 minutes of inactivity.
User (192.168.1.1:(none)):
230 Anonymous user logged in
ftp> bin
200 TYPE is now 8-bit binary
ftp> put E:\ftproot\ZLD_FW\101XL\101XL0C0\1.01(XL.0)C0.db
```

10 Wait for the file transfer to complete.

**Figure 53** FTP Default System Database Transfer Complete

```
200 PORT command successful
150 Connecting to port 3709
226-248.5 Mbytes free disk space
226-File successfully transferred
226 0.008 seconds (measured here), 13.31 Mbytes per second
ftp: 112398 bytes sent in 0.02Seconds 7024.88Kbytes/sec.
ftp> _
```

11 The console session displays “done” after the default system database is recovered.

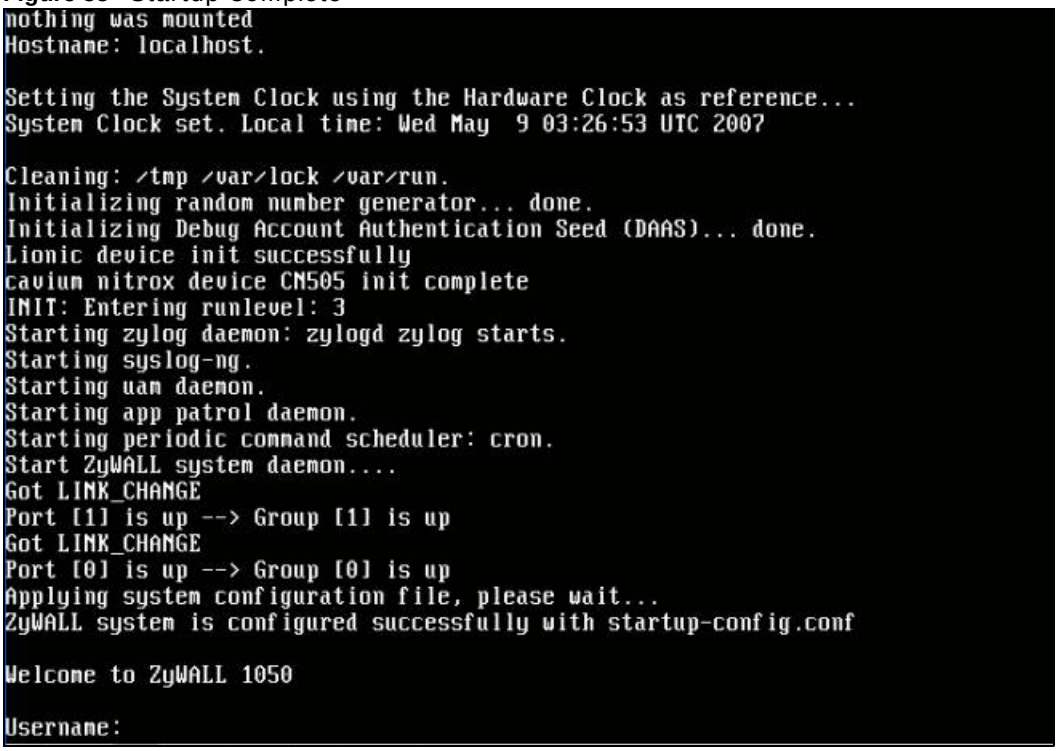
**Figure 54** Default System Database Received and Recovery Complete

```
Default System Database received ...

[Update Filesystem]
        Updating Database
        .
        done
```

**12** The username prompt displays after the ZyWALL / USG starts up successfully. The default system database recovery process is now complete and the ZyWALL / USG IDP and anti-virus features are ready to use again.

**Figure 55** Startup Complete



# 44

# Logs

This chapter provides information about the ZyWALL / USG's logs.

Note: When the system log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

See the User's Guide for the maximum number of system log messages in the ZyWALL / USG.

## 44.1 Log Commands Summary

The following table describes the values required for many log commands. Other values are discussed with the corresponding commands.

**Table 204** Input Values for Log Commands

| LABEL | DESCRIPTION |
|---|---|
| *interface_name* | The name of the interface.<br>Ethernet interface: For the ZyWALL / USG USG 300 and above, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model.<br>The ZyWALL / USG USG 200 and lower models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.<br>Virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4<br>VLAN interface: vlan*x*, *x* = 0 - 4094<br>Virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 12<br>Bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ZyWALL / USG model supports.<br>Virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4<br>PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL / USG model supports. |
| *module_name* | The name of the category; `kernel`, `syslog`, .... The `default` category includes debugging messages generated by open source software. The `all` category includes all messages in all categories. |
| *protocol* | The name of a protocol such as TCP, UDP, ICMP. |

The following sections list the logging commands.

## 44.1.1 Log Entries Commands

This table lists the commands to look at log entries.

**Table 205** logging Commands: Log Entries

| COMMAND | DESCRIPTION |
|---|---|
| show logging entries [priority *pri*] [category *module_name*] [srcip *ip*] [srcip6 *ipv6_addr*] [dstip *ip*] [dstip6 *ipv6_addr*] [service *service_name]* [begin <1..512> end <1..512>] [keyword *keyword*] [srciface *interface_name*] [dstiface *interface_name*] [protocol *protocol*] | Displays the specified entries in the system log.<br>*pri*: alert \| crit \| debug \| emerg \| error \| info \| notice \| warn<br>*keyword*: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 63 characters long. This searches the message, source, destination, and notes fields. |
| show logging entries field *field* [begin <1..512> end <1..512>] | Displays the specified fields in the system log.<br>*field*: time \| msg \| src \| dst \| note \| pri \| cat \| all |

## 44.1.2 System Log Commands

This table lists the commands for the system log settings.

**Table 206** logging Commands: System Log Settings

| COMMAND | DESCRIPTION |
|---|---|
| show logging status system-log | Displays the current settings for the system log. |
| logging system-log category *module_name* {disable \| level normal \| level all} | Specifies what kind of information, if any, is logged in the system log and debugging log for the specified category. |
| [no] logging system-log suppression interval <10..600> | Sets the log consolidation interval for the system log. The no command sets the interval to ten. |
| [no] logging system-log suppression | Enables log consolidation in the system log. The no command disables log consolidation in the system log. |
| [no] connectivity-check continuous-log activate | Has the ZyWALL / USG generate a log for each connectivity check. The no command has the ZyWALL / USG only log the first connectivity check. |
| show connectivity-check continuous-log status | Displays whether or not the ZyWALL / USG generates a log for each connectivity check. |
| clear logging system-log buffer | Clears the system log. |

#### 44.1.2.1 System Log Command Examples

The following command displays the current status of the system log.

```
Router# configure terminal
Router(config)# show logging status system-log
512 events logged
suppression active  : yes
suppression interval: 10
category settings   :
    content-filter    : normal , forward-web-sites : no     ,
    blocked-web-sites : normal , user              : normal ,
    myZyXEL.com       : normal , zysh              : normal ,
    idp               : normal , app-patrol        : normal ,
    ike               : normal , ipsec             : normal ,
    firewall          : normal , sessions-limit    : normal ,
    policy-route      : normal , built-in-service  : normal ,
    system            : normal , connectivity-check: normal ,
    device-ha         : normal , routing-protocol  : normal ,
    nat               : normal , pki               : normal ,
    interface         : normal , interface-statistics: no     ,
    account           : normal , port-grouping     : normal ,
    force-auth        : normal , l2tp-over-ipsec   : normal ,
    anti-virus        : normal , white-list        : normal ,
    black-list        : normal , ssl-vpn           : normal ,
    cnm               : normal , traffic-log       : no     ,
    file-manage       : normal , dial-in           : normal ,
    adp               : normal , default           : all    ,
```

## 44.1.3 Debug Log Commands

This table lists the commands for the debug log settings.

**Table 207** logging Commands: Debug Log Settings

| COMMAND | DESCRIPTION |
|---|---|
| `show logging debug status` | Displays the current settings for the debug log. |
| `show logging debug entries [priority` *pri*`] [category` *module_name*`] [srcip` *ip*`] [srcip6` *ipv6_addr*`] [dstip` *ip*`] [dstip6` *ipv6_addr*`] [service` *service_name]* `[srciface` *interface_name*`] [dstiface` *interface_name*`] [protocol` *protocol*`] [begin <1..512> end <1..512>] [keyword` *keyword*`]` | Displays the specified entries in the system log.<br>*pri*: alert \| crit \| debug \| emerg \| error \| info \| notice \| warn<br>*keyword*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 63 characters long. This searches the message, source, destination, and notes fields. |
| `show logging debug entries field` *field* `[begin <1..1024> end <1..1024>]` | Displays the specified field in the debug log.<br>*field*: time \| msg \| src \| dst \| note \| pri \| cat \| all |
| `[no] logging debug suppression` | Enables log consolidation in the debug log. The `no` command disables log consolidation in the debug log. |
| `[no] logging debug suppression interval <10..600>` | Sets the log consolidation interval for the debug log. The `no` command sets the interval to ten. |
| `clear logging debug buffer` | Clears the debug log. |

This table lists the commands for the remote syslog server settings.

**Table 208** logging Commands: Remote Syslog Server Settings

| COMMAND | DESCRIPTION |
|---|---|
| show logging status syslog | Displays the current settings for the remote servers. |
| [no] logging syslog <1..4> | Enables the specified remote server. The no command disables the specified remote server. |
| [no] logging syslog <1..4> address {*ip* \| *hostname*} | Sets the URL or IP address of the specified remote server. The no command clears this field.<br>*hostname*: You may up to 63 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period. |
| [no] logging syslog <1..4> {disable \| level normal \| level all} | Specifies what kind of information, if any, is logged for the specified category. |
| [no] logging syslog <1..4> facility {local_1 \| local_2 \| local_3 \| local_4 \| local_5 \| local_6 \| local_7} | Sets the log facility for the specified remote server. The no command sets the facility to local_1. |
| [no] logging syslog <1..4> format {cef \| vrpt} | Sets the format of the log information.<br>cef: Common Event Format, syslog-compatible format.<br>vrpt: ZyXEL's Vantage Report, syslog-compatible format. |

This table lists the commands for setting how often to send information to the VRPT (ZyXEL's Vantage Report) server.

**Table 209** logging Commands: VRPT Settings

| COMMAND | DESCRIPTION |
|---|---|
| vrpt send device information interval <15..3600> | Sets the interval (in seconds) for how often the ZyWALL / USG sends a device information log to the VRPT server. |
| vrpt send interface statistics interval <15..3600> | Sets the interval (in seconds) for how often the ZyWALL / USG sends an interface statistics log to the VRPT server. |
| vrpt send system status interval <15..3600> | Sets the interval (in seconds) for how often the ZyWALL / USG sends a system status log to the VRPT server. |
| show vrpt send device information interval | Displays the interval (in seconds) for how often the ZyWALL / USG sends a device information log to the VRPT server. |
| show vrpt send interface statistics interval | Displays the interval (in seconds) for how often the ZyWALL / USG sends an interface statistics log to the VRPT server. |
| show vrpt send system status interval | Displays the interval (in seconds) for how often the ZyWALL / USG sends a system status log to the VRPT server. |

## 44.1.4 E-mail Profile Commands

This table lists the commands for the e-mail profile settings.

**Table 210** logging Commands: E-mail Profile Settings

| COMMAND | DESCRIPTION |
|---|---|
| show logging status mail | Displays the current settings for the e-mail profiles. |
| [no] logging mail <1..2> | Enables the specified e-mail profile. The no command disables the specified e-mail profile. |

**Table 210** logging Commands: E-mail Profile Settings (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] logging mail <1..2> address {*ip* \| *hostname*} | Sets the URL or IP address of the mail server for the specified e-mail profile. The no command clears the mail server field.<br>*hostname*: You may up to 63 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period. |
| logging mail <1..2> sending_now | Sends mail for the specified e-mail profile immediately, according to the current settings. |
| [no] logging mail <1..2> authentication | Enables SMTP authentication. The no command disables SMTP authentication. |
| [no] logging mail <1..2> authentication username *username* password *password* | Sets the username and password required by the SMTP mail server. The no command clears the username and password fields.<br>*username*: You can use alphanumeric characters, underscores (_), and dashes (-), and it can be up to 31 characters long.<br>*password*: You can use most printable ASCII characters. You cannot use square brackets [ ], double quotation marks (“), question marks (?), tabs or spaces. It can be up to 31 characters long. |
| [no] logging mail <1..2> port <1..65535> | Sets the port number of the mail server for the specified e-mail profile. |
| [no] logging mail <1..2> {send-log-to \| send-alerts-to} *e_mail* | Sets the e-mail address for logs or alerts. The no command clears the specified field.<br>*e_mail*: You can use up to 63 alphanumeric characters, underscores (_), or dashes (-), and you must use the @ character. |
| [no] logging mail <1..2> subject *subject* | Sets the subject line when the ZyWALL / USG mails to the specified e-mail profile. The no command clears this field.<br>*subject*: You can use up to 60 alphanumeric characters, underscores (_), dashes (-), or !@#$%*()+=;:',./ characters. |
| [no] logging mail <1..2> category *module_name* level {alert \| all} | Specifies what kind of information is logged for the specified category. The no command disables logging for the specified category. |
| [no] logging mail <1..2> schedule {full \| hourly} | Sets the e-mail schedule for the specified e-mail profile. The no command clears the schedule field. |
| logging mail <1..2> schedule daily hour <0..23> minute <0..59> | Sets a daily e-mail schedule for the specified e-mail profile. |
| logging mail <1..2> schedule weekly day *day* hour <0..23> minute <0..59> | Sets a weekly e-mail schedule for the specified e-mail profile.<br>*day*: sun \| mon \| tue \| wed \| thu \| fri \| sat |

#### 44.1.4.1 E-mail Profile Command Examples

The following commands set up e-mail log 1.

```
Router# configure terminal
Router(config)# logging mail 1 address mail.zyxel.com.tw
Router(config)# logging mail 1 subject AAA
Router(config)# logging mail 1 authentication username lachang.li password XXXXXX
Router(config)# logging mail 1 send-log-to lachang.li@zyxel.com.tw
Router(config)# logging mail 1 send-alerts-to lachang.li@zyxel.com.tw
Router(config)# logging mail 1 from lachang.li@zyxel.com.tw
Router(config)# logging mail 1 schedule weekly day mon hour 3 minute 3
Router(config)# logging mail 1
```

### 44.1.5 Console Port Logging Commands

This table lists the commands for the console port settings.

**Table 211** logging Commands: Console Port Settings

| COMMAND | DESCRIPTION |
|---|---|
| `show logging status console` | Displays the current settings for the console log. (This log is not discussed above.) |
| `[no] logging console` | Enables the console log. The no command disables the console log. |
| `logging console category` *module_name* `level {alert \| crit \| debug \| emerg \| error \| info \| notice \| warn}` | Controls whether or not debugging information for the specified priority is displayed in the console log, if logging for this category is enabled. |
| `[no] logging console category` *module_name* | Enables logging for the specified category in the console log. The no command disables logging. |

# 45

# Reports and Reboot

This chapter provides information about the report associated commands and how to restart the ZyWALL / USG using commands. It also covers the daily report e-mail feature.

## 45.1 Report Commands Summary

The following sections list the report, session, and packet size statistics commands.

### 45.1.1 Report Commands

This table lists the commands for reports.

**Table 212** report Commands

| COMMAND | DESCRIPTION |
|---|---|
| `[no] report` | Begins data collection. The `no` command stops data collection. |
| `show report status` | Displays whether or not the ZyWALL / USG is collecting data and how long it has collected data. |
| `clear report [interface_name]` | Clears the report for the specified interface or for all interfaces. |
| `show report [interface_name {ip \| service \| url}]` | Displays the traffic report for the specified interface and controls the format of the report. Formats are:<br>`ip` - traffic by IP address and direction<br>`service` - traffic by service and direction<br>`url` - hits by URL |

## 45.1.2 Report Command Examples

The following commands start collecting data, display the traffic reports, and stop collecting data.

```
Router# configure terminal
Router(config)# show report ge1 ip
No. IP Address      User                  Amount          Direction
================================================================
1   192.168.1.4     admin                 1273(bytes)     Outgoing
2   192.168.1.4     admin                 711(bytes)      Incoming
Router(config)# show report ge1 service
No. Port  Service          Amount          Direction
================================================================
1   21    ftp              1273(bytes)     Outgoing
2   21    ftp              711(bytes)      Incoming
Router(config)# show report ge1 url
No. Hit        URL
================================================================
1   1          140.114.79.60
Router(config)# show report status
Report status: on
Collection period: 0 days 0 hours 0 minutes 18 seconds
```

## 45.1.3 Session Commands

This table lists the commands to display the current sessions for debugging or statistical analysis.

**Table 213** Session Commands

| COMMAND | DESCRIPTION |
|---|---|
| `show conn [user {username\|any\|unknown}] [service {service-name\|any\|unknown}] [source {ip\|any}] [destination {ip\|any}] [begin <1..128000>] [end <1..128000>]` | Displays information about the selected sessions or about all sessions. You can look at all the active sessions or filter the information by user name, service object, source IP, destination IP, or session number(s).<br>`any` means all users, services and IP addresses respectively.<br>`unknow` means unknown users and services respectively. |
| `show conn ip-traffic destination` | Displays information about traffic session sorted by the destination. |
| `show conn ip-traffic source` | Displays information about traffic session sorted by the source. |
| `show conn status` | Displays the number of active sessions. |

## 45.1.4 Packet Size Statistics Commands

Using the packet size statistics to view packet size distribution may aid you in troubleshooting network performance. In particular, a large number of small packets can drastically reduce throughput. This table lists the commands to enable and disable packet size statistics data collection and display the setting status and statistics.

**Table 214** Packet Size Statistics Commands

| COMMAND | DESCRIPTION |
|---|---|
| `[no] report packet size statistics` | Enables or disables packet size statistics data collection. |
| `show report packet size statistics status` | Shows whether packet size statistics data collection is enabled or disabled. |

**Table 214** Packet Size Statistics Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| show report packet size statistics {*interface_name*} [interval *interval*] | Displays the specified interface's packet size distribution statistics. You can also specify the packet size interval into which to group the statistics.<br>*interval*: 128, 256, or 512 (bytes) |
| report packet size statistics clear | Clears the packet size statistics data for all interface. |

# 45.2 Email Daily Report Commands

The following table identifies the values used in some of these commands. Other input values are discussed with the corresponding commands.

**Table 215** Input Values for Email Daily Report Commands

| LABEL | DESCRIPTION |
|---|---|
| *e_mail* | An e-mail address. You can use up to 80 alphanumeric characters, underscores (_), periods (.), or dashes (-), and you must use the @ character. |

Use these commands to have the ZyWALL / USG e-mail you system statistics every day. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 216** Email Daily Report Commands

| COMMAND | DESCRIPTION |
|---|---|
| show daily-report status | Displays the e-mail daily report settings. |
| daily-report | Enters the sub-command mode for configuring daily e-mail reports settings. |
| [no] activate | Turns daily e-mail reports on or off. |
| draw-usage-graphics | Has the report e-mail include usage graphs. |
| smtp-address {*ip* \| *hostname*} | Sets the SMTP mail server IP address or domain name. |
| [no] smtp-auth activate | Enables or disables SMTP authentication. |
| smtp-auth username *username* password *password* | Sets the username and password for SMTP authentication. |
| no smtp-address | Resets the SMTP mail server configuration. |
| no smtp-auth username | Resets the authentication configuration. |
| [no] smtp-port <1..65535> | Sets the SMTP authentication port. The `no` command deletes the setting. |
| mail-subject set *subject* | Configures the subject of the report e-mails. Spaces are allowed. |
| no mail-subject set | Clears the configured subject for the report e-mails. |
| [no] mail-subject append system-name | Determines whether the system name will be appended to the subject of the report e-mails. |
| [no] mail-subject append date-time | Determines whether the sending date-time will be appended at subject of the report e-mails. |
| [no] mail-from *e_mail* | Sets the sender e-mail address of the report e-mails. |
| [no] mail-to-1 *e_mail* | Sets to whom the ZyWALL / USG sends the report e-mails (up to five recipients). |
| [no] mail-to-2 *e_mail* | See above. |

**Table 216** Email Daily Report Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| [no] mail-to-3 *e_mail* | See above. |
| [no] mail-to-4 *e_mail* | See above. |
| [no] mail-to-5 *e_mail* | See above. |
| [no] item as-report | Determines whether or not anti-spam statistics are included in the report e-mails. |
| [no] item av-report | Determines whether or not anti-virus statistics are included in the report e-mails. |
| [no] item cf-report | Determines whether or not content filtering statistics are included in the report e-mails. |
| [no] item cpu-usage | Determines whether or not CPU usage statistics are included in the report e-mails. |
| [no] item idp-report | Determines whether or not IDP statistics are included in the report e-mails. |
| [no] item mem-usage | Determines whether or not memory usage statistics are included in the report e-mails. |
| [no] item port-usage | Determines whether or not port usage statistics are included in the report e-mails. |
| [no] item session-usage | Determines whether or not session usage statistics are included in the report e-mails. |
| [no] item traffic-report | Determines whether or not network traffic statistics are included in the report e-mails. |
| schedule hour <0..23> minute <00..59> | Sets the time for sending out the report e-mails. |
| [no] reset-counter | Determines whether or not to discard all report data and starts all of the report statistics data counters over at zero after successfully sending out a report e-mail. |
| send-now | Sends the daily e-mail report immediately. |
| reset-counter-now | Discards all report data and starts all of the report statistics data counters over at zero. |
| exit | Leaves the sub-command mode. |

## 45.2.1 Email Daily Report Example

This example sets the following about sending a daily report e-mail:

- Disables the reporting.
- Specifies example-SMTP-mail-server.com as the address of the SMTP mail server.
- Sets the subject of the report e-mails to test.
- Stops the system name from being appended to the mail subject.
- Appends the date and time to the mail subject.
- Sets the sender as my-email@example.com.
- Sets example-administrator@example.com as the first account to which to send the mail.
- Has the ZyWALL / USG not use the second and third mail-to options.
- Sets my-email@example.com as the fourth mail-to option.
- Has the ZyWALL / USG not use the fifth mail-to option.

- Has the ZyWALL / USG provide username 12345 and password 12345 to the SMTP server for authentication.
- Sets the ZyWALL / USG to send the report at 1:57 PM.
- Has the ZyWALL / USG not reset the counters after sending the report.
- Has the report include CPU, memory, port, and session usage along with traffic statistics.
- Turns on the daily e-mail reporting.

```
Router(config)# daily-report
Router(config-daily-report)# no activate
Router(config-daily-report)# smtp-address example-SMTP-mail-server.com
Router(config-daily-report)# mail-subject set test
Router(config-daily-report)# no mail-subject append system-name
Router(config-daily-report)# mail-subject append date-time
Router(config-daily-report)# mail-from my-email@example.com
Router(config-daily-report)# mail-to-1 example-administrator@example.com
Router(config-daily-report)# no mail-to-2
Router(config-daily-report)# no mail-to-3
Router(config-daily-report)# mail-to-4 my-email@example.com
Router(config-daily-report)# no mail-to-5
Router(config-daily-report)# smtp-auth activate
Router(config-daily-report)# smtp-auth username 12345 password pass12345
Router(config-daily-report)# schedule hour 13 minutes 57
Router(config-daily-report)# no reset-counter
Router(config-daily-report)# item cpu-usage
Router(config-daily-report)# item mem-usage
Router(config-daily-report)# item port-usage
Router(config-daily-report)# item session-usage
Router(config-daily-report)# item traffic-report
Router(config-daily-report)# activate
Router(config-daily-report)# exit
Router(config)#
```

This displays the email daily report settings and has the ZyWALL / USG send the report.

```
Router(config)# show daily-report status
email daily report status
=========================
activate: yes
scheduled time: 13:57
reset counter: no
smtp address: example-SMTP-mail-server.com
smtp port: 25
smtp auth: yes
smtp username: 12345
smtp password: pass12345
mail subject:  test subject
append system name: no
append date time: yes
mail from: my-email@example.com
mail-to-1: example-administrator@example.com
mail-to-2:
mail-to-3:
mail-to-4: my-email@example.com
mail-to-5:
cpu-usage: yes
mem-usage: yes
session-usage: yes
port-usage: yes
traffic-report: yes

Router(config)# daily-report send-now
```

# 45.3 Reboot

Use this to restart the device (for example, if the device begins behaving erratically).

If you made changes in the CLI, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot.

Use the `reboot` command to restart the device.

# 46

# Session Timeout

Use these commands to modify and display the session timeout values. You must use the `configure terminal` command before you can use these commands.

**Table 217** Session Timeout Commands

| COMMAND | DESCRIPTION |
|---|---|
| `session timeout {udp-connect <1..300> \| udp-deliver <1..300> \| icmp <1..300>}` | Sets the timeout for UDP sessions to connect or deliver and for ICMP sessions. |
| `session timeout session {tcp-established \| tcp-synrecv \| tcp-close \| tcp-finwait \| tcp-synsent \| tcp-closewait \| tcp-lastack \| tcp-timewait} <1..300>` | Sets the timeout for TCP sessions in the ESTABLISHED, SYN_RECV, FIN_WAIT, SYN_SENT, CLOSE_WAIT, LAST_ACK, or TIME_WAIT state. |
| `show session timeout {icmp \| tcp-timewait \| udp}` | Displays ICMP, TCP, and UDP session timeouts. |

The following example sets the UDP session connect timeout to 10 seconds, the UDP deliver session timeout to 15 seconds, and the ICMP timeout to 15 seconds.

```
Router(config)# session timeout udp-connect 10
Router(config)# session timeout udp-deliver 15
Router(config)# session timeout icmp 15
Router(config)# show session timeout udp
UDP session connect timeout: 10 seconds
UDP session deliver timeout: 15 seconds
Router(config)# show session timeout icmp
ICMP session timeout: 15 seconds
```

# 47

# Diagnostics

This chapter covers how to use the diagnostics feature.

## 47.1 Diagnostics

The diagnostics feature provides an easy way for you to generate a file containing the ZyWALL / USG's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting.

## 47.2 Diagnosis Commands

The following table lists the commands that you can use to have the ZyWALL / USG collect diagnostics information. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

**Table 218** diagnosis Commands

| COMMAND | DESCRIPTION |
|---|---|
| `diag-info collect` | Has the ZyWALL / USG create a new diagnostic file. |
| `show diag-info` | Displays the name, size, and creation date (in yyyy-mm-dd hh:mm:ss format) of the diagnostic file. |

## 47.3 Diagnosis Commands Example

The following example creates a diagnostic file and displays its name, size, and creation date.

```
Router# configure terminal
Router(config)# diag-info collect
Please wait, collecting information
Router(config)# show diag-info
Filename  : diaginfo-20070423.tar.bz2
File size : 1259 KB
Date      : 2007-04-23 09:55:09
```

# 48

# Packet Flow Explore

This chapter covers how to use the packet flow explore feature.

## 48.1 Packet Flow Explore

Use this to get a clear picture on how the ZyWALL / USG determines where to forward a packet and how to change the source IP address of the packet according to your current settings. This function provides you a summary of all your routing and SNAT settings and helps troubleshoot the related problems.

## 48.2 Packet Flow Explore Commands

The following table lists the commands that you can use to have the ZyWALL / USG display routing and SNAT related settings.

**Table 219** Packet Flow Explore Commands

| COMMAND | DESCRIPTION |
|---|---|
| `show route order` | Displays the order of routing related functions the ZyWALL / USG checks for packets. Once a packet matches the criteria of a routing rule, the ZyWALL / USG takes the corresponding action and does not perform any further flow checking. |
| `show system snat order` | Displays the order of SNAT related functions the ZyWALL / USG checks for packets. Once a packet matches the criteria of an SNAT rule, the ZyWALL / USG uses the corresponding source IP address and does not perform any further flow checking. |
| `show system route policy-route` | Displays activated policy routes. |
| `show system route nat-1-1` | Displays activated 1-to-1 NAT rules. |
| `show system route site-to-site-vpn` | Displays activated site-to-site VPN rules. |
| `show system route dynamic-vpn` | Displays activated dynamic VPN rules. |
| `show system route default-wan-trunk` | Displays the default WAN trunk settings. |
| `show ip route static-dynamic` | Displays activated static-dynamic routes. |
| `show system snat policy-route` | Displays activated policy routes which use SNAT. |
| `show system snat nat-1-1` | Displays activated NAT rules which use SNAT. |
| `show system snat nat-loopback` | Displays activated activated NAT rules which use SNAT with NAT loopback enabled. |
| `show system snat default-snat` | Displays the default WAN trunk settings. |

# 48.3 Packet Flow Explore Commands Example

The following example shows all routing related functions and their order.

```
Router> show route order
route order: Policy Route, Direct Route, 1-1 SNAT, SiteToSite VPN, Dynamic VPN,
Static-Dynamic Route, Default WAN Trunk, Main Route
```

The following example shows all SNAT related functions and their order.

```
Router> show system snat order
snat order: Policy Route SNAT, 1-1 SNAT, Loopback SNAT, Default SNAT
```

The following example shows all SNAT related functions and their order.

```
Router> show system route policy-route
No.  PR NO. Source   Destination      Incoming     DSCP   Service   Nexthop Type
Nexthop Info
================================================================================
```

The following example shows all activated 1-to-1 SNAT rules.

```
Router> show system route nat-1-1
No.  VS Name         Source     Destination   Outgoing        Gateway
================================================================================
```

The following example shows all activated site-to-site VPN rules.

```
Router> show system route site-to-site-vpn
No.  Source         Destination          VPN Tunnel
================================================================================
```

The following example shows all activated dynamic VPN rules.

```
Router> show system route dynamic-vpn
No.  Source         Destination             VPN Tunnel
================================================================================
```

The following example shows the default WAN trunk's settings.

```
Router> show system route default-wan-trunk
No.  Source          Destination     Trunk
================================================================================
1    any             any             trunk_ex
```

The following example shows all activated dynamic VPN rules.

```
Router> show system route dynamic-vpn
No.  Source         Destination             VPN Tunnel
================================================================================
```

The following example shows all activated static-dynamic VPN rules.

```
Router> show ip route static-dynamic
Flags: A - Activated route, S - Static route, C - directly Connected
       O - OSPF derived, R - RIP derived, G - selected Gateway
       ! - reject, B - Black hole, L - Loop

IP Address/Netmask    Gateway          IFace           Metric    Flags    Persis
t
================================================================================
0.0.0.0/0             10.1.1.254       wan1            0         ASG      -
```

The following example shows all activated policy routes which use SNAT.

```
Router> show system snat policy-route
No.  PR NO. Outgoing        SNAT
================================================================================
```

The following example shows all activated 1-to-1 NAT rules.

```
Router> show system snat nat-1-1
No.  VS Name     Source        Destination   Outgoing        SNAT
================================================================================
```

The following example shows all activated policy routes which use SNAT and enable NAT loopback..

```
Router> show system snat nat-loopback
Note: Loopback SNAT will be only applied only when the initiator is located at the
network which the server locates at

No.  VS Name        Source        Destination     SNAT
================================================================================
```

The following example shows all activated 1-to-1 NAT rules.

```
Router> show system snat nat-1-1
No.  VS Name     Source        Destination   Outgoing        SNAT
================================================================================
```

The following example shows the default WAN trunk settings.

```
Router> show system snat default-snat
Incoming                Outgoing                SNAT
==========================================================================
Internal Interface      External Interface      Outgoing Interface IP


Internal Interfaces: lan1, hidden, lan2, dmz
External Interfaces: wan1, wan2, wan1_ppp, wan2_ppp
Router>
```

# 49

# Packet Flow Filter

This chapter covers how to use the packet flow filter feature.

## 49.1 Packet Flow Filter

Use the packet flow filter to troubleshoot firewall rules and policy routes when specific packets you expect to go through the ZyWALL / USG do not.

## 49.2 Packet Flow Filter Commands

The following table identifies some common values used in packet-flow commands. Other input values are discussed with the corresponding commands.

**Table 220** Packet Flow Filter Command Input Values

| LABEL | DESCRIPTION |
|---|---|
| *pf_filter_num_range* | The filter number to be displayed.<br>1 ~ 3 depending on the product. |
| *pf_cpu_core_num* | The CPU core number of packet buffer to be displayed. This is not necessary for single-core products. For multi-core products the number ranges from 1 to the model's limit. |

The following table lists the commands that you can use to have the ZyWALL / USG display how the firewall and policy routes handle certain traffic. Use the configure terminal command to be able to use the commands that configure settings.

**Table 221** Packet Flow Filter Commands

| COMMAND | DESCRIPTION |
|---|---|
| `packet-flow filter` *pf_filter_num_range* | Enters sub-command mode for configuring the specified packet flow filter. |
| `[no] enable` | Enables or disables the packet flow filter you are configuring. |
| `[no] source {any\|`*ipv4*`}` | Sets the source address to any address or a specific IPv4 address. |
| `[no] destination {any\|`*ipv4*`}` | Sets the destination address to any address or a specific IPv4 address. |
| `[no] host {any\|`*ipv4*`}` | Sets the source address to any address or a specific IPv4 address. |
| `[no] protocol {any\|<1..255>}` | Sets the filter to work on any protocol's traffic or a specific one. |
| `[no] src-port {any\|<1..65535>}` | Sets the source port to any address or a specific port number. |
| `[no] dst-port {any\|<1..65535>}` | Sets the destination port to any address or a specific port number. |

**Table 221** Packet Flow Filter Commands (continued)

| COMMAND | DESCRIPTION |
|---|---|
| exit | Leaves the sub-command mode. |
| [no] packet-flow activate | Turns the packet flow filter on or off. |
| show packet-flow status | Displays whether or not the packet flow filter is activated and whether the ring buffer is enabled or disabled. |
| show packet-flow buffer [*pf_cpu_core_num*] | Displays the details of the captured packet flow. |
| show packet-flow filter *pf_filter_num_range* | Displays the specified packet flow filter's settings. |
| packet-flow buffer clear *pf_cpu_core_num* | Clears the specified CPU core's buffer. |
| packet-flow buffer write | Writes buffer content (of all CPU cores) to a file you can download from the FTP / tmp directory. |
| [no] packet-flow ring-buffer activate | Activate the packet flow ring buffer to overwrite the oldest record with the newest record. Use the no command to stop to capture packet after the buffer is full. |

# 49.3 Packet Flow Filter Commands Examples

The following example configures packet flow filter 1 to display how the firewall and policy routes handle UDP (protocol 17) traffic with source port 123 sent from IP address 1.2.3.4 to IP address 5.6.7.8, port 456. Then it turns on the packet flow filter.

```
Router> configure terminal
Router(coonfig)#packet-flow filter 1
Router(coonfig-packet-flow-filter 1)#source 1.2.3.4
Router(coonfig-packet-flow-filter 1)#destination 5.6.7.8
Router(coonfig-packet-flow-filter 1)#src-port 123
Router(coonfig-packet-flow-filter 1)#dst-port 456
Router(coonfig-packet-flow-filter 1)#protocol 17
Router(coonfig-packet-flow-filter 1)#enable
Router(coonfig-packet-flow-filter 1)#exit
Router(config)#packet-flow activate
Router(config)#exit
Router#
```

This example displays whether or not the packet flow filter is activated and whether the ring buffer is enabled or disabled.

```
Router> show packet-flow status
Packet Flow Debugger Status:
Activation: Yes
Ring Buffer: Disabled
```

This example displays the packet flow filter 1's settings.

```
Router> show packet-flow filter 1
Filter #1 Status:
  Activation: Yes
  Src IP: 1.2.3.4
  Dst IP: 5.6.7.8
  Host Configured: No
  Protocol: 17
  Src Port: 123
```

This example displays the details of a captured packet flow. In this case traffic matches and is dropped by firewall rule 3.

```
Router> show packet-flow buffer
#1 Tracking ID: 1
Feature: Firewall (type:IPTables)
Action: Drop
Pkt Info:
 Src :192.168.30.1:67
 Dst :255.255.255.255:68
 Protocol: 17
Feature Info:
 Matched 'Firewall' Rule #3

#2 Tracking ID: 2
Feature: Firewall (type:IPTables)
Action: Drop
Pkt Info:
 Src :192.168.30.1:67
 Dst :255.255.255.255:68
 Protocol: 17
Feature Info:
 Matched 'Firewall' Rule #3

#3 Tracking ID: 3
Feature: Firewall (type:IPTables)
Action: Drop
Pkt Info:
 Src :192.168.30.33:138
 Dst :192.168.30.255:138
 Protocol: 17
Feature Info:
 Matched 'Firewall' Rule #3

#4 Tracking ID: 4
Feature: Firewall (type:IPTables)
Action: Drop
Pkt Info:
 Src :172.23.6.248:0
 Dst :192.168.30.112:0
 Protocol: 1
Feature Info:
 Matched 'Firewall' Rule #3
```

This example activates the packet flow ring buffer feature.

```
Router> configure terminal
Router(config)#packet-flow ring-buffer activate
Router(config)#exit
Router#
```

# 50

# Maintenance Tools

Use the maintenance tool commands to check the conditions of other devices through the ZyWALL / USG. The maintenance tools can help you to troubleshoot network problems.

Here are maintenance tool commands that you can use in privilege mode.

**Table 222** Maintenance Tools Commands in Privilege Mode

| COMMAND | DESCRIPTION |
|---|---|
| packet-trace [interface *interface_name*] [[ip-proto\|ipv6-proto] \| *protocol_name* \| any}] [src-host {*ip* \| *hostname* \| any}] [dst-host {*ip* \| *hostname* \| any}] [port {<1..65535> \| any}] [file] [duration <1..3600>] [extension-filter *filter_extension*] | Sniffs traffic going through the specified interface with the specified protocol, source address, destination address, and/or port number.<br>If you specify `file`, the ZyWALL / USG dumps the traffic to / `packet_trace/packet_trace_interface`. Use FTP to retrieve the files (see Section 43.6 on page 340).<br>If you do not assign the duration, the ZyWALL / USG keeps dumping traffic until you use Ctrl-C.<br>Use the extension filter to extend the use of this command.<br>*protocol_name*: You can use the name, instead of the number, for some IP protocols, such as `tcp`, `udp`, `icmp`, and so on. The names consist of 1-16 alphanumeric characters or dashes (-). The first character cannot be a number.<br>*hostname*: You can use up to 252 alphanumeric characters, dashes (-), or periods (.). The first character cannot be a period.<br>*filter_extension*: You can use 1-256 alphanumeric characters, spaces, or '()+,/:=?;!*#@$_%.- characters. |
| traceroute {*ip* \| *hostname*} | Displays the route taken by packets to the specified destination. Use `Ctrl+c` to return to the prompt. |
| traceroute6 {*ipv6* \| *hostname*} | Displays the route taken by packets to the specified destination. Use `Ctrl+c` to return to the prompt. |
| [no] packet-capture activate | Performs a packet capture that captures network traffic going through the set interface(s). Studying these packet captures may help you identify network problems.<br>The `no` command stops the running packet capture on the ZyWALL / USG.<br>Note: Use the `packet-capture configure` command to configure the packet-capture settings before using this command. |
| packet-capture configure | Enters the sub-command mode. |
| duration <0..300> | Sets a time limit in seconds for the capture. The ZyWALL / USG stops the capture and generates the capture file when either this period of time has passed or the file reaches the size specified using the `files-size` command below. 0 means there is no time limit. |

**Table 222** Maintenance Tools Commands in Privilege Mode (continued)

| COMMAND | DESCRIPTION |
|---|---|
| file-suffix <*profile_name*> | Specifies text to add to the end of the file name (before the dot and filename extension) to help you identify the packet capture files. Modifying the file suffix also avoids making new capture files that overwrite existing files of the same name.<br>The file name format is “interface name-file suffix.cap”, for example “vlan2-packet-capture.cap”. |
| files-size <1..10000> | Specify a maximum size limit in megabytes for the total combined size of all the capture files on the ZyWALL, including any existing capture files and any new capture files you generate.<br>The ZyWALL / USG stops the capture and generates the capture file when either the file reaches this size or the time period specified ( using the duration command above) expires. |
| host-ip {*ip-address* \| *profile_name* \| any> | Sets a host IP address or a host IP address object for which to capture packets. any means to capture packets for all hosts. |
| host-port <0..65535> | If you set the IP Type to any, tcp, or udp using the proto-type command below, you can specify the port number of traffic to capture. |
| iface {add \| del} {*interface_name* \| *virtual_interface_name*} | Adds or deletes an interface or a virtual interface for which to capture packets to the capture interfaces list. |
| ip-version {ip\|ip6\|any} | Sets wether to capture IPv4 or IPv6 traffic. Any means to capture packets for all types of traffic. |
| proto-type {icmp \| icmp6 \| igmp \| igrp \| pim \| ah \| esp \| vrrp \| udp \| tcp \| any} | Sets the protocol of traffic for which to capture packets. any means to capture packets for all types of traffic. |
| snaplen <68..1512> | Specifies the maximum number of bytes to capture per packet. The ZyWALL / USG automatically truncates packets that exceed this size. As a result, when you view the packet capture files in a packet analyzer, the actual size of the packets may be larger than the size of captured packets. |
| storage <internal\|usbstorage> | Sets to have the ZyWALL / USG only store packet capture entries on the ZyWALL / USG (internal) or on a USB storage connected to the ZyWALL / USG. |
| ring-buffer <enable\|disable> | Enables or disables the ring buffer used as a temporary storage. |
| split-size <1..2048> | Specify a maximum size limit in megabytes for individual packet capture files. After a packet capture file reaches this size, the ZyWALL / USG starts another packet capture file. |
| Ping {*ipv4* \| *hostname*} [source *ipv4*] [size <0..65507>] [forever\| count <1..4096>] | Sends an ICMP ECHO_REQUEST to test the reachability of a host on an IPv4 network and to measure the round-trip time for a message sent from the originating host to the destination computer.<br>size: specifies the number of data bytes to be sent<br>count: Stop after sending this number of ECHO_REQUEST packets.<br>forever: keep sending ECHO_REQUEST packets until you use Ctrl+c to stop. |
| ping6{*ipv6* \| *hostname*} [source *ipv6*] [size <0..65527>] [forever\| count <1..4096>] [interface {*interface_name* \| *virtual_interface_name*}][extension *filter_extension*] | Sends an ICMP ECHO_REQUEST to test the reachability of a host on an IPv6 network and to measure the round-trip time for a message sent from the originating host to the destination computer.<br>*interface_name*: specifies interface through which to send the ECHO_REQUEST packets.<br>*filter_extension*: You can use 1-256 alphanumeric characters, spaces, or '()+,/:=?;!*#@$_%.- characters. |
| show packet-capture status | Displays whether a packet capture is ongoing. |

**Table 222** Maintenance Tools Commands in Privilege Mode (continued)

| COMMAND | DESCRIPTION |
|---|---|
| tracepath6 {*ipv6* \| *hostname*} | Displays the path MTU for the target address. |
| show ipv6 neighbor-list | Displays the ZyWALL / USG's IPv6 neighbors. |
| show packet-capture config | Displays current packet capture settings. |

Here are maintenance tool commands that you can use in configuration mode.

**Table 223** Maintenance Tools Commands in Configuration Mode

| COMMAND | DESCRIPTION |
|---|---|
| ipv6 neighbor flush {*ipv6* \| all} | Clears the specified IPv6 address or all IPv6 addresses from the IPv6 neighbor cache. |

# 50.1 Maintenance Command Examples

Some packet-trace command examples are shown below.

```
Router# packet-trace duration 3
tcpdump: listening on eth0
19:24:43.239798 192.168.1.10 > 192.168.1.1: icmp: echo request
19:24:43.240199 192.168.1.1 > 192.168.1.10: icmp: echo reply
19:24:44.258823 192.168.1.10 > 192.168.1.1: icmp: echo request
19:24:44.259219 192.168.1.1 > 192.168.1.10: icmp: echo reply
19:24:45.268839 192.168.1.10 > 192.168.1.1: icmp: echo request
19:24:45.269238 192.168.1.1 > 192.168.1.10: icmp: echo reply

6 packets received by filter
0 packets dropped by kernel
```

```
Router# packet-trace interface ge2 ip-proto icmp file extension-filter -s
-> 500 -n
tcpdump: listening on eth1
07:24:07.898639 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:24:07.900450 192.168.105.40 > 192.168.105.133: icmp: echo reply
07:24:08.908749 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:24:08.910606 192.168.105.40 > 192.168.105.133: icmp: echo reply

8 packets received by filter
0 packets dropped by kernel
```

```
Router# packet-trace interface ge2 ip-proto icmp file extension-filter
-> and src host 192.168.105.133 and dst host 192.168.105.40 -s 500 -n
tcpdump: listening on eth1
07:26:51.731558 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:26:52.742666 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:26:53.752774 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:26:54.762887 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)

8 packets received by filter
0 packets dropped by kernel
```

```
Router# traceroute www.zyxel.com
traceroute to www.zyxel.com (203.160.232.7), 30 hops max, 38 byte packets
 1  172.23.37.254  3.049 ms  1.947 ms  1.979 ms
 2  172.23.6.253  2.983 ms  2.961 ms  2.980 ms
 3  172.23.6.1  5.991 ms  5.968 ms  6.984 ms
 4  * * *
```

Here are maintenance tool commands that you can use in configure mode.

**Table 224** Maintenance Tools Commands in Configuration Mode

| COMMAND | DESCRIPTION |
|---|---|
| show arp-table | Displays the current Address Resolution Protocol table. |
| arp IP *mac_address* | Edits or creates an ARP table entry. |
| no arp *ip* | Removes an ARP table entry. |

The following example creates an ARP table entry for IP address 192.168.1.10 and MAC address 01:02:03:04:05:06. Then it shows the ARP table and finally removes the new entry.

```
Router# arp 192.168.1.10 01:02:03:04:05:06
Router# show arp-table
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.10             ether   01:02:03:04:05:06   CM                    ge1
172.23.19.254            ether   00:04:80:9B:78:00   C                     ge2
Router# no arp 192.168.1.10
Router# show arp-table
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.10                     (incomplete)                              ge1
172.23.19.254            ether   00:04:80:9B:78:00   C                     ge2
```

## 50.1.1 Packet Capture Command Example

The following examples show how to configure packet capture settings and perform a packet capture. First you have to check whether a packet capture is running. This example shows no other packet capture is running. Then you can also check the current packet capture settings.

```
Router(config)# show packet-capture status
capture status: off
Router(config)#
Router(config)# show packet-capture config
iface: None
ip-version: any
proto-type: any
host-port: 0
host-ip: any
file-suffix: -packet-capture
snaplen: 1500
duration: 0
file-size: 10
split-size: 2
ring-buffer: 0
storage: 0
```

Then configure the following settings to capture packets going through the ZyWALL / USG's WAN1 interface only.

- IP address: any
- Host IP: any
- Host port: any (then you do not need to configure this setting)
- File suffix: Example
- File size: 10 megabytes
- Duration: 150 seconds
- Save the captured packets to: USB storage device
- Use the ring buffer: no
- The maximum size of a packet capture file: 100 megabytes

```
Router(config)# packet-capture configure
Router(packet-capture)# iface add wan1
Router(packet-capture)# ip-type any
Router(packet-capture)# host-ip any
Router(packet-capture)# file-suffix Example
Router(packet-capture)# files-size 10
Router(packet-capture)# duration 150
Router(packet-capture)# storage usbstorage
Router(packet-capture)# ring-buffer disable
Router(packet-capture)# split-size 100
Router(packet-capture)#
```

Exit the sub-command mode and have the ZyWALL / USG capture packets according to the settings you just configured.

```
Router(packet-capture)# exit
Router(config)# packet-capture activate
Router(config)#
```

Manually stop the running packet capturing.

```
Router(config)# no packet-capture activate
Router(config)#
```

Check current packet capture status and list all stored packet captures.

```
Router(config)# show packet-capture status
capture status: off
Router(config)# dir /packet_trace
File Name                                          Size     Modified Time
=============================================================================
wan1-Example.cap                                   575160   2009-11-24 09:06:59
Router(config)#
```

You can use FTP to download a capture file. Open and study it using a packet analyzer tool (for example, Ethereal or Wireshark).

# 51

# Watchdog Timer

This chapter provides information about the ZyWALL / USG's watchdog timers.

## 51.1 Hardware Watchdog Timer

The hardware watchdog has the system restart if the hardware fails.

**The `hardware-watchdog-timer` commands are for support engineers. It is recommended that you not modify the hardware watchdog timer settings.**

**Table 225** hardware-watchdog-timer Commands

| COMMAND | DESCRIPTION |
|---|---|
| `[no] hardware-watchdog-timer <4..37>` | Sets how long the system's hardware can be unresponsive before resetting. The `no` command turns the timer off. |
| `show hardware-watchdog-timer status` | Displays the settings of the hardware watchdog timer. |

## 51.2 Software Watchdog Timer

The software watchdog has the system restart if the core firmware fails.

**The `software-watchdog-timer` commands are for support engineers. It is recommended that you not modify the software watchdog timer settings.**

**Table 226** software-watchdog-timer Commands

| COMMAND | DESCRIPTION |
|---|---|
| `[no] software-watchdog-timer <10..600>` | Sets how long the system's core firmware can be unresponsive before resetting. The `no` command turns the timer off. |
| `show software-watchdog-timer status` | Displays the settings of the software watchdog timer. |
| `show software-watchdog-timer log` | Displays a log of when the software watchdog timer took effect. |

# 51.3 Application Watchdog

The application watchdog has the system restart a process that fails. These are the `app-watchdog` commands. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

**Table 227** app-watchdog Commands

| COMMAND | DESCRIPTION |
|---|---|
| `[no] app-watch-dog activate` | Turns the application watchdog timer on or off. |
| `[no] app-watch-dog auto-recover` | If app-watch-dog detects a dead process, app-watch-dog will try to auto recover. The `no` command turns off auto-recover |
| `[no] app-watch-dog console-print {always\|once}` | Display debug messages on the console (every time they occur or once). The `no` command changes the setting back to the default. |
| `[no] app-watch-dog cpu-threshold min <1..100> max <1..100>` | Sets the percentage thresholds for sending a CPU usage alert. The ZyWALL / USG starts sending alerts when CPU usage exceeds the maximum (the second threshold you enter). The ZyWALL / USG stops sending alerts when the CPU usage drops back below the minimum threshold (the first threshold you enter). The `no` command changes the setting back to the default. |
| `[no] app-watch-dog interval <6..300>` | Sets how frequently (in seconds) the ZyWALL / USG checks the system processes. The `no` command changes the setting back to the default. |
| `[no] app-watch-dog retry-count <1..5>` | Set how many times the ZyWALL / USG is to re-check a process before considering it failed. The `no` command changes the setting back to the default. |
| `[no] app-watch-dog alert` | Has the ZyWALL / USG send an alert the user when the system is out of memory or disk space. |
| `[no] app-watch-dog disk-threshold min <1..100> max <1..100>` | Sets the percentage thresholds for sending a disk usage alert. The ZyWALL / USG starts sending alerts when disk usage exceeds the maximum (the second threshold you enter). The ZyWALL / USG stops sending alerts when the disk usage drops back below the minimum threshold (the first threshold you enter). The `no` command changes the setting back to the default. |
| `[no] app-watch-dog mem-threshold min <1..100> max <1..100>` | Sets the percentage thresholds for sending a memory usage alert. The ZyWALL / USG starts sending alerts when memory usage exceeds the maximum (the second threshold you enter). The ZyWALL / USG stops sending alerts when the memory usage drops back below the minimum threshold (the first threshold you enter). The `no` command changes the setting back to the default. |
| `app-watch-dog reboot-log flush` | Flushes the reboot log record. |
| `[no] app-watch-dog sys-reboot` | If auto recover fail reaches the maximum retry count, app-watch-dog reboots the device. The `no` command turns off system auto reboot. |
| `show app-watch-dog config` | Displays the application watchdog timer settings. |
| `show app-watch-dog monitor-list` | Display the list of applications that the application watchdog is monitoring. |
| `show app-watch-dog reboot-log` | Displays the application watchdog reboot log. |

### 51.3.1 Application Watchdog Commands Example

The following example displays the application watchdog configuration and lists the processes that the application watchdog is monitoring.

```
Application Watch Dog Setting:
  activate: yes
    alert: yes
  console print: always
  retry count: 3
  auto recover: yes
  system reboot: yes
  interval: 60 seconds
  mem threshold: 80% ~ 90%
    cpu threshold: 80% ~ 90%
    disk threshold: 80% ~ 90%
Router(config)# show app-watch-dog monitor-list
#app_name      min_process_count      max_process_count(-1 unlimited) recover_enable  recover_reboot  recover_always  recover_max_try_count   recover_max_fail_count
uamd                1                          -1                1               2               1                       1                       3
firewalld           1                          -1                0               1               1                       1                       3
policyd             1                          -1                1               1               1                       1                       3
contfltd            1                          -1                1               1               1                       1                       3
classify            1                          -1                0               1               1                       1                       3
ospfd               1                          -1                0               1               1                       1                       3
ripd                1                          -1                0               1               1                       1                       3
resd                1                          -1                0               1               1                       1                       3
zyshd_wd            1                          -1                0               1               1                       1                       3
zyshd               1                          -1                0               0               1                       1                       3
httpd               1                          -1                1               1               1                       1                       3
dhcpd               1                          -1                1               1               1                       1                       3
sshipsecpm          1                          -1                1               1               1                       1                       3
zylogd              1                          -1                0               1               1                       1                       3
syslog-ng           1                          -1                0               1               1                       1                       3
zylogger            1                          -1                0               1               1                       1                       3
ddns_had            1                          -1                0               1               1                       1                       3
tpd                 1                          -1                0               1               1                       1                       3
wdtd                1                          -1                0               1               1                       1                       3
zebra               1                          -1                0               1               1                       1                       3
link_updown         1                          -1                0               1               1                       1                       3
fauthd              1                          -1                0               1               1                       1                       3
pro                 1                          -1                0               1               1                       1                       3
signal_wrapper      1                          -1                0               1               1                       1                       3
asd                 1                          -1                0               1               1                       1                       3
ctipd.bin           1                          -1                1               1               1                       1                       3
ipmonitord          1                          -1                0               1               1                       1                       3
```

# List of Commands (Alphabetical)

This section lists the commands and sub-commands in alphabetical order. Commands and subcommands appear at the same level.


Ping {*ipv4* | *hostname*} [source *ipv4*] [size <0..65507>] [forever| count <1..4096>] .....378
[no] {anti-virus | personal-firewall} activate .....306
[no] {*ipv4* | *ipv4_cidr* | *ipv4_range* | *wildcard_domainname* | *tld*} .....239
[no] aaa authentication default *member1* [*member2*] [*member3*] [*member4*] .....291
[no] aaa authentication *profile-name* .....291
[no] aaa authentication *profile-name member1* [*member2*] [*member3*] [*member4*] .....292
[no] aaa group server ad *group-name* .....287
[no] aaa group server ldap *group-name* .....288
[no] aaa group server radius *group-name* .....289
[no] access-page color-window-background .....316
[no] access-page message-text *message* .....316
[no] account {pppoe | pptp} *profile_name* .....300
[no] account cellular *profile_name* .....301
[no] account *profile_name* .....92
[no] account *profile_name* .....94
[no] action-block {login|message|audio|video|file-transfer} .....201
[no] action-block {login|message|audio|video|file-transfer} .....202
[no] action-block {login|message|audio|video|file-transfer} .....204
[no] activate .....103
[no] activate .....163
[no] activate .....166
[no] activate .....166
[no] activate .....172
[no] activate .....184
[no] activate .....188
[no] activate .....201
[no] activate .....202
[no] activate .....204
[no] activate .....211
[no] activate .....219
[no] activate .....248
[no] activate .....262
[no] activate .....270
[no] activate .....331
[no] activate .....361
[no] activate .....59
[no] additional-ddns-options .....139
[no] address *address6_object* .....167
[no] address *address_object* .....166
[no] address6-object *object_name* {*ipv6_address* | *ipv6_range* | *ipv6_subnet*} .....274
[no] address6-object *object_name* interface-ip *interface* {dhcpv6 | link-local | slaac | static} {*addr_index*} .....274
[no] address6-object *object_name* interface-subnet *interface* {dhcpv6 | slaac | static} {*addr_index*} .....274
[no] address-object *object_name* .....276
[no] ad-server basedn *basedn* .....285
[no] ad-server binddn *binddn* .....286
[no] ad-server cn-identifier *uid* .....286
[no] ad-server host *ad_server* .....286
[no] ad-server password *password* .....286

[no] ad-server password-encrypted *password* .....286
[no] ad-server port *port_no* .....286
[no] ad-server search-time-limit *time* .....286
[no] ad-server ssl .....286
[no] agreement-url *url* .....173
[no] ampdu .....103
[no] ampdu .....104
[no] ampdu .....60
[no] amsdu .....103
[no] amsdu .....104
[no] amsdu .....61
[no] answer-rings .....331
[no] anti-spam {smtp | pop3} defaultport *port_number* .....249
[no] anti-spam activate .....247
[no] anti-spam black-list [*rule_number*] e-mail *email* {activate|deactivate} .....251
[no] anti-spam black-list [*rule_number*] ip-address *ip subnet_mask* {activate|deactivate} 251
[no] anti-spam black-list [*rule_number*] mail-header *mail-header mail-header-value* {activate|deactivate} .....251
[no] anti-spam black-list [*rule_number*] subject *subject* {activate|deactivate} .....251
[no] anti-spam black-list activate .....251
[no] anti-spam dnsbl activate .....253
[no] anti-spam ip-reputation activate .....249
[no] anti-spam ip-reputation private-check activate .....249
[no] anti-spam mail-content activate .....249
[no] anti-spam statistics collect .....255
[no] anti-spam virus-outbreak activate .....249
[no] anti-spam white-list [*rule_number*] e-mail *email* {activate|deactivate} .....251
[no] anti-spam white-list [*rule_number*] ip-address *ip subnet_mask* {activate|deactivate} 251
[no] anti-spam white-list [*rule_number*] mail-header *mail-header mail-header-value* {activate|deactivate} .....251
[no] anti-spam white-list [*rule_number*] subject *subject* {activate|deactivate} .....251
[no] anti-spam white-list activate .....251
[no] anti-spam xheader {mail-content | virus-outbreak} *xheader-name xheader-value* .....249
[no] anti-spam xheader {white-list | black-list} *mail-header mail-header-value* .....251
[no] anti-spam xheader dnsbl *mail-header mail-header-value* .....254
[no] anti-spam xheader query-timeout *xheader-name xheader-value* .....249
[no] anti-virus activate .....210
[no] anti-virus *anti_virus_software_name* detect-auto-protection {enable | disable | ignore} 306
[no] anti-virus black-list activate .....212
[no] anti-virus black-list file-pattern *av_file_pattern* {activate|deactivate} .....213
[no] anti-virus eicar activate .....210
[no] anti-virus skip-unknown-file-type activate .....210
[no] anti-virus statistics collect .....215
[no] anti-virus update auto .....214
[no] anti-virus white-list activate .....212
[no] anti-virus white-list file-pattern *av_file_pattern* {activate|deactivate} .....212
[no] apn *access_point_name* .....301
[no] app activate .....205
[no] app highest sip bandwidth priority .....205
[no] app other log [alert] .....203
[no] app other *protocol_name* bandwidth-graph .....205
[no] app *protocol_name* activate .....200
[no] app *protocol_name* allowport <1..65535> .....200
[no] app *protocol_name* bandwidth-graph .....205
[no] app *protocol_name* bwm .....200
[no] app *protocol_name* defaultport <1..65535> .....200
[no] app *protocol_name* log [alert] .....200
[no] application *application_object* .....188

[no] application forbidden-process *process_name* .....307
[no] application trusted-process *process_name* .....307
[no] app-watch-dog activate .....384
[no] app-watch-dog alert .....384
[no] app-watch-dog auto-recover .....384
[no] app-watch-dog console-print {always|once} .....384
[no] app-watch-dog cpu-threshold min <1..100> max <1..100> .....384
[no] app-watch-dog disk-threshold min <1..100> max <1..100> .....384
[no] app-watch-dog interval <6..300> .....384
[no] app-watch-dog mem-threshold min <1..100> max <1..100> .....384
[no] app-watch-dog retry-count <1..5> .....384
[no] app-watch-dog sys-reboot .....384
[no] area IP [{stub | nssa}] .....131
[no] area IP authentication .....131
[no] area IP authentication authentication-key *authkey* .....131
[no] area IP authentication message-digest .....131
[no] area IP authentication message-digest-key <1..255> md5 *authkey* .....131
[no] area IP virtual-link IP .....131
[no] area IP virtual-link IP authentication .....131
[no] area IP virtual-link IP authentication authentication-key *authkey* .....131
[no] area IP virtual-link IP authentication message-digest .....131
[no] area IP virtual-link IP authentication message-digest-key <1..255> md5 *authkey* ....131
[no] area IP virtual-link IP authentication same-as-area .....131
[no] area IP virtual-link IP authentication-key *authkey* .....131
[no] authentication {chap-pap | chap | pap | mschap | mschap-v2} .....110
[no] authentication {chap-pap | chap | pap | mschap | mschap-v2} .....300
[no] authentication {force | required} .....172
[no] authentication {force | required} .....270
[no] authentication {none | pap | chap} .....301
[no] authentication {string *password* | ah-md5 *password*} .....262
[no] authentication mode {md5 | text} .....130
[no] authentication string *authkey* .....130
[no] auto-destination .....121
[no] auto-disable .....121
[no] backmx .....139
[no] backup-custom *ip* .....138
[no] backup-iface *interface_name* .....139
[no] band {auto|wcdma|gsm} .....94
[no] bandwidth <1..1048576> priority <1..1024> [maximize-bandwidth-usage] .....121
[no] bandwidth <1..1048576> priority <1..1024> [maximize-bandwidth-usage] .....122
[no] bandwidth excess-usage .....201
[no] bandwidth excess-usage .....202
[no] bandwidth excess-usage .....204
[no] bind *interface_name* .....92
[no] block .....134
[no] block-ack .....103
[no] block-ack .....104
[no] block-ack .....61
[no] block-intra .....104
[no] block-intra .....64
[no] budget active .....95
[no] budget active .....96
[no] budget data active {download-upload|download|upload} <1..100000> .....95
[no] budget data active {download-upload|download|upload} <1..100000> .....96
[no] budget time active <1..672> .....95
[no] budget time active <1..672> .....96
[no] bwm activate .....120
[no] bwm activate .....205
[no] bypass {ip-reputation | mail-content | virus-outbreak} .....248

[no] bypass {white-list | black-list | dnsbl} ..... 248
[no] bypass {white-list | black-list} ..... 211
[no] bypass-firewall activate ..... 153
[no] cache-clean activate ..... 188
[no] case-sensitive ..... 287
[no] case-sensitive ..... 289
[no] case-sensitive ..... 290
[no] client-identifier *mac_address* ..... 82
[no] client-name *host_name* ..... 82
[no] clock daylight-saving ..... 318
[no] clock saving-interval begin {apr|aug|dec|feb|jan|jul|jun|mar|may|nov|oct|sep}
{1|2|3|4|last} {fri|mon|sat|sun|thu|tue|wed} *hh:mm* end
{apr|aug|dec|feb|jan|jul|jun|mar|may|nov|oct|sep} {1|2|3|4|last}
{fri|mon|sat|sun|thu|tue|wed} *hh:mm* offset ..... 318
[no] clock time-zone {-|+*hh*} ..... 318
[no] cnm-agent acs password <password for ACS connection request> ..... 333
[no] cnm-agent acs username <username for ACS connection request> ..... 333
[no] cnm-agent activate ..... 332
[no] cnm-agent auth activate ..... 333
[no] cnm-agent manager *url* ..... 332
[no] cnm-agent password <TR-069 password> ..... 333
[no] cnm-agent periodic-inform activate ..... 332
[no] cnm-agent username <TR-069 username> ..... 333
[no] compression {yes | no} ..... 300
[no] connection-id *connection_id* ..... 301
[no] connectivity {nail-up | dial-on-demand} ..... 93
[no] connectivity-check continuous-log activate ..... 354
[no] connectivity-check continuous-log activate ..... 88
[no] connlimit max-per-host <1..8192> ..... 161
[no] connlimit6 max-per-host <1..8192> ..... 162
[no] console baud *baud_rate* ..... 318
[no] content-filter active ..... 238
[no] content-filter block message *message* ..... 238
[no] content-filter block redirect *redirect_url* ..... 238
[no] content-filter default block ..... 238
[no] content-filter license *license* ..... 238
[no] content-filter license *license* ..... 239
[no] content-filter policy *policy_number address schedule filtering_profile* ..... 238
[no] content-filter profile *filtering_profile* ..... 239
[no] content-filter profile *filtering_profile* commtouch-url category {category_name} ... 241
[no] content-filter profile *filtering_profile* custom ..... 239
[no] content-filter profile *filtering_profile* custom activex ..... 239
[no] content-filter profile *filtering_profile* custom cookie ..... 239
[no] content-filter profile *filtering_profile* custom java ..... 239
[no] content-filter profile *filtering_profile* custom proxy ..... 240
[no] content-filter profile *filtering_profile* custom trust-allow-features ..... 240
[no] content-filter profile *filtering_profile* custom trust-only ..... 240
[no] content-filter profile *filtering_profile* url category {category_name} ..... 240
[no] content-filter profile *filtering_profile* url url-server ..... 241
[no] content-filter service-timeout *service_timeout* ..... 241
[no] content-filter statistics collect ..... 242
[no] content-filter -timeout *_timeout* ..... 238
[no] content-filter -timeout *_timeout* ..... 242
[no] corefile copy usb-storage ..... 102
[no] crypto ignore-df-bit ..... 180
[no] crypto map *map_name* ..... 181
[no] crypto *map_name* ..... 184
[no] crypto *profile_name* ..... 134
[no] ctmatch {dnat | snat} ..... 163

[no] ctsrts <0..2347> ..... 60
[no] ctsrts <256..2346> ..... 103
[no] custom *ip* ..... 138
[no] deactivate ..... 121
[no] deactivate ..... 122
[no] default-router *ip* ..... 82
[no] description *description* ..... 121
[no] description *description* ..... 122
[no] description *description* ..... 163
[no] description *description* ..... 166
[no] description *description* ..... 167
[no] description *description* ..... 172
[no] description *description* ..... 188
[no] description *description* ..... 262
[no] description *description* ..... 267
[no] description *description* ..... 270
[no] description *description* ..... 277
[no] description *description* ..... 281
[no] description *description* ..... 307
[no] description *description* ..... 331
[no] description *description* ..... 74
[no] description *description* ..... 75
[no] description *description* ..... 82
[no] destination {*address6_object*|any} ..... 122
[no] destination {*address_object* | *group_name*} ..... 172
[no] destination {*address_object* | *group_name*} ..... 270
[no] destination {*address_object*|any} ..... 121
[no] destination {any|*ipv4*} ..... 373
[no] destination *profile_name* ..... 201
[no] destination *profile_name* ..... 202
[no] destination *profile_name* ..... 204
[no] destinationip *address_object* ..... 163
[no] destinationip6 *address_object* ..... 164
[no] device-ha activate ..... 258
[no] device-ha ap-mode authentication {string *key* | ah-md5 *key*} ..... 260
[no] device-ha ap-mode backup sync authentication password *password* ..... 260
[no] device-ha ap-mode backup sync auto ..... 260
[no] device-ha ap-mode backup sync from *master_address* port *port* ..... 260
[no] device-ha ap-mode backup sync interval <1..1440> ..... 260
[no] device-ha ap-mode *interface_name* activate ..... 260
[no] device-ha ap-mode *interface_name* manage-ip *ip subnet_mask* ..... 260
[no] device-ha ap-mode master sync authentication password *password* ..... 260
[no] device-ha ap-mode preempt ..... 259
[no] device-ha sync authentication password *password* ..... 263
[no] device-ha sync auto ..... 263
[no] device-ha sync from {*hostname* | *ip*} ..... 263
[no] device-ha sync interval <5..1440> ..... 263
[no] device-ha sync now ..... 263
[no] device-ha sync port <1..65535> ..... 263
[no] device-ha vrrp-group *vrrp_group_name* ..... 262
[no] diag-info copy usb-storage ..... 102
[no] dialing-type {tone | pulse} ..... 110
[no] dial-string *isp_dial_string* ..... 301
[no] dial-timeout <30..120> ..... 110
[no] disable-dfs-switch ..... 59
[no] domainname *domain_name* ..... 317
[no] domain-name *domain_name* ..... 83
[no] dot11n-disable-coexistence ..... 60
[no] dot1x-eap ..... 66

[no] downstream <0..1048576> .....100
[no] downstream <0..1048576> .....74
[no] downstream <0..1048576> .....75
[no] dpd .....179
[no] dscp {any | <0..63>} .....121
[no] dscp {any | <0..63>} .....122
[no] dscp class {default | *dscp_class*} .....121
[no] dscp class {default | *dscp_class*} .....122
[no] dst-port {any|<1..65535>} .....373
[no] duplex <full | half> .....90
[no] enable .....309
[no] enable .....373
[no] encryption {nomppe | mppe-40 | mppe-128} .....301
[no] eps <1..8> *eps_object_name* .....172
[no] eps <1..8> *eps_object_name* .....270
[no] eps <1..8> *eps_profile_name* .....188
[no] eps activate .....172
[no] eps activate .....188
[no] eps activate .....270
[no] eps failure-messages *failure_messages* .....306
[no] eps periodical-check <1..1440> .....172
[no] eps periodical-check <1..1440> .....189
[no] eps periodical-check <1..1440> .....270
[no] eps periodical-check activate .....189
[no] eps profile *profile_name* .....306
[no] eps rename *profile_name new_profile_name* .....309
[no] error-url *url* .....170
[no] fall-back .....179
[no] file-decompression [unsupported destroy] .....211
[no] file-info file-path *file_path* .....307
[no] file-info file-path *file_path* {eq | gt | lt | ge | le | neq} file-size <1..1073741824> 307
[no] file-info file-path *file_path* {eq | gt | lt | ge | le | neq} file-size <1..1073741824> {eq | gt | lt | ge | le | neq} file-version *file_version* .....307
[no] file-info file-path *file_path* {eq | gt | lt | ge | le | neq} file-version *file_version* 307
[no] firewall activate .....161
[no] firewall activate .....162
[no] firewall asymmetrical-route activate .....161
[no] firewall6 asymmetrical-route activate .....163
[no] first-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns} | ZyWALL} .....83
[no] first-wins-server *ip* .....83
[no] flood-detection {tcp-flood | udp-flood | ip-flood | icmp-flood} {activate | log [alert] | block} .....221
[no] *forbid_hosts* .....239
[no] force .....172
[no] force .....270
[no] force vlan .....56
[no] force-auth activate .....269
[no] frag <256..2346> .....103
[no] frag <256..2346> .....60
[no] from *zone_name* .....201
[no] from *zone_name* .....202
[no] from *zone_name* .....204
[no] from *zone_object* .....164
[no] from *zone_object* .....211
[no] from-zone *zone_object* .....248
[no] from-zone *zone_profile* .....219
[no] groupname *groupname* .....267

[no] groupname *groupname* ..... 267
[no] ha-iface *interface_name* ..... 139
[no] hardware-address *mac_address* ..... 82
[no] hardware-watchdog-timer <4..37> ..... 383
[no] hide ..... 104
[no] hide ..... 64
[no] host {any|*ipv4*} ..... 373
[no] host *hostname* ..... 138
[no] host *ip* ..... 82
[no] hostname *hostname* ..... 317
[no] htprotection ..... 62
[no] http-inspection {http-xxx} action {drop | reject-sender | reject-receiver | reject-both}} 222
[no] http-inspection {http-xxx} activate ..... 222
[no] icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} activate ..... 222
[no] idle <0..360> ..... 110
[no] idle <0..360> ..... 300
[no] idle <0..360> ..... 301
[no] idle-detection [timeout <1..60>] ..... 173
[no] idp ..... 218
[no] idp {signature | system-protect} update auto ..... 231
[no] idp statistics collect ..... 232
[no] inbound-dscp-mark {<0..63> | class {default | *dscp_class*}} ..... 201
[no] inbound-dscp-mark {<0..63> | class {default | *dscp_class*}} ..... 202
[no] inbound-dscp-mark {<0..63> | class {default | *dscp_class*}} ..... 204
[no] in-dnat activate ..... 182
[no] infected-action {destroy | send-win-msg} ..... 211
[no] initial-string *initial_string* ..... 110
[no] initial-string *initial_string* ..... 331
[no] in-snat activate ..... 182
[no] interface {*num*|*interface-name*} ..... 115
[no] interface *ap_interface* ..... 104
[no] interface *interface_name* ..... 121
[no] interface *interface_name* ..... 123
[no] interface *interface_name* ..... 134
[no] interface *interface_name* ..... 262
[no] interface *interface_name* ..... 74
[no] interface *interface_name* ..... 75
[no] interface *interface_name* ..... 94
[no] interface *tunnel_iface* ..... 100
[no] interface-group *group-name* ..... 114
[no] internal-page-customization ..... 173
[no] internal-welcome-url *url* ..... 171
[no] ip address dhcp ..... 74
[no] ip address dhcp ..... 75
[no] ip address *ip subnet_mask* ..... 104
[no] ip address *ip subnet_mask* ..... 74
[no] ip address *ip subnet_mask* ..... 75
[no] ip ddns profile *profile_name* ..... 138
[no] ip dhcp pool *profile_name* ..... 81
[no] ip dhcp-pool *profile_name* ..... 83
[no] ip dns server a-record *fqdn w.x.y.z* ..... 319
[no] ip dns server mx-record *domain_name* {*w.x.y.z*|*fqdn*} ..... 320
[no] ip dns server zone-forwarder {<1..32>|append|insert <1..32>} {*domain_zone_name*|*} interface *interface_name* ..... 320
[no] ip ftp server ..... 327
[no] ip ftp server cert *certificate_name* ..... 327
[no] ip ftp server port <1..65535> ..... 327

[no] ip ftp server tls-required ..... 327
[no] ip gateway *ip* ..... 74
[no] ip gateway *ip* ..... 75
[no] ip gateway *ip* [metric <0..15>] ..... 104
[no] ip helper-address *ip* ..... 83
[no] ip http authentication *auth_method* ..... 322
[no] ip http port <1..65535> ..... 322
[no] ip http secure-port <1..65535> ..... 322
[no] ip http secure-server ..... 322
[no] ip http secure-server auth-client ..... 322
[no] ip http secure-server cert *certificate_name* ..... 323
[no] ip http secure-server force-redirect ..... 323
[no] ip http server ..... 323
[no] ip load-balancing link-sticking activate ..... 117
[no] ip load-balancing link-sticking timeout *timeout* ..... 117
[no] ip ospf authentication-key *password* ..... 87
[no] ip ospf cost <1..65535> ..... 87
[no] ip ospf dead-interval <1..65535> ..... 87
[no] ip ospf hello-interval <1..65535> ..... 87
[no] ip ospf priority <0..255> ..... 87
[no] ip ospf retransmit-interval <1..65535> ..... 87
[no] ip rip {send | receive} version <1..2> ..... 86
[no] ip rip v2-broadcast ..... 86
[no] ip route {*w.x.y.z*} {*w.x.y.z*} {*interface*|*w.x.y.z*} <0..127> ..... 126
[no] ip route control-virtual-server-rules activate ..... 126
[no] ip ssh server ..... 325
[no] ip ssh server cert *certificate_name* ..... 325
[no] ip ssh server port <1..65535> ..... 325
[no] ip ssh server v1 ..... 325
[no] ip telnet server ..... 326
[no] ip telnet server port <1..65535> ..... 326
[no] ip-select {iface | auto | custom} ..... 138
[no] ip-select-backup {iface | auto | custom} ..... 138
[no] ipv6 activate ..... 334
[no] ipv6 address *dhcp6_profile dhcp6_suffix_128* ..... 93
[no] ipv6 dhcp6 address-request ..... 93
[no] ipv6 dhcp6 rapid-commit ..... 93
[no] ipv6 dhcp6-request-object *dhcp6_profile* ..... 93
[no] ipv6 enable ..... 93
[no] ipv6 metric <0..15> ..... 93
[no] ipv6 nd ra accept ..... 93
[no] isakmp policy *policy_name* ..... 179
[no] item as-report ..... 362
[no] item av-report ..... 362
[no] item cf-report ..... 362
[no] item cpu-usage ..... 362
[no] item idp-report ..... 362
[no] item mem-usage ..... 362
[no] item port-usage ..... 362
[no] item session-usage ..... 362
[no] item traffic-report ..... 362
[no] join *interface_name* ..... 109
[no] *keyword* ..... 240
[no] l2tp-over-ipsec activate; ..... 195
[no] l2tp-over-ipsec first-dns-server {*ip* | *interface_name*} {1st-dns|2nd-dns|3rd-dns}|
{*ppp_interface*|aux}{1st-dns|2nd-dns}} ..... 196
[no] l2tp-over-ipsec first-wins-server *ip* ..... 196
[no] l2tp-over-ipsec keepalive-timer <1..180> ..... 196
[no] l2tp-over-ipsec second-dns-server {*ip* | *interface_name*} {1st-dns|2nd-dns|3rd-dns}|

{*ppp_interface*|aux}{1st-dns|2nd-dns}} .....196
[no] l2tp-over-ipsec second-wins-server *ip* .....196
[no] l2tp-over-ipsec user user_name .....196
[no] ldap-server basedn *basedn* .....286
[no] ldap-server binddn *binddn* .....286
[no] ldap-server cn-identifier *uid* .....286
[no] ldap-server host *ldap_server* .....286
[no] ldap-server password *password* .....286
[no] ldap-server password-encrypted *password* .....286
[no] ldap-server port *port_no* .....286
[no] ldap-server search-time-limit *time* .....286
[no] ldap-server ssl .....286
[no] lease {<0..365> [<0..23> [<0..59>]] | infinite} .....83
[no] limit <0..8192> .....166
[no] limit <0..8192> .....167
[no] listen-interface *interface_name* .....153
[no] local-address <*ip*> .....97
[no] local-address *ip* .....93
[no] log [alert] .....164
[no] log [alert] .....201
[no] log [alert] .....202
[no] log [alert] .....204
[no] log [alert] .....211
[no] log [alert] .....248
[no] logging console .....358
[no] logging console category *module_name* .....358
[no] logging debug suppression .....355
[no] logging debug suppression interval <10..600> .....355
[no] logging mail <1..2> .....356
[no] logging mail <1..2> {send-log-to | send-alerts-to} *e_mail* .....357
[no] logging mail <1..2> address {*ip* | *hostname*} .....357
[no] logging mail <1..2> authentication .....357
[no] logging mail <1..2> authentication username *username* password *password* .....357
[no] logging mail <1..2> category *module_name* level {alert | all} .....357
[no] logging mail <1..2> port <1..65535> .....357
[no] logging mail <1..2> schedule {full | hourly} .....357
[no] logging mail <1..2> subject *subject* .....357
[no] logging syslog <1..4> .....356
[no] logging syslog <1..4> {disable | level normal | level all} .....356
[no] logging syslog <1..4> address {*ip* | *hostname*} .....356
[no] logging syslog <1..4> facility {local_1 | local_2 | local_3 | local_4 | local_5 | local_6 | local_7} .....356
[no] logging syslog <1..4> format {cef | vrpt} .....356
[no] logging system-log suppression .....354
[no] logging system-log suppression interval <10..600> .....354
[no] logging usb-storage .....101
[no] login-page color-background .....316
[no] login-page color-window-background .....316
[no] login-page message-text % *message* .....316
[no] login-url *url* .....171
[no] logout-ip *ipv4_address* .....171
[no] logout-url *url* .....171
[no] mac description *description2* .....68
[no] macfilter *macfilterprofile* .....64
[no] mail-from *e_mail* .....361
[no] mail-subject append date-time .....361
[no] mail-subject append system-name .....361
[no] mail-to-1 *e_mail* .....361
[no] mail-to-2 *e_mail* .....361

[no] mail-to-3 *e_mail* ..... 362
[no] mail-to-4 *e_mail* ..... 362
[no] mail-to-5 *e_mail* ..... 362
[no] manage-ip IP ..... 262
[no] match-action pop3 {forward | forward-with-tag} ..... 248
[no] match-action smtp {drop | forward | forward-with-tag} ..... 248
[no] message *eps_warning_message* ..... 309
[no] metric <0..15> ..... 74
[no] metric <0..15> ..... 75
[no] mss <536..1452> ..... 93
[no] mss <536..1460> ..... 74
[no] mss <536..1460> ..... 75
[no] mtu <576..1480> ..... 100
[no] mtu <576..1500> ..... 74
[no] mtu <576..1500> ..... 75
[no] mtu <576..2304> ..... 105
[no] multicast-to-unicast ..... 61
[no] mute ..... 331
[no] mx {*ip* | *domain_name*} ..... 139
[no] nail-up ..... 182
[no] nat-pmp activate ..... 154
[no] natt ..... 180
[no] negotiation auto ..... 90
[no] netbios-broadcast ..... 182
[no] network *interface* area IP ..... 131
[no] network *interface_name* ..... 130
[no] network *interface_name* ..... 86
[no] network *interface_name* area *ip* ..... 86
[no] network-extension {activate | ip-pool *address_object* | 1st-dns {*address_object* | *ip* } | 2nd-dns {*address_object* | *ip* } | 1st-wins {*address_object* | *ip* } | 2nd-wins {*address_object* | *ip* } | network *address_object*} ..... 189
[no] network-extension traffic-enforcement ..... 189
[no] network-selection {auto|home} ..... 95
[no] network-selection {auto|home} ..... 96
[no] next-hop {auto|gateway *address object* |interface *interface_name* |trunk *trunk_name*|tunnel *tunnel_name*} ..... 121
[no] next-hop {auto|gateway *gatewayv6* |interface *interface_name* |trunk *trunk_name*|tunnel *tunnel_name*} ..... 123
[no] ntp ..... 318
[no] ntp server {*fqdn*|*w.x.y.z*} ..... 318
[no] object-group address *group_name* ..... 276
[no] object-group *group_name* ..... 276
[no] object-group *group_name* ..... 281
[no] object-group service *group_name* ..... 280
[no] outbound-dscp-mark {<0..63> | class {default | *dscp_class*}} ..... 201
[no] outbound-dscp-mark {<0..63> | class {default | *dscp_class*}} ..... 203
[no] outbound-dscp-mark {<0..63> | class {default | *dscp_class*}} ..... 204
[no] outonly-interface *interface_name* ..... 130
[no] outonly-interface *interface_name* ..... 86
[no] out-snat activate ..... 182
[no] packet-capture activate ..... 377
[no] packet-flow activate ..... 374
[no] packet-flow ring-buffer activate ..... 374
[no] passive-interface *interface_name* ..... 130
[no] passive-interface *interface_name* ..... 130
[no] passive-interface *interface_name* ..... 86
[no] passive-interface *interface_name* ..... 87
[no] password *password* ..... 110
[no] password *password* ..... 300

[no] password *password* ..... 301
[no] personal-firewall *personal_firewall_software_name* detect-auto-protection {enable | disable | ignore} ..... 307
[no] phone-number *phone* ..... 110
[no] pin <*pin code*> ..... 97
[no] ping-check activate ..... 88
[no] policy controll-ipsec-dynamic-rules activate ..... 123
[no] policy controll-virtual-server-rules activate ..... 123
[no] policy override-direct-route activate ..... 123
[no] policy6 override-direct-route activate ..... 123
[no] policy-enforcement ..... 182
[no] port <0..65535> ..... 204
[no] port *interface_name* ..... 108
[no] port-speed {9600 | 19200 | 38400 | 57600 | 115200} ..... 110
[no] port-speed {9600 | 19200 | 38400 | 57600 | 115200} ..... 332
[no] preempt ..... 262
[no] priority <1..254> ..... 262
[no] protocol {any|<1..255>} ..... 373
[no] protocol {tcp | udp} ..... 204
[no] radius-server host *radius_server* auth-port *auth_port* ..... 287
[no] radius-server key *secret* ..... 287
[no] radius-server timeout *time* ..... 287
[no] reauth <30..30000> ..... 66
[no] redistribute {static | ospf} ..... 130
[no] redistribute {static | rip} ..... 130
[no] redistribute {static | rip} metric-type <1..2> metric <0..16777214> ..... 130
[no] remote-address <*ip*> ..... 97
[no] remote-address *ip* ..... 93
[no] replay-detection ..... 182
[no] report ..... 359
[no] report packet size statistics ..... 360
[no] reset-counter ..... 362
[no] role {master | backup} ..... 262
[no] Router(config-sso-primary)# ip <*w.x.y.z*> ..... 174
[no] router-id IP ..... 130
[no] rssi-thres ..... 59
[no] scan {http | ftp | imap4 | smtp | pop3} ..... 211
[no] scan {smtp | pop3} ..... 248
[no] scan-detection {icmp-sweep | icmp-filtered-sweep} {activate | log [alert] | block} 221
[no] scan-detection {ip-xxx} {activate | log [alert] | block} ..... 221
[no] scan-detection {tcp-xxx} {activate | log [alert] | block} ..... 221
[no] scan-detection {udp-xxx} {activate | log [alert] | block} ..... 221
[no] scan-detection open-port {activate | log [alert] | block} ..... 221
[no] schedule *profile_name* ..... 201
[no] schedule *profile_name* ..... 203
[no] schedule *profile_name* ..... 204
[no] schedule *schedule_name* ..... 172
[no] schedule *schedule_name* ..... 270
[no] schedule *schedule_object* ..... 122
[no] schedule *schedule_object* ..... 123
[no] schedule *schedule_object* ..... 164
[no] second-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns} | ZyWALL} ..... 83
[no] second-wins-server *ip* ..... 83
[no] security dot1x acct *ip* port <1..65535> ..... 105
[no] security dot1x activate ..... 105
[no] security dot1x auth *ip* port <1..65535> ..... 105
[no] security external acct *ip* port <1..65535> ..... 106
[no] security external auth *ip* port <1..65535> ..... 106
[no] server alternative-cn-identifier *uid* ..... 288

[no] server alternative-cn-identifier *uid* ..... 289
[no] server basedn *basedn* ..... 288
[no] server basedn *basedn* ..... 289
[no] server binddn *binddn* ..... 288
[no] server binddn *binddn* ..... 289
[no] server cn-identifier *uid* ..... 288
[no] server cn-identifier *uid* ..... 289
[no] server description *description* ..... 288
[no] server description *description* ..... 289
[no] server description *description* ..... 290
[no] server group-attribute <1-255> ..... 290
[no] server group-attribute *group-attribute* ..... 288
[no] server group-attribute *group-attribute* ..... 289
[no] server host *ad_server* ..... 288
[no] server host *ldap_server* ..... 289
[no] server host *radius_server* ..... 290
[no] server *ip* ..... 301
[no] server key *secret* ..... 290
[no] server password *password* ..... 288
[no] server password *password* ..... 289
[no] server port *port_no* ..... 288
[no] server port *port_no* ..... 289
[no] server search-time-limit *time* ..... 288
[no] server search-time-limit *time* ..... 289
[no] server ssl ..... 288
[no] server ssl ..... 289
[no] server timeout *time* ..... 290
[no] server-auth <1..2> ..... 66
[no] server-auth <1..2> activate ..... 66
[no] service {*service_name*|any} ..... 122
[no] service {*service_name*|any} ..... 123
[no] service *service_name* ..... 164
[no] service-name {*ip* | *hostname* | *service_name*} ..... 300
[no] service-object *object_name* ..... 280
[no] service-type {dyndns | dyndns_static | dyndns_custom | dynu-basic | dynu-premium | no-ip | peanut-hull | 3322-dyn | 3322-static | Selfhost | User custom} ..... 138
[no] session-limit activate ..... 166
[no] session-limit6 activate ..... 166
[no] session-url *url* ..... 171
[no] shutdown ..... 100
[no] shutdown ..... 74
[no] shutdown ..... 75
[no] signature *sid* activate ..... 220
[no] signature *sid* activate ..... 224
[no] smtp-auth activate ..... 361
[no] smtp-port <1..65535> ..... 361
[no] snat {outgoing-interface|pool {*address_object*}} ..... 122
[no] snmp-server ..... 329
[no] snmp-server community *community_string* {ro|rw} ..... 329
[no] snmp-server contact *description* ..... 329
[no] snmp-server enable {informs|traps} ..... 329
[no] snmp-server host {*w.x.y.z*} [*community_string*] ..... 329
[no] snmp-server location *description* ..... 329
[no] snmp-server port <1..65535> ..... 329
[no] software-watchdog-timer <10..600> ..... 383
[no] source {*address6_object*|any} ..... 123
[no] source {*address_object* | *group_name*} ..... 172
[no] source {*address_object* | *group_name*} ..... 270
[no] source {*address_object*|any} ..... 122

[no] source {any|*ipv4*} ..... 373
[no] source *profile_name* ..... 201
[no] source *profile_name* ..... 203
[no] source *profile_name* ..... 204
[no] sourceip *address_object* ..... 164
[no] sourceip6 *address_object* ..... 164
[no] sourceport {tcp|udp} {eq <1..65535>|range <1..65535> <1..65535>} ..... 164
[no] speed <100,10> ..... 90
[no] src-port {any|<1..65535>} ..... 373
[no] ssid-profile *wlan_interface_index ssid_profile* ..... 62
[no] sslvpn application *application_object* ..... 302
[no] sslvpn *profile_name* ..... 134
[no] sslvpn *tunnel_name* ..... 122
[no] starting-address *ip* pool-size <1..65535> ..... 83
[no] super ..... 103
[no] system default-snat ..... 115
[no] tcp-decoder {tcp-xxx} action {drop | reject-sender | reject-receiver | reject-both}} 222
[no] tcp-decoder {tcp-xxx} activate ..... 222
[no] terms-of-service ..... 171
[no] third-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns} | ZyWALL} ..... 83
[no] to {*zone_object*|ZyWALL} ..... 164
[no] to *zone_name* ..... 201
[no] to *zone_name* ..... 203
[no] to *zone_name* ..... 204
[no] to *zone_object* ..... 211
[no] to-zone *zone_object* ..... 248
[no] to-zone *zone_profile* ..... 219
[no] trigger <1..8> incoming *service_name* trigger *service_name* ..... 122
[no] *trust_hosts* ..... 240
[no] tunnel *tunnel_name* ..... 122
[no] udp-decoder {truncated-header | undersize-len | oversize-len} activate ..... 222
[no] upnp-igd activate ..... 154
[no] upstream <0..1048576> ..... 74
[no] upstream <0..1048576> ..... 75
[no] usb-storage activate ..... 101
[no] user *user_name* ..... 122
[no] user *user_name* ..... 123
[no] user *user_name* ..... 164
[no] user *user_name* ..... 166
[no] user *user_name* ..... 167
[no] user *user_name* ..... 189
[no] user *username* ..... 201
[no] user *username* ..... 203
[no] user *username* ..... 204
[no] user *username* ..... 267
[no] user *username* ..... 300
[no] user *username* ..... 301
[no] username *username* ..... 110
[no] username *username* password *password* ..... 138
[no] users idle-detection ..... 268
[no] users idle-detection timeout <1..60> ..... 268
[no] users lockout-period <1..65535> ..... 268
[no] users retry-count <1..99> ..... 268
[no] users retry-limit ..... 268
[no] users simultaneous-logon {administration | access} enforce ..... 268
[no] users simultaneous-logon {administration | access} limit <1..1024> ..... 268
[no] users update-lease automation ..... 268
[no] version <1..2> ..... 130
[no] vlan-id <1..4094> ..... 108

[no] vlan-support ....64
[no] vpn-concentrator *profile_name* ....183
[no] vpn-configuration-provision activate ....184
[no] vrid <1..254> ....262
[no] wan-iface *interface_name* ....139
[no] web-auth activate ....169
[no] webpage-encrypt ....303
[no] welcome-url <*url*> ....173
[no] welcome-url *url* ....171
[no] wildcard ....139
[no] windows-auto-update {enable | disable | ignore} ....308
[no] windows-registry *registry_key* {eq | gt | lt | ge | le | neq} *registry_value* ....308
[no] windows-security-patch *security_patch* ....308
[no] windows-service-pack <1..10> ....308
[no] wlan mac-filter activate ....107
[no] wlan mac-filter *mac_address* [description *description*] ....107
[no] wlan-macfilter-profile *macfilter_profile_name* ....67
[no] wlan-radio-profile *radio_profile_name* ....59
[no] wlan-security-profile *security_profile_name* ....65
[no] wlan-ssid-profile *ssid_profile_name* ....64
[no] wpa2-preauth ....66
[no] xauth type {server *xauth_method* | client name *username* password *password*} ....180
[no] zone *profile_name* ....134
[no]addersss6-object *object_name* interface-gateway *interface* { slaac | static} {*addr_index*} 274
[no]https activate ....138
[no]igmp activate ....80
{signature | anomaly | system-protect} activate ....218
{signature | anomaly | system-protect} activation ....218
| uint32 <0..4294967295> | ip *ipv4* [ *ipv4* [ *ipv4*]] | fqdn *fqdn* [ *fqdn* [ *fqdn*]] | text *text* | hex *hex* | vivc *enterprise_id hex_s* [*enterprise_id hex_s* ] | vivs *enterprise_id hex_s* [*enterprise_id hex_s* ] ....82
2g-basic-speed *wlan_2g_basic_speed* ....61
2g-channel *wireless_channel_2g* ....61
2g-mcs-speed {disable | *wlan_mcs_speed*} ....61
2g-multicast-speed *wlan_2g_support_speed* ....61
2g-support-speed {disable | *wlan_2g_support_speed*} ....61
5g-basic-speed *wlan_5g_basic_speed* ....61
5g-channel *wireless_channel_5g* ....61
5g-mcs-speed {disable | *wlan_mcs_speed*} ....61
5g-multicast-speed {*wlan_5g_basic_speed*} ....61
5g-support-speed {disable | *wlan_5g_support_speed*} ....62
aaa authentication [no] match-default-group ....292
aaa authentication rename *profile-name-old profile-name-new* ....291
aaa group server ad *group-name* ....287
aaa group server ad rename *group-name group-name* ....287
aaa group server ldap *group-name* ....288
aaa group server ldap rename *group-name group-name* ....288
aaa group server radius *group-name* ....290
aaa group server radius rename {*group-name-old*} *group-name-new* ....289
access {forward | drop | reject} ....201
access {forward | drop | reject} ....202
access {forward | drop | reject} ....204
access-page message-color {*color-rgb* | *color-name* | *color-number*} ....316
access-page title *title* ....316
access-page window-color {*color-rgb* | *color-name* | *color-number*} ....316
action {allow|deny|reject} ....163
activate ....179
activate ....181

address *ipv6_addr_prefix* .....74
address *ipv6_addr_prefix* .....75
address *ipv6_addr_prefix* .....77
address-object *object_name* {*ip* | *ip_range* | *ip_subnet* | interface-ip | interface-subnet | interface-gateway} {*interface*} .....274
address-object rename *object_name* *object_name* .....274
adjust-mss {auto | <200..1500>} .....181
algorithm {wrr|llf|spill-over} .....114
anti-spam dnsbl [1..5] domain *dnsbl_domain* {activate|deactivate} .....253
anti-spam dnsbl ip-check-order {forward | backward} .....253
anti-spam dnsbl max-query-ip [1..5] .....253
anti-spam dnsbl query-timeout pop3 {forward | forward-with-tag} .....253
anti-spam dnsbl query-timeout smtp {drop | forward | forward-with-tag} .....253
anti-spam dnsbl query-timeout time [1..10] .....253
anti-spam dnsbl statistics flush .....253
anti-spam ip-reputation query-timeout time [*timeout*] .....249
anti-spam mail-scan query-timeout pop3 {forward | forward-with-tag} .....249
anti-spam mail-scan query-timeout smtp {drop | forward | forward-with-tag} .....249
anti-spam mail-scan query-timeout time [*timeout*] .....249
anti-spam rule append .....248
anti-spam rule delete *rule_number* .....248
anti-spam rule insert *rule_number* .....248
anti-spam rule move *rule_number* to *rule_number* .....248
anti-spam rule *rule_number* .....248
anti-spam statistics flush .....255
anti-spam tag {dnsbl | dnsbl-timeout} [*tag*] .....253
anti-spam tag {mail-content | virus-outbreak} [*tag*] .....249
anti-spam tag black-list [*tag*] .....251
anti-spam tag query-timeout [*tag*] .....249
anti-virus black-list replace *old_av_file_pattern* *new_av_file_pattern* {activate|deactivate} 213
anti-virus mail-infect-ext activate .....210
anti-virus reload signatures .....210
anti-virus rule <1..32> .....211
anti-virus rule append .....210
anti-virus rule delete <1..32> .....211
anti-virus rule insert <1..32> .....210
anti-virus rule move <1..32> to <1..32> .....211
anti-virus search signature {all | category *category* | id *id* | name *name* | severity *severity* [{from *id* to *id*}] .....213
anti-virus statistics flush .....215
anti-virus update daily <0..23> .....214
anti-virus update hourly .....214
anti-virus update signatures .....214
anti-virus update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23> .....214
anti-virus white-list replace *old_av_file_pattern* *new_av_file_pattern* {activate|deactivate} 212
app other {del | forward | drop | reject} .....203
app other <1..64> .....203
app other append .....203
app other default .....203
app other insert *rule_number* .....203
app other move *rule_number* to *rule_number* .....203
app *protocol_name* {forward | drop | reject} .....200
app *protocol_name* bandwidth <0..102400> .....200
app *protocol_name* exception append .....202
app *protocol_name* exception default .....202
app *protocol_name* exception insert *rule_number* .....202
app *protocol_name* exception modify default .....202

app *protocol_name* exception modify *rule_number* ..... 202
app *protocol_name* exception move *rule_number* to *rule_number* ..... 202
app *protocol_name* exception *rule_number* ..... 202
app *protocol_name* exception *rule_number* ..... 202
app *protocol_name* mode {portless | portbase} ..... 200
app *protocol_name* rule append ..... 200
app *protocol_name* rule default ..... 201
app *protocol_name* rule insert *rule_number* ..... 200
app *protocol_name* rule modify default ..... 201
app *protocol_name* rule modify *rule_number* ..... 200
app *protocol_name* rule *rule_number* ..... 200
apply ..... 35
apply /conf/*file_name.conf* [ignore-error] [rollback] ..... 339
app-watch-dog reboot-log flush ..... 384
area IP virtual-link IP message-digest-key <1..255> md5 *authkey* ..... 131
arp IP *mac_address* ..... 380
atse ..... 35
authentication {pre-share | rsa-sig} ..... 179
authentication key <1..255> key-string *authkey* ..... 130
band {2.4G |5G} [band-mode {11n | bg | a}] ..... 59
band <b | g | bg| bgn | gn> ..... 103
bandwidth {inbound | outbound} <0..1048576> ..... 202
bandwidth {inbound|outbound} <0..1048576> ..... 201
bandwidth {inbound|outbound} <0..1048576> ..... 204
bandwidth priority <1..7> ..... 201
bandwidth priority <1..7> ..... 202
bandwidth priority <1..7> ..... 204
bandwidth-graph ..... 200
beacon-interval <40..1000> ..... 60
bind *profile* ..... 219
budget {log|log-alert}[recursive <1..65535>] ..... 95
budget {log|log-alert}[recursive <1..65535>] ..... 96
budget {log-percentage|log-percentage-alert} [recursive <1..65535>] ..... 97
budget current-connection {keep|drop} ..... 95
budget current-connection {keep|drop} ..... 96
budget new-connection {allow|disallow} ..... 95
budget new-connection {allow|disallow} ..... 96
budget percentage {ptime|pdata} <0..99> ..... 97
budget reset-counters ..... 95
budget reset-counters ..... 96
budget reset-day <0..31> ..... 95
budget reset-day <0..31> ..... 96
ca enroll cmp name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa} key-len *key_length* num <0..99999999> password *password* ca *ca_name* url *url*; ..... 296
ca enroll scep name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa} .. key-len *key_length* password *password* ca *ca_name* url *url* ..... 296
ca generate pkcs10 name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa} key-len *key_length* ..... 296
ca generate pkcs12 name *name* password *password* ..... 296
ca generate x509 name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa} key-len *key_length* ..... 296
ca rename category {local|remote} *old_name new_name* ..... 296
ca validation *remote_certificate* ..... 297
capwap ap add *ap_mac* [*ap_model*] ..... 56
capwap ap *ap_mac* ..... 56

capwap ap kick {all | *ap_mac*} ..... 56
capwap ap reboot *ap_mac* ..... 56
capwap manual-add {enable | disable} ..... 56
capwap show statistic ..... 56
capwap station kick *sta_mac* ..... 56
cdp {activate|deactivate} ..... 297
certificate *certificate-name* ..... 179
certificate *cert_name* ..... 196
channel <*wireless_channel* | auto> ..... 103
channel-width <auto | 20m | 40m> ..... 103
ch-width *wlan_htcw* ..... 61
clear ..... 35
clear aaa authentication *profile-name* ..... 291
clear aaa group server ad [*group-name*] ..... 287
clear aaa group server ldap [*group-name*] ..... 288
clear aaa group server radius *group-name* ..... 289
clear ip dhcp binding {*ip* | *} ..... 83
clear logging debug buffer ..... 355
clear logging system-log buffer ..... 354
clear report [*interface_name*] ..... 359
clock date *yyyy-mm-dd* time *hh:mm:ss* ..... 318
clock time *hh:mm:ss* ..... 318
cnm-agent keepalive interval <10..90> ..... 332
cnm-agent periodic-inform interval <10..86400> ..... 332
cnm-agent server-type {vantage | tr069} ..... 333
cnm-agent trigger-inform [interval] ..... 332
configure ..... 35
connectivity {nail-up | dial-on-demand} ..... 97
content-filter common-list {trust|forbid} ..... 238
content-filter passed warning flush ..... 238
content-filter passed warning timeout <1..1440> ..... 238
content-filter policy *policy_number* shutdown ..... 238
content-filter profile *filtering_profile* commtouch-url match {block | log | warn | pass} 241
content-filter profile *filtering_profile* commtouch-url match-unsafe {block | log | pass} 241
content-filter profile *filtering_profile* commtouch-url offline {block | log | warn | pass} 241
content-filter profile *filtering_profile* commtouch-url unrate {block | log | warn | pass} 241
content-filter profile *filtering_profile* custom-list forbid ..... 239
content-filter profile *filtering_profile* custom-list keyword ..... 240
content-filter profile *filtering_profile* custom-list trust ..... 240
content-filter profile *filtering_profile* url match {block | log | warn | pass} ..... 240
content-filter profile *filtering_profile* url match-unsafe {block | log | pass} ..... 240
content-filter profile *filtering_profile* url offline {block | log | warn | pass} ..... 240
content-filter profile *filtering_profile* url unrate {block | log | warn | pass} ..... 240
content-filter statistics flush ..... 242
content-filter url-cache test ..... 242
content-filter url-server test bluecoat ..... 238
content-filter url-server test commtouch ..... 238
content-filter zsb port <1..65535> ..... 238
copy ..... 35
copy {/cert | /conf | /idp | /packet_trace | /script | /tmp}*file_name-a.conf* {/cert | /conf | /idp | /packet_trace | /script | /tmp}/*file_name-b.conf* ..... 339
copy running-config /conf/*file_name.conf* ..... 339
copy running-config startup-config ..... 339
crypto map dial *map_name* ..... 181
crypto map *map_name* ..... 181
crypto map *map_name* ..... 183
crypto map rename *map_name map_name* ..... 181
crypto *map_name* ..... 184

daily-report ..... 361
deactivate ..... 179
deactivate ..... 181
debug (*) ..... 35
debug [cmdexec|corefile|ip |kernel|mac-id-rewrite|observer|switch |system|zyinetpkt|zysh-ipt-op] (*) ..... 38
debug alg ..... 37
debug anti-spam ..... 37
debug app ..... 37
debug app show l7protocol (*) ..... 37
debug ca (*) ..... 37
debug content-filter ..... 37
debug device-ha (*) ..... 37
debug eps ..... 37
debug force-auth (*) ..... 37
debug gui (*) ..... 37
debug gui (*) ..... 37
debug hardware (*) ..... 37
debug idp ..... 37
debug idp-av ..... 37
debug interface ..... 37
debug interface ifconfig [interface] ..... 37
debug interface-group ..... 37
debug ip dns ..... 37
debug ip virtual-server ..... 37
debug ipsec ..... 37
debug logging ..... 37
debug manufacture ..... 37
debug myzyxel server (*) ..... 37
debug network arpignore (*) ..... 37
debug no myzyxel server (*) ..... 37
debug policy-route (*) ..... 37
debug reset content-filter profiling ..... 37
debug service-register ..... 37
debug service-register erase service as ..... 49
debug show content-filter server ..... 37
debug show ipset ..... 37
debug show myzyxel server status ..... 37
debug show myzyxel server status ..... 37
debug sslvpn ..... 37
debug system ipv6 ..... 38
debug update server (*) ..... 38
delete ..... 35
delete {/cert | /conf | /idp | /packet_trace | /script | /tmp}/*file_name* ..... 339
description *ap_description* ..... 56
details ..... 35
device-ha ap-mode backup sync now ..... 260
device-ha ap-mode cluster-id <1..32> ..... 259
device-ha ap-mode priority <1..254> ..... 259
device-ha ap-mode role {master|backup} ..... 259
device-ha link-monitoring activate ..... 263
device-ha mode {active-passive | legacy} ..... 258
device-ha stop-stub-interface activate ..... 263
device-register checkuser *user_name* ..... 48
device-register username *user_name* password *password* [e-mail *user@domainname*] [country-code *country_code*] [reseller-name *name*] [reseller-mail *email-address*] [reseller-phone *phone-number*] [vat *vat-number*] ..... 48
dhcp6 ..... 78
dhcp6 { server | client | relay upper { *config_interface* | *ipv6_addr* } } ..... 77

dhcp6 address-request ..... 77
dhcp6 address-request ..... 78
dhcp6 duid { *duid* | mac } ..... 77
dhcp6 rapid-commit ..... 77
dhcp6 rapid-commit ..... 78
dhcp6 refresh-time { <600..4294967294> | infinity } ..... 77
dhcp6-lease-object *dhcp6_profile* ..... 77
dhcp6-lease-object *dhcp6_profile* ..... 78
dhcp6-lease-object *dhcp6_profile* { sip-server | ntp-server | dns-server } { *ipv6_addr* | *dhcp6_profile* } ..... 313
dhcp6-lease-object *dhcp6_profile* address *ipv6_addr* duid *duid* ..... 312
dhcp6-lease-object *dhcp6_profile* address-pool *ipv6_addr ipv6_addr* ..... 312
dhcp6-lease-object *dhcp6_profile* prefix-delegation *ipv6_addr_prefix* duid *duid* ..... 312
dhcp6-lease-object rename *dhcp6_profile dhcp6_profile* ..... 313
dhcp6-request-object *dhcp6_profile* ..... 77
dhcp6-request-object *dhcp6_profile* ..... 78
dhcp6-request-object *dhcp6_profile* { dns-server | ntp-server | prefix-delegation | sip-server } ..... 313
dhcp6-request-object rename *dhcp6_profile dhcp6_profile* ..... 313
dhcp-option <1..254> *option_name* {boolean <0..1>| uint8 <0..255> | uint16 <0..65535> ..... 82
diag ..... 35
diag-info ..... 35
diag-info collect ..... 367
dial-in ..... 331
dir ..... 35
dir {/cert | /conf | /idp | /packet_trace | /script | /tmp} ..... 339
disable ..... 35
draw-usage-graphics ..... 361
dscp-marking <0..63> ..... 121
dscp-marking <0..63> ..... 122
dscp-marking class {default | *dscp_class*} ..... 121
dscp-marking class {default | *dscp_class*} ..... 123
dtim-period <1..255> ..... 60
duration <0..300> ..... 377
eap {external | internal *auth_method*} ..... 66
enable ..... 35
enable ..... 76
enable ..... 77
encapsulation {tunnel | transport} ..... 181
eps insert <1..8> *eps_object_name* ..... 172
eps insert <1..8> *eps_object_name* ..... 270
eps insert <1..8> *eps_profile_name* ..... 188
eps move <1..8> to <1..8> ..... 172
eps move <1..8> to <1..8> ..... 188
eps move <1..8> to <1..8> ..... 270
eps warning-message {windows-auto-update | windows-security-patch | anti-virus | personal-firewall | windows-registry | process | file-path} ..... 309
exit ..... 100
exit ..... 104
exit ..... 114
exit ..... 121
exit ..... 123
exit ..... 166
exit ..... 167
exit ..... 170
exit ..... 184
exit ..... 238
exit ..... 238
exit ..... 239

exit ....239
exit ....240
exit ....240
exit ....242
exit ....309
exit ....36
exit ....362
exit ....374
exit ....56
exit ....62
exit ....64
exit ....66
exit ....68
exit ....74
exit ....75
exit ....90
fall-back-check-interval <60..86400> ....179
files-size <1..10000> ....378
file-suffix <*profile_name*> ....378
filter-action {allow | deny} ....67
firewall append ....161
firewall default-rule action {allow | deny | reject} { no log | log [alert] } ....161
firewall delete *rule_number* ....161
firewall flush ....161
firewall insert *rule_number* ....162
firewall move *rule_number* to *rule_number* ....162
firewall *rule_number* ....161
firewall *zone_object* {*zone_object*|ZyWALL} append ....161
firewall *zone_object* {*zone_object*|ZyWALL} delete <1..5000> ....161
firewall *zone_object* {*zone_object*|ZyWALL} flush ....161
firewall *zone_object* {*zone_object*|ZyWALL} insert *rule_number* ....161
firewall *zone_object* {*zone_object*|ZyWALL} move *rule_number* to *rule_number* ....161
firewall *zone_object* {*zone_object*|ZyWALL} *rule_number* ....161
firewall6 append ....162
firewall6 default-rule action {allow | deny | reject} { no log | log [alert] } ....162
firewall6 delete *rule_number* ....163
firewall6 flush ....163
firewall6 insert *rule_number* ....163
firewall6 move *rule_number* to *rule_number* ....163
firewall6 *rule_number* ....162
firewall6 *zone_object* {*zone_object*|ZyWALL} append ....162
firewall6 *zone_object* {*zone_object*|ZyWALL} delete <1..5000> ....162
firewall6 *zone_object* {*zone_object*|ZyWALL} flush ....162
firewall6 *zone_object* {*zone_object*|ZyWALL} insert *rule_number* ....162
firewall6 *zone_object* {*zone_object*|ZyWALL} move *rule_number* to *rule_number* ....162
firewall6 *zone_object* {*zone_object*|ZyWALL} *rule_number* ....162
flood-detection block-period <1..3600> ....221
flush ....114
force-auth [no] exceptional-service *service_name* ....269
force-auth default-rule authentication {required | unnecessary} {no log | log [alert]} ....269
force-auth policy <1..1024> ....269
force-auth policy append ....269
force-auth policy delete <1..1024> ....269
force-auth policy flush ....269
force-auth policy insert <1..1024> ....269
force-auth policy move <1..1024> to <1..1024> ....269
gateway ....77
gateway *ipv6_addr* metric <0..15> ....74
gateway *ipv6_addr* metric <0..15> ....75

group1 ..... 180
group2 ..... 180
group5 ..... 180
group-key <30..30000> ..... 104
group-key <30..30000> ..... 66
groupname rename *groupname groupname* ..... 267
guard-interval [short | long] ..... 104
guard-interval <short | long> ..... 103
guard-interval *wlan_htgi* ..... 61
host-ip {*ip-address* | *profile_name* | any> ..... 378
host-port <0..65535> ..... 378
htm ..... 36
http-inspection {http-xxx} log [alert] ..... 222
icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} action {drop | reject-sender | reject-receiver | reject-both}} ..... 222
icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} log [alert] ..... 222
idle <30..30000> ..... 104
idle <30..30000> ..... 66
idp {signature | system-protect} update daily <0..23> ..... 231
idp {signature | system-protect} update hourly ..... 231
idp {signature | system-protect} update signatures ..... 231
idp {signature | system-protect} update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23> 231
idp {signature| anomaly } rule { append | <1..32> | insert <1..32> } ..... 219
idp {signature| anomaly } rule { delete <1..32> | move <1..32> to <1..32> } ..... 219
idp anomaly *newpro* [base {all | none}] ..... 221
idp customize signature edit *quoted_string* ..... 227
idp customize signature *quoted_string* ..... 227
idp reload ..... 218
idp rename {signature | anomaly} *profile1 profile2* ..... 218
idp search signature *my_profile* name *quoted_string* sid SID severity *severity_mask* platform *platform_mask* policytype *policytype_mask* service *service_mask* activate {any | yes | no} log {any | no | log | log-alert} action *action_mask* ..... 225
idp search system-protect *my_profile* name *quoted_string* sid SID severity *severity_mask* platform *platform_mask* policytype *policytype_mask* service *service_mask* activate {any | yes | no} log {any | no | log | log-alert} action *action_mask* ..... 225
idp signature *newpro* [base {all | lan | wan | dmz | none}] ..... 220
idp statistics flush ..... 232
idp system-protect ..... 224
idp system-protect deactivate ..... 218
iface {add | del} {*interface_name* | *virtual_interface_name*} ..... 378
igmp direction ..... 80
igmp version *<1..3>* ..... 80
in-dnat <1..10> protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535> *mapped-ip address_name* <0..65535> <0..65535> ..... 182
in-dnat append protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535> mapped-ip *address_name* <0..65535> <0..65535> ..... 182
in-dnat delete <1..10> ..... 182
in-dnat insert <1..10> protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535> mapped-ip *address_name* <0..65535> <0..65535> ..... 182
in-dnat move <1..10> to <1..10> ..... 182
in-snat source *address_name* destination *address_name* snat *address_name* ..... 182
interface ..... 36
interface {*num*|append|insert *num*} *interface-name* [weight <1..10>|limit <1..2097152>|passive] 114
interface aux ..... 110
interface cellular budget-auto-save <5..1440> ..... 97
interface dial aux ..... 110

interface dial *interface_name* ..... 92
interface disconnect aux ..... 110
interface disconnect *interface_name* ..... 92
interface *interface_name* ..... 108
interface *interface_name* ..... 109
interface *interface_name* ..... 172
interface *interface_name* ..... 83
interface *interface_name* ..... 86
interface *interface_name* ..... 87
interface *interface_name* ..... 88
interface *interface_name* ..... 89
interface *interface_name* ..... 92
interface *interface_name* ipv6 ..... 74
interface *interface_name* ipv6 ..... 75
interface *interface_name* no ipv6 ..... 77
interface reset {*interface_name*|*virtual_interface_name*|all} ..... 78
interface send statistics interval <15..3600> ..... 78
interface-name {*ppp_interface* | *ethernet_interface*} *user_defined_name* ..... 78
interface-rename *old_user_defined_name new_user_defined_name* ..... 78
ip address *ipv4 ipv4* ..... 100
ip dhcp pool rename *profile_name profile_name* ..... 81
ip dns server cache-flush ..... 319
ip dns server rule {<1..32>|append|insert <1..32>} access-group {ALL|*address_object*} zone {ALL|*address_object*} action {accept|deny} ..... 320
ip dns server rule move <1..32> to <1..32> ..... 320
ip dns server zone-forwarder {<1..32>|append|insert <1..32>} {*domain_zone_name*|*} user-defined *w.x.y.z* [private | interface {*interface_name* | auto}] ..... 320
ip dns server zone-forwarder move <1..32> to <1..32> ..... 320
ip ftp server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} ..... 327
ip ftp server rule move *rule_number* to *rule_number* ..... 327
ip gateway *ip* metric <0..15> ..... 74
ip gateway *ip* metric <0..15> ..... 75
ip http secure-server cipher-suite {*cipher_algorithm*} [*cipher_algorithm*] [*cipher_algorithm*] [*cipher_algorithm*] ..... 323
ip http secure-server table {admin|user} rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} ..... 323
ip http secure-server table {admin|user} rule move *rule_number* to *rule_number* ..... 323
ip http server table {admin|user} rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} ..... 323
ip http server table {admin|user} rule move *rule_number* to *rule_number* ..... 323
ip http-redirect activate *description* ..... 146
ip http-redirect deactivate *description* ..... 146
ip http-redirect *description* interface *interface_name* redirect-to *w.x.y.z* <1..65535> ...146
ip http-redirect *description* interface *interface_name* redirect-to *w.x.y.z* <1..65535> deactivate 146
ip http-redirect flush ..... 146
ip ospf authentication ..... 87
ip ospf authentication message-digest ..... 87
ip ospf authentication same-as-area ..... 87
ip ospf message-digest-key <1..255> md5 *password* ..... 87
ip route replace {*w.x.y.z*} {*w.x.y.z*} {*interface*|*w.x.y.z*} <0..127> with {*w.x.y.z*} {*w.x.y.z*} {*interface*|*w.x.y.z*} <0..127> ..... 126
ip ssh server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} ..... 325
ip ssh server rule move *rule_number* to *rule_number* ..... 325
ip telnet server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} ..... 326
ip telnet server rule move *rule_number* to *rule_number* ..... 326

ip virtual-server {activate | deactivate} *profile_name* .....143
ip virtual-server delete *profile_name* .....143
ip virtual-server flush .....143
ip virtual-server *profile_name* interface *interface_name* original-ip {any | *ip* | *address_object*} map-to {*address_object* | *ip*} map-type any [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate] .....142
ip virtual-server *profile_name* interface *interface_name* original-ip {any | IP | *address_object*} map-to {*address_object* | *ip*} map-type original-service *service_object* mapped-service *service_object* [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate] .....143
ip virtual-server *profile_name* interface *interface_name* original-ip {any | IP | *address_object*} map-to {*address_object* | *ip*} map-type port protocol {any | tcp | udp} original-port <1..65535> mapped-port <1..65535> [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate] .....142
ip virtual-server *profile_name* interface *interface_name* original-ip {any | IP | *address_object*} map-to {*address_object* | *ip*} map-type ports protocol {any | tcp | udp} original-port-begin <1..65535> original-port-end <1..65535> mapped-port-begin <1..65535> [nat-loopback [nat-1-1-map] [deactivate] | nat-1-1-map [deactivate] | deactivate] .....142
ip virtual-server rename *profile_name profile_name* .....143
ip6 route *destv6/prefix* { *ipv6_global_address* | *ipv6_link_local* | *interface*} [<0..127>] 126
ip6 route *destv6/prefix* { *ipv6_link_local interface*} [<0..127>] .....126
ip6 route replace *destv6/prefix* { *gatewayv6* | *interface*} [<0..127>] with *destv6/prefix* { *gatewayv6* | *interface*} [<0..127>] .....126
ipsec-isakmp *policy_name* .....181
ipv6 6to4 [ prefix *ipv6_addr_prefix* | destination-prefix *ipv4_cidr* | relay *ipv4* ] .....100
ipv6 address *dhcp6_profile dhcp6_suffix_128* .....76
ipv6 address *dhcp6_profile dhcp6_suffix_128* .....78
ipv6 address *ipv6_addr_prefix* .....100
ipv6 dhcp6 [client] .....93
ipv6 dhcp6 duid { *duid* | mac } .....93
ipv6 neighbor flush {*ipv6* | all} .....379
ip-version {ip|ip6|any} .....378
isakmp keepalive <2..60> .....179
isakmp policy rename *policy_name policy_name* .....180
keystring *pre_shared_key* .....180
l2tp-over-ipsec authentication *aaa authentication profile_name* .....195
l2tp-over-ipsec crypto *map_name* .....195
l2tp-over-ipsec pool *address-object* .....195
l2tp-over-ipsec recover default-ipsec-policy .....195
language <English | Simplified_Chinese | Traditional_Chinese> .....334
ldap {activate|deactivate} .....297
ldap ip {*ip*|*fqdn*} port <1..65535> [id *name* password *password*] [deactivate] .....297
lifetime <180..3000000> .....180
limit-ampdu <100..65535> .....60
limit-amsdu <2290..4096> .....61
link-sticking outgoing interface {*interface_name* | all} .....153
list signature {anti-virus | personal-firewall | status} .....308
loadbalancing-index <inbound|outbound|total> .....115
local-id type {ip *ip* | fqdn *domain_name* | mail *e_mail* | dn *distinguished_name*} .....180
local-ip {ip {*ip* | *domain_name*} | interface *interface_name*} .....180
local-ip *ip* .....183
local-policy *address_name* .....181
logging console category *module_name* level {alert | crit | debug | emerg | error | info | notice | warn} .....358
logging mail <1..2> schedule daily hour <0..23> minute <0..59> .....357
logging mail <1..2> schedule weekly day *day* hour <0..23> minute <0..59> .....357
logging mail <1..2> sending_now .....357
logging system-log category *module_name* {disable | level normal | level all} .....354
logging usb-storage category *category* disable .....101

logging usb-storage category *category* level <all|normal> ..... 101
logging usb-storage flushThreshold <1..100> ..... 101
login-page background-color {*color-rgb* | *color-name* | *color-number*} ..... 316
login-page message-color {*color-rgb* | *color-name* | *color-number*} ..... 316
login-page title *title* ..... 316
login-page title-color {*color-rgb* | *color-name* | *color-number*} ..... 316
login-page window-color {*color-rgb* | *color-name* | *color-number*} ..... 317
logo background-color {*color-rgb* | *color-name* | *color-number*} ..... 317
logon-re-auth-time <0..1440> ..... 173
mac *mac* ..... 89
mail-subject set *subject* ..... 361
matching-criteria {any | all} ..... 308
mode {main | aggressive} ..... 179
mode {none | wep | wpa | wpa2 | wpa2-mix} ..... 65
mode {normal|trunk} ..... 115
move <1..8> to <1..8> ..... 115
mtu <576..1492> ..... 93
mtu <576..1492> ..... 97
nd ra accept ..... 76
nd ra accept ..... 77
nd ra advertise ..... 76
nd ra advertise ..... 77
nd ra default-lifetime ..... 78
nd ra default-lifetime <4..9000> ..... 76
nd ra hop-limit ..... 78
nd ra hop-limit <0..255> ..... 76
nd ra managed-config-flag ..... 76
nd ra managed-config-flag ..... 77
nd ra max-rtr-interval ..... 78
nd ra max-rtr-interval <4..1800> ..... 76
nd ra min-rtr-interval ..... 78
nd ra min-rtr-interval <3..1350> ..... 76
nd ra mtu ..... 77
nd ra mtu <1280..1500> | <0> ..... 76
nd ra other-config-flag ..... 76
nd ra other-config-flag ..... 77
nd ra prefix-advertisement *dhcp6_profile dhcp6_suffix_64* ..... 77
nd ra prefix-advertisement DHCP6_PROFILE DHCP6_SUFFIX_64 ..... 78
nd ra prefix-advertisement *ipv6_addr_prefix* [ auto { on | off } ] [ link{ on | off } ] [ pre-
ferred-time { <0..4294967294> | infinity }] [valid-time{ <0..4294967294> | infinity }]
76
nd ra reachable-time ..... 78
nd ra reachable-time <0..3600000> ..... 76
nd ra retrans-timer ..... 78
nd ra retrans-timer <0..4294967295> ..... 76
nd ra router-preference { low | medium | high } ..... 76
network *ip mask* ..... 82
network IP/<1..32> ..... 82
no address-object *object_name* ..... 274
no anti-spam dnsbl domain *dnsbl_domain* ..... 253
no anti-virus mail-infect-ext activate ..... 210
no app other *rule_number* ..... 203
no app *protocol_name* rule *rule_number* ..... 201
no area IP virtual-link IP message-digest-key <1..255> ..... 131
no arp *ip* ..... 380
no authentication key ..... 130
no bind ..... 219
no budget log [recursive] ..... 95
no budget log [recursive] ..... 96

no budget log-percentage ....97
no ca category {local|remote} *certificate_name* ....297
no ca validation *name* ....297
no content-filter profile *filtering_profile* commtouch-url match {log} ....241
no content-filter profile *filtering_profile* commtouch-url match-unsafe {log} ....241
no content-filter profile *filtering_profile* commtouch-url offline {log} ....241
no content-filter profile *filtering_profile* commtouch-url unrate {log} ....241
no content-filter profile *filtering_profile* url match {log} ....240
no content-filter profile *filtering_profile* url match-unsafe {log} ....240
no content-filter profile *filtering_profile* url offline {log} ....240
no content-filter profile *filtering_profile* url unrate {log} ....241
no device-ha link-monitoring ....263
no device-ha stop-stub-interface ....263
no dhcp6-lease-object *dhcp6_profile* ....313
no dhcp6-request-object *dhcp6_profile* ....313
no dhcp-option <1..254> ....82
no dscp-marking ....121
no dscp-marking ....123
no http-inspection {http-xxx} log ....222
no icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} action ....222
no icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} log 222
no idp {signature | anomaly} *profile3* ....218
no idp {signature| anomaly } rule <1..32> ....219
no idp customize signature *custom_sid* ....227
no ip dns server rule <1..32> ....320
no ip ftp server rule *rule_number* ....327
no ip http secure-server cipher-suite {*cipher_algorithm*} ....323
no ip http secure-server table {admin|user} rule *rule_number* ....323
no ip http server table {admin|user} rule *rule_number* ....323
no ip http-redirect *description* ....146
no ip ospf authentication ....87
no ip ospf message-digest-key ....87
no ip ssh server rule *rule_number* ....325
no ip telnet server rule *rule_number* ....326
no ip virtual-server *profile_name* ....142
no ip6 route *destv6/prefix* { *gatewayv6* | *interface*} [<0..127>] ....126
no l2tp-over-ipsec session tunnel-id <0..65535> ....196
no mac ....89
no mail-subject set ....361
no network ....82
no packet-trace ....36
no port <1..*x*> ....90
no sa spi *spi* ....185
no sa tunnel-name *map_name* ....185
no scan-detection sensitivity ....221
no schedule-object *object_name* ....283
no security {none | wep | wpa | wpa-wpa2 | wpa2} ....106
no server-type ....303
no service-object *object_name* ....279
no signature *sid* action ....220
no signature *SID* action ....224
no signature *sid* log ....220
no signature *sid* log ....224
no *slot_name* ap-profile ....56
no smtp-address ....361
no smtp-auth username ....361
no snmp-server rule *rule_number* ....329

no sslvpn policy *profile_name* .....189
no tcp-decoder {tcp-xxx} log .....222
no udp-decoder {truncated-header | undersize-len | oversize-len} action .....222
no udp-decoder {truncated-header | undersize-len | oversize-len} log .....222
no use-defined-mac .....90
no user .....184
no username *username* .....266
nslookup .....36
ntp sync .....318
object-group address rename *group_name group_name* .....277
object-group service rename *group_name group_name* .....281
ocsp {activate|deactivate} .....297
ocsp url *url* [id *name* password *password*] [deactivate] .....297
or .....200
or .....201
or .....202
or .....202
os-type {windows | linux | mac-osx | others} .....307
output-power [100% | 50% | 25% | 12.5%] .....103
output-power *wlan_power* .....62
out-snat source *address_name* destination *address_name* snat *address_name* .....182
packet-capture configure .....377
packet-flow buffer clear *pf_cpu_core_num* .....374
packet-flow buffer write .....374
packet-flow filter *pf_filter_num_range* .....373
packet-trace .....36
packet-trace [interface *interface_name*] [[ip-proto|ipv6-proto] | *protocol_name* | any}] [src-host {*ip* | *hostname* | any}] [dst-host {*ip* | *hostname* | any}] [port {<1..65535> | any}] [file] [duration <1..3600>] [extension-filter *filter_extension*] .....377
peer-id type {any | ip *ip* | fqdn *domain_name* | mail *e_mail* | dn *distinguished_name*} ....180
peer-ip {*ip* | *domain_name*} [*ip* | *domain_name*] .....180
peer-ip *ip* .....183
ping .....36
ping6 .....36
ping6{*ipv6* | *hostname*} [source *ipv6*] [size <0..65527>] [forever| count <1..4096>] [interface {*interface_name* | *virtual_interface_name*}][extension *filter_extension*] .....378
ping-check {*domain_name* | *ip* | default-gateway} .....88
ping-check {*domain_name* | *ip* | default-gateway} fail-tolerance <1..10> .....88
ping-check {*domain_name* | *ip* | default-gateway} method {icmp | tcp} .....88
ping-check {*domain_name* | *ip* | default-gateway} period <5..30> .....88
ping-check {*domain_name* | *ip* | default-gateway} port <1..65535> .....88
ping-check {*domain_name* | *ip* | default-gateway} timeout <1..10> .....88
policy {*policy_number* | append | insert *policy_number*} .....120
policy default-route .....123
policy delete *policy_number* .....123
policy flush .....123
policy list table .....123
policy move *policy_number* to *policy_number* .....123
policy6 {*policy_number* | append | insert *policy_number*} .....122
port <0..65535> .....201
port <0..65535> .....203
port <1..65535> ending-port <1..65535>] .....303
port <1..65535> ending-port <1..65535>] [program-path *program-path*] .....303
port status Port<1..*x*> .....90
port-grouping *representative_interface* port <1..*x*> .....90
proto-type {icmp | icmp6 | igmp | igrp | pim | ah | esp | vrrp | udp | tcp | any} .....378
psm .....36
qos [none | wmm} .....104
qos <none | wmm> .....103

qos *wlan_qos* .....64
reauth <30..30000> .....105
reboot .....36
redistribute {static | ospf} metric <0..16> .....130
release .....36
release dhcp *interface-name* .....83
remote-policy *address_name* .....181
rename .....36
rename {/cert | /conf | /idp | /packet_trace | /script | /tmp}/*old-file_name* {/cert | /conf | /idp | /packet_trace | /script | /tmp}/*new-file_name* .....339
rename /script/*old-file_name* /script/*new-file_name* .....339
renew .....36
renew dhcp *interface-name* .....83
report packet size statistics clear .....361
reset-counter-now .....362
ring-buffer <enable|disable> .....378
role ap .....103
role ap .....59
router ospf .....130
router ospf .....131
router ospf .....131
router ospf .....86
router rip .....130
router rip .....86
Router(config-sso-secondary)#[no] [no] port *<1025..65535>* .....174
Router(SIP Signaling Port)# [no] port <1025..65535> .....150
rssi-dbm <-20~-76> .....59
run .....36
run /script/*file_name.zysh* .....339
rx-mask *chain_mask* .....62
scan-detection block-period <1..3600> .....221
scan-detection sensitivity {low | medium | high} .....221
scenario {site-to-site-static|site-to-site-dynamic|remote-access-server|remote-access-client} .....181
schedule hour <0..23> minute <00..59> .....362
schedule-object *object_name date time date time* .....284
schedule-object *object_name time time* [*day*] [*day*] [*day*] [*day*] [*day*] [*day*] [*day*] .....284
schedule-run 1 *file_name.zysh* {daily | monthly | weekly} time {*date* | sun | mon | tue | wed | thu | fri | sat} .....340
security mode {none | wep | wpa | wpa-wpa2 | wpa2} .....105
security *securityprofile* .....64
security wep <64 | 128> default-key <1..4> .....105
security wep mode <open | share> .....105
security wpa <tkip | aes> eap external .....105
security wpa <tkip | aes> eap internal *profile-name* tls-cert *certificate name* .....105
security wpa <tkip | aes> psk key *psk-key* .....105
security wpa2 <tkip | aes> eap external .....105
security wpa2 <tkip | aes> eap internal *profile-name* tls-cert *certificate name* .....105
security wpa2 <tkip | aes> psk key *psk-key* .....105
security wpa-wpa2 <tkip | aes> eap external .....105
security wpa-wpa2 <tkip | aes> eap internal *profile-name* tls-cert *certificate name* .....105
security wpa-wpa2 <tkip | aes> psk key *psk-key* .....105
send-now .....362
server-auth <1..2> ip address *ipv4_address* port <1..65535> secret *secret* .....66
server-type {file-sharing | owa | web-server} url URL [entry-point *entry_point*] .....302
server-type file-sharing share-path *share-path* .....303
server-type rdp server-address *server-address* [starting- .....303
server-type vnc server-address *server-address* [starting- .....303
server-type weblink url *url* .....303

service-object *object_name* {tcp | udp} {eq <1..65535> | range <1..65535> <1..65535>} ...279
service-object *object_name* icmp *icmp_value* .....280
service-object *object_name* icmpv6 {<0..255> | neighbor-solicitation | router-advertisement | echo | packet-toobig | router-solicitation | echo-reply | parameter-problem | time-exceeded | neighbor-advertisement | redirect | unreachable} .....280
service-object *object_name* protocol <1..255> .....280
service-object rename *object_name object_name* .....280
service-register checkexpire .....49
service-register content-filter-engine { bluecoat | commtouch } .....49
service-register service-type standard license-key *key_value* .....49
service-register service-type trial av-engine {kav|zav} .....49
service-register service-type trial service {content-filter|idp} .....49
service-register service-type trial service all {kav|zav} .....49
service-register service-type trial service as .....49
service-register service-type trial service av {kav|zav} .....49
session timeout {udp-connect <1..300> | udp-deliver <1..300> | icmp <1..300>} .....365
session timeout session {tcp-established | tcp-synrecv | tcp-close | tcp-finwait | tcp-synsent | tcp-closewait | tcp-lastack | tcp-timewait} <1..300> .....365
session-limit append .....166
session-limit delete *rule_number* .....166
session-limit flush .....166
session-limit insert *rule_number* .....166
session-limit limit <0..8192> .....166
session-limit move *rule_number* to *rule_number* .....166
session-limit *rule_number* .....166
session-limit6 append .....167
session-limit6 delete *rule_number* .....167
session-limit6 flush .....167
session-limit6 insert *rule_number* .....167
session-limit6 limit <0..8192> .....166
session-limit6 move *rule_number* to *rule_number* .....167
session-limit6 *rule_number* .....166
set pfs {group1 | group2 | group5 | none} .....181
set security-association lifetime seconds <180..3000000> .....181
set session-key {ah <256..4095> *auth_key* | esp <256..4095> [cipher *enc_key*] authenticator *auth_key*} .....183
setenv .....36
setenv-startup stop-on-error off .....340
show .....172
show .....201
show .....203
show .....204
show .....248
show .....267
show .....270
show .....36
show .....81
show [all] .....211
show {address-object | address6-object | service-object | schedule-object} [*object_name*] 274
show aaa authentication {*group-name*|default} .....291
show aaa group server ad *group-name* .....287
show aaa group server ldap *group-name* .....288
show aaa group server radius *group-name* .....289
show access-page settings .....317
show account [pppoe *profile_name* | pptp *profile_name*] .....300
show account cellular *profile_name* .....301
show ad-server .....285
show anti-spam {smtp | pop3} defaultport .....249
show anti-spam activation .....247

show anti-spam black-list [status] ..... 251
show anti-spam dnsbl domain ..... 253
show anti-spam dnsbl ip-check-order ..... 253
show anti-spam dnsbl max-query-ip ..... 253
show anti-spam dnsbl query-timeout {smtp | pop3} ..... 253
show anti-spam dnsbl query-timeout time ..... 253
show anti-spam dnsbl statistics ..... 253
show anti-spam dnsbl status ..... 253
show anti-spam ip-reputation private-check ..... 249
show anti-spam ip-reputation query-timeout time ..... 249
show anti-spam ip-reputation statistics ..... 256
show anti-spam mail-scan query-timeout pop3 ..... 249
show anti-spam mail-scan query-timeout smtp ..... 249
show anti-spam mail-scan query-timeout time ..... 249
show anti-spam mail-scan statistics ..... 256
show anti-spam mail-scan status ..... 249
show anti-spam rule [*rule_number*] ..... 248
show anti-spam statistics collect ..... 255
show anti-spam statistics ranking {source | mail-address} ..... 255
show anti-spam statistics summary ..... 255
show anti-spam tag {dnsbl | dnsbl-timeout} ..... 253
show anti-spam tag {mail-content | virus-outbreak} ..... 249
show anti-spam tag black-list ..... 251
show anti-spam tag query-timeout ..... 249
show anti-spam white-list [status] ..... 251
show anti-spam xheader {mail-content | virus-outbreak} ..... 249
show anti-spam xheader {white-list | black-list} ..... 251
show anti-spam xheader dnsbl ..... 254
show anti-spam xheader query-timeout ..... 249
show anti-virus activation ..... 210
show anti-virus eicar activation ..... 210
show anti-virus signatures status ..... 214
show anti-virus skip-unknown-file-type activation ..... 210
show anti-virus statistics collect ..... 215
show anti-virus statistics ranking {destination | source | virus-name} ..... 215
show anti-virus statistics summary ..... 215
show anti-virus update ..... 214
show anti-virus update status ..... 214
show app {general|im|p2p|stream} ..... 205
show app all ..... 205
show app all defaultport ..... 205
show app all statistics ..... 205
show app config ..... 205
show app highest sip bandwidth priority ..... 206
show app im support action ..... 205
show app other config ..... 205
show app other rule all ..... 205
show app other rule all statistics ..... 205
show app other rule default ..... 205
show app other rule default statistics ..... 205
show app other rule *rule_number* ..... 205
show app other rule *rule_number* statistics ..... 205
show app other statistics ..... 205
show app *protocol_name* config ..... 205
show app *protocol_name* defaultport ..... 205
show app *protocol_name* rule all ..... 205
show app *protocol_name* rule all statistics ..... 205
show app *protocol_name* rule default ..... 205
show app *protocol_name* rule default statistics ..... 205

show app *protocol_name* rule *rule_number* ..... 205
show app *protocol_name* rule *rule_number* statistics ..... 205
show app *protocol_name* statistics ..... 205
show app-watch-dog config ..... 384
show app-watch-dog monitor-list ..... 384
show app-watch-dog reboot-log ..... 384
show arp-table ..... 380
show boot status ..... 43
show bridge available member ..... 109
show bwm activation ..... 123
show bwm activation ..... 206
show bwm-usage < [policy-route *policy_number*] | [interface *interface_name*] ..... 124
show ca category {local|remote} [name *certificate_name* format {text|pem}] ..... 298
show ca category {local|remote} name *certificate_name* certpath ..... 298
show ca spaceusage ..... 298
show ca validation name *name* ..... 298
show capwap ap {all | *ap_mac*} ..... 56
show capwap ap {all | *ap_mac*} config status ..... 56
show capwap ap all statistics ..... 56
show capwap ap *ap_mac slot_name* detail ..... 56
show capwap ap wait-list ..... 56
show capwap manual-add ..... 56
show capwap station all ..... 56
show clock date ..... 318
show clock status ..... 318
show clock time ..... 318
show cnm-agent configuration ..... 333
show comport status ..... 43
show conn [user {*username*|any|unknown}] [service {*service-name*|any|unknown}] [source {*ip*|any}] [destination {*ip*|any}] [begin <1..128000>] [end <1..128000>] ..... 360
show conn ip-traffic destination ..... 360
show conn ip-traffic source ..... 360
show conn status ..... 360
show connectivity-check continuous-log status ..... 354
show connectivity-check continuous-log status ..... 88
show connlimit max-per-host ..... 162
show connlimit6 max-per-host ..... 163
show console ..... 318
show content-filter common-list {trust|forbid} ..... 239
show content-filter passed warning ..... 239
show content-filter policy ..... 239
show content-filter profile [*filtering_profile*] ..... 241
show content-filter settings ..... 239
show content-filter statistics collect ..... 242
show content-filter statistics summary ..... 242
show content-filter statistics summary ..... 242
show content-filter url-cache ..... 242
show content-filter url-cache [all-category] [begin *url_cache_range* end *url_cache_range*] [_count] ..... 242
show corefile copy usb-storage ..... 102
show cpu status ..... 43
show crypto map [*map_name*] ..... 180
show daily-report status ..... 361
show ddns [*profile_name*] ..... 138
show ddns-status ..... 138
show device-ha ap-mode backup sync ..... 260
show device-ha ap-mode backup sync status ..... 260
show device-ha ap-mode backup sync summary ..... 261
show device-ha ap-mode forwarding-port *interface_name* ..... 261

show device-ha ap-mode interfaces ..... 260
show device-ha ap-mode master sync ..... 260
show device-ha ap-mode next-sync-time ..... 260
show device-ha ap-mode status ..... 260
show device-ha link-monitoring ..... 263
show device-ha status ..... 258
show device-ha stop-stub-interface ..... 263
show device-ha sync ..... 263
show device-ha sync backup next-sync-time ..... 263
show device-ha sync status ..... 263
show device-ha vrrp-group ..... 262
show device-register status ..... 49
show dhcp6 interface ..... 312
show dhcp6 object-binding *interface_name* ..... 312
show dhcp6-lease-object [*dhcp6_profile*] ..... 312
show dhcp6-request-object [*dhcp6_profile*] ..... 312
show diag-info ..... 367
show diag-info copy usb-storage ..... 102
show dial-in ..... 332
show disk ..... 43
show eps failure-messages ..... 306
show eps profile [*profile_name*] ..... 308
show eps profile *profile_name* signature {anti-virus | personal-firewall} ..... 308
show eps signature {anti-virus | personal-firewall | status} ..... 308
show eps warning-message {windows-auto-update | windows-security-patch | anti-virus | personal-firewall | windows-registry | process | file-path} ..... 309
show extension-slot ..... 43
show fan-speed ..... 43
show firewall any ZyWALL ..... 162
show firewall block_rules ..... 162
show firewall6 ..... 163
show firewall6 any ZyWALL ..... 163
show firewall6 block_rules ..... 163
show firewall6 *rule_number* ..... 163
show firewall6 status ..... 163
show firewall6 *zone_object* {*zone_object*|ZyWALL} ..... 163
show firewall6 *zone_object* {*zone_object*|ZyWALL} *rule_number* ..... 163
show firewallsecure-policy ..... 162
show firewallsecure-policy *rule_number* ..... 162
show firewallsecure-policy status ..... 162
show firewallsecure-policy *zone_object* {*zone_object*|ZyWALL} ..... 162
show firewallsecure-policy *zone_object* {*zone_object*|ZyWALL} *rule_number* ..... 162
show force-auth activation ..... 269
show force-auth exceptional-service ..... 269
show force-auth policy {<1..1024> | all} ..... 269
show fqdn ..... 317
show groupname [*groupname*] ..... 267
show hardware-watchdog-timer status ..... 383
show idp ..... 218
show idp {signature | anomaly} base profile ..... 218
show idp {signature | system-protect} signatures {version | date | number} ..... 231
show idp {signature | system-protect} update ..... 231
show idp {signature | system-protect} update status ..... 231
show idp {signature| anomaly } rules ..... 219
show idp anomaly *profile* flood-detection [all details] ..... 223
show idp anomaly *profile* flood-detection {tcp-flood | udp-flood | ip-flood | icmp-flood} details 223
show idp anomaly *profile* http-inspection {ascii-encoding | u-encoding | bare-byte-unicode-encoding | base36-encoding | utf-8-encoding | iis-unicode-codepoint-encoding | multi-

slash-encoding | iis-backslash-evasion | self-directory-traversal | directory-traversal | apache-whitespace | non-rfc-http-delimiter | non-rfc-defined-char | oversize-request-uri-directory | oversize-chunk-encoding | webroot-directory-traversal} details ...223
show idp anomaly *profile* http-inspection all details .....223
show idp anomaly *profile* icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} details .....223
show idp anomaly *profile* icmp-decoder all details .....223
show idp anomaly *profile* scan-detection [all details] .....222
show idp anomaly *profile* scan-detection {icmp-sweep | icmp-filtered-sweep | open-port} details 223
show idp anomaly *profile* scan-detection {ip-protocol-scan | ip-decoy-protocol-scan | ip-protocol-sweep | ip-distributed-protocol-scan | ip-filtered-protocol-scan | ip-filtered-decoy-protocol-scan | ip-filtered-distributed-protocol-scan | ip-filtered-protocol-sweep} details .....223
show idp anomaly *profile* scan-detection {tcp-portscan | tcp-decoy-portscan | tcp-portsweep | tcp-distributed-portscan | tcp-filtered-portscan | tcp-filtered-decoy-portscan | tcp-filtered-distributed-portscan | tcp-filtered-portsweep} details .....223
show idp anomaly *profile* scan-detection {udp-portscan | udp-decoy-portscan | udp-portsweep | udp-distributed-portscan | udp-filtered-portscan | udp-filtered-decoy-portscan | .223
show idp anomaly *profile* tcp-decoder {undersize-len | undersize-offset | oversize-offset | bad-length-options | truncated-options | ttcp-detected | obsolete-options | experimental-options} details .....223
show idp anomaly *profile* tcp-decoder all details .....223
show idp anomaly *profile* udp-decoder {truncated-header | undersize-len | oversize-len} details 223
show idp anomaly *profile* udp-decoder all details .....223
show idp *profile* signature {all | custom-signature} details .....220
show idp *profile* signature *sid* details .....220
show idp profiles .....218
show idp search signature *my_profile* name *quoted_string* sid SID severity *severity_mask* platform *platform_mask* policytype *policytype_mask* service *service_mask* activate {any | yes | no} log {any | no | log | log-alert} action *action_mask* .....225
show idp search system-protect *my_profile* name *quoted_string* sid SID severity *severity_mask* platform *platform_mask* policytype *policytype_mask* service *service_mask* activate {any | yes | no} log {any | no | log | log-alert} action *action_mask* .....225
show idp signature all details .....218
show idp signature base profile {all|none|wan|lan|dmz} settings .....218
show idp signature *profile* signature all details .....218
show idp signatures custom-signature all details .....227
show idp signatures custom-signature *custom_sid* {details | contents | non-contents} ....227
show idp signatures custom-signature number .....227
show idp statistics collect .....232
show idp statistics ranking {signature-name | source | destination} .....232
show idp statistics summary .....232
show idp system-protect all details .....224
show interface {ethernet | vlan | bridge | ppp | auxiliary} status .....73
show interface {*interface_name* | ethernet | vlan | bridge | ppp | virtual ethernet | virtual vlan | virtual bridge | auxiliary | all} .....73
show interface cellular [corresponding-slot|device-status|support-device] .....97
show interface cellular budget-auto-save .....97
show interface cellular corresponding-slot .....97
show interface cellular device-status .....97
show interface cellular status .....97
show interface cellular support-device .....97
show interface *interface_name* [budget] .....97
show interface *interface_name* device profile .....97
show interface *interface_name* device status .....97
show interface ppp system-default .....93
show interface ppp user-define .....93

show interface send statistics interval ..... 74
show interface send statistics interval ..... 75
show interface summary all ..... 74
show interface summary all ..... 75
show interface summary all status ..... 74
show interface summary all status ..... 75
show interface tunnel status ..... 100
show interface *tunnel_iface* ..... 100
show interface-group {system-default|user-define|*group-name*} ..... 114
show interface-name ..... 78
show ip dhcp binding [*ip*] ..... 83
show ip dhcp dhcp-options ..... 81
show ip dhcp pool [*profile_name*] ..... 81
show ip dhcp pool *profile_name* dhcp-options ..... 81
show ip dns server ..... 320
show ip dns server database ..... 320
show ip dns server status ..... 320
show ip ftp server status ..... 327
show ip http server secure status ..... 323
show ip http server status ..... 323
show ip http-redirect [*description*] ..... 146
show ip load-balancing link-sticking status ..... 117
show ip route [kernel | connected | static | ospf | rip | bgp] ..... 132
show ip route control-virtual-server-rules ..... 126
show ip route static-dynamic ..... 369
show ip route-settings ..... 126
show ip ssh server status ..... 325
show ip telnet server status ..... 326
show ip virtual-server [*profile_name*] ..... 142
show ipv6 dhcp6 binding ..... 312
show ipv6 interface {*interface_name* | all} ..... 73
show ipv6 nd ra status *config_interface* ..... 73
show ipv6 neighbor-list ..... 379
show ipv6 static address *interface* ..... 73
show ipv6 status ..... 334
show isakmp keepalive ..... 179
show isakmp policy [*policy_name*] ..... 179
show isakmp sa ..... 185
show l2tp-over-ipsec ..... 196
show l2tp-over-ipsec session ..... 196
show language {setting | all} ..... 334
show ldap-server ..... 286
show led status ..... 43
show lockout-users ..... 271
show logging debug entries [priority *pri*] [category *module_name*] [srcip *ip*] [srcip6 *ipv6_addr*] [dstip *ip*] [dstip6 *ipv6_addr*] [service *service_name]* [srciface *interface_name*] [dstiface *interface_name*] [protocol *protocol*] [begin <1..512> end <1..512>] [keyword *keyword*] . 355
show logging debug entries field *field* [begin <1..1024> end <1..1024>] ..... 355
show logging debug status ..... 355
show logging entries [priority *pri*] [category *module_name*] [srcip *ip*] [srcip6 *ipv6_addr*] [dstip *ip*] [dstip6 *ipv6_addr*] [service *service_name]* [begin <1..512> end <1..512>] [keyword *keyword*] [srciface *interface_name*] [dstiface *interface_name*] [protocol *protocol*] ....354
show logging entries field *field* [begin <1..512> end <1..512>] ..... 354
show logging status console ..... 358
show logging status mail ..... 356
show logging status syslog ..... 356
show logging status system-log ..... 354
show logging status usb-storage ..... 101

show login-page default-title ..... 317
show login-page settings ..... 317
show logo settings ..... 317
show mac ..... 43
show mem status ..... 43
show ntp server ..... 318
show object-group {address | address6} [group_name] ..... 276
show object-group service group_name ..... 280
show ospf area IP virtual-link ..... 131
show packet-capture config ..... 379
show packet-capture status ..... 378
show packet-flow buffer [pf_cpu_core_num] ..... 374
show packet-flow filter pf_filter_num_range ..... 374
show packet-flow status ..... 374
show page-customization ..... 317
show ping-check [interface_name | status] ..... 88
show policy-route [policy_number] ..... 124
show policy-route begin <1..200> end <1..200> ..... 124
show policy-route controll-ipsec-dynamic-rules ..... 124
show policy-route controll-virtual-server-rules ..... 124
show policy-route override-direct-route ..... 124
show policy-route rule_count ..... 124
show policy-route underlayer-rules ..... 124
show policy-route6 override-direct-route ..... 124
show port setting ..... 90
show port status ..... 90
show port vlan-id ..... 108
show port-grouping ..... 90
show radius-server ..... 287
show ram-size ..... 43
show redundant-power status ..... 43
show reference object aaa authentication [default | auth_method] ..... 41
show reference object account pppoe [object_name] ..... 41
show reference object account pptp [object_name] ..... 41
show reference object address [object_name] ..... 41
show reference object address6 [object_name] ..... 41
show reference object ca category {local|remote} [cert_name] ..... 41
show reference object crypto map [crypto_name] ..... 41
show reference object dhcp6-lease-object [object_name] ..... 42
show reference object dhcp6-request-object [object_name] ..... 42
show reference object eps [object_name] ..... 41
show reference object interface [interface_name | virtual_interface_name] ..... 41
show reference object isakmp policy [isakmp_name] ..... 41
show reference object schedule [object_name] ..... 41
show reference object service [object_name] ..... 41
show reference object sslvpn application [object_name] ..... 41
show reference object sslvpn policy [object_name] ..... 41
show reference object username [username] ..... 41
show reference object zone [object_name] ..... 42
show reference object-group aaa ad [group_name] ..... 42
show reference object-group aaa ldap [group_name] ..... 42
show reference object-group aaa radius [group_name] ..... 42
show reference object-group address [object_name] ..... 42
show reference object-group address6 [object_name] ..... 42
show reference object-group interface [object_name] ..... 42
show reference object-group service [object_name] ..... 42
show reference object-group username [username] ..... 42
show report [interface_name {ip | service | url}] ..... 359
show report packet size statistics {interface_name} [interval interval] ..... 361

show report packet size statistics status .....360
show report status .....359
show rip {global | interface {all | *interface_name*}} .....86
show route order .....369
show running-config .....340
show sa monitor [{begin <1..1000>} | {end <1..1000>} | {crypto-map *regexp*} | {policy *regexp*} |{rsort *sort_order*} | {sort *sort_order*}] .....185
show schedule-object .....283
show serial-number .....43
show service-object [*object_name*] .....279
show service-register content-filter-engine .....49
show service-register reseller-info .....49
show service-register server-type .....49
show service-register status {all|idp|av|sslvpn|sslvpn-status} .....49
show service-register status as .....49
show service-register status content-filter { bluecoat | commtouch } .....49
show session timeout {icmp | tcp-timewait | udp} .....365
show session-limit .....166
show session-limit begin *rule_number* end *rule_number* .....166
show session-limit *rule_number* .....166
show session-limit status .....166
show session-limit6 .....167
show session-limit6 begin *rule_number* end *rule_number* .....167
show session-limit6 *rule_number* .....167
show session-limit6 status .....167
show setenv-startup .....340
show snmp status .....329
show socket listen .....43
show socket open .....43
show software-watchdog-timer log .....383
show software-watchdog-timer status .....383
show sslvpn application [*application_object*] .....302
show sslvpn monitor .....188
show ssl-vpn network-extension local-ip .....188
show sslvpn policy [*profile_name*] .....188
show sso agent .....175
show sso port .....175
show sso presharekey .....175
show system default-interface-group .....115
show system default-snat .....115
show system route default-wan-trunk .....369
show system route dynamic-vpn .....369
show system route nat-1-1 .....369
show system route policy-route .....369
show system route site-to-site-vpn .....369
show system snat default-snat .....369
show system snat nat-1-1 .....369
show system snat nat-loopback .....369
show system snat order .....369
show system snat policy-route .....369
show system uptime .....43
show usb-storage .....101
show username [*username*] .....266
show users {*username* | all | current} .....271
show users default-setting {all | user-type {admin|user|guest|limited-admin|ext-user| ext-group-user}} .....267
show users idle-detection-settings .....268
show users retry-settings .....268
show users simultaneous-logon-settings .....268

show users update-lease-settings ..... 268
show version ..... 43
show vpn-concentrator [*profile_name*] ..... 183
show vpn-configuration-provision activation ..... 184
show vpn-configuration-provision authentication ..... 184
show vpn-configuration-provision rules ..... 184
show vpn-counters ..... 185
show vrpt send device information interval ..... 356
show vrpt send interface statistics interval ..... 356
show vrpt send system status interval ..... 356
show web-auth activation ..... 170
show web-auth default-rule ..... 170
show web-auth exceptional-service ..... 170
show web-auth method ..... 170
show web-auth policy {<1..1024> | all} ..... 170
show web-auth portal status ..... 170
show web-auth status ..... 170
show web-auth user-agreement status ..... 170
show wlan mac-filter ..... 107
show wlan mac-filter status ..... 107
show wlan-macfilter-profile {all | *macfilter_profile_name*} ..... 67
show wlan-radio-profile {all | *radio_profile_name*} ..... 59
show wlan-security-profile {all | *security_profile_name*} ..... 65
show wlan-ssid-profile *{all | ssid_profile_name}* ..... 64
show workspace application ..... 189
show workspace cifs ..... 189
show zone [*profile_name*] ..... 134
show zone binding-iface ..... 134
show zone default-binding ..... 134
show zone none-binding ..... 134
show zone system-default ..... 134
show zone user-define ..... 134
shutdown ..... 36
signature *sid* action {drop | reject-sender | reject-receiver | reject-both} ..... 220
signature *sid* action {drop | reject-sender | reject-receiver | reject-both} ..... 224
signature *sid* log [alert] ..... 220
signature *sid* log [alert] ..... 224
*slot_name* ap-profile *profile_name* ..... 56
smtp-address {*ip* | *hostname*} ..... 361
smtp-auth username *username* password *password* ..... 361
snaplen <68..1512> ..... 378
snmp-server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*}
zone {ALL|*zone_object*} action {accept|deny} ..... 329
snmp-server rule move *rule_number* to *rule_number* ..... 329
split-size <1..2048> ..... 378
ssid ..... 64
ssid *ssid* ..... 106
sslvpn network-extension local-ip *ip* ..... 188
sslvpn no connection username *user_name* ..... 189
sslvpn policy {*profile_name* | *profile_name* append | *profile_name* insert <1..16>} ..... 188
sslvpn policy move <1..16> to <1..16> ..... 189
sslvpn policy rename *profile_name profile_name* ..... 189
sso agent primary ..... 174
sso agent secondary ..... 174
*sso encrypted-presharekey <ciphertext>* ..... 174
*sso presharekey <preshared key>* ..... 174
station-limit <1..255> ..... 106
storage <internal|usbstorage> ..... 378
subframe-ampdu <2..64> ..... 60

system default-interface-group *group-name* ..... 115
tcp-decoder {tcp-xxx} log [alert] ..... 222
telnet ..... 36
test aaa ..... 36
test aaa {server|secure-server} {ad|ldap} host {*hostname*|*ipv4-address*} [host {*hostname*|*ipv4-address*}] port <1..65535> base-dn *base-dn-string* [bind-dn *bind-dn-string* password *password*] login-name-attribute *attribute* [alternative-login-name-attribute *attribute*] account *account-name* ..... 292
tracepath6 {*ipv6* | *hostname*} ..... 379
traceroute ..... 36
traceroute {*ip* | *hostname*} ..... 377
traceroute6 ..... 36
traceroute6 {*ipv6* | *hostname*} ..... 377
traffic-prioritize {tcp-ack|content-filter|dns} bandwidth <0..1048576> priority <1..7> [maximize-bandwidth-usage]; ..... 100
traffic-prioritize {tcp-ack|content-filter|dns} deactivate ..... 100
traffic-prioritize {tcp-ack|content-filter|dns|ipsec-vpn|ssl-vpn} bandwidth <0..1048576> priority <1..7> [maximize-bandwidth-usage]; ..... 74
traffic-prioritize {tcp-ack|content-filter|dns|ipsec-vpn|ssl-vpn} bandwidth <0..1048576> priority <1..7> [maximize-bandwidth-usage]; ..... 75
traffic-prioritize {tcp-ack|content-filter|dns|ipsec-vpn|ssl-vpn} deactivate ..... 74
traffic-prioritize {tcp-ack|content-filter|dns|ipsec-vpn|ssl-vpn} deactivate ..... 75
transform-set *crypto_algo_ah* [*crypto_algo_ah* [*crypto_algo_ah*]] ..... 181
transform-set *crypto_algo_esp* [*crypto_algo_esp* [*crypto_algo_esp*]] ..... 181
transform-set isakmp-algo [isakmp_algo [*isakmp_algo*]] ..... 179
trigger append incoming *service_name* trigger *service_name* ..... 122
trigger delete <1..8> ..... 122
trigger insert <1..8> incoming *service_name* trigger *service_name* ..... 122
trigger move <1..8> to <1..8> ..... 122
tunnel destination *ipv4* ..... 100
tunnel mode [ ipv6ip [ manual | 6to4 ] ] ..... 100
tunnel mode ip gre ..... 100
tunnel source [*ipv4*|*tunnel_bind_interface*|_any] ..... 100
tx-mask *chain_mask* ..... 62
type {external | internal} ..... 170
type {external | internal} ..... 173
type {internal | external | general} ..... 90
udp-decoder {truncated-header | undersize-len | oversize-len} action {drop | reject-sender | reject-receiver | reject-both} ..... 222
udp-decoder {truncated-header | undersize-len | oversize-len} log [alert] ..... 222
udp-filtered-distributed-portscan | udp-filtered-portsweep} details ..... 223
unlock lockout-users {*ip* | console| *ipv6_addr*} ..... 271
*url* ..... 242
*url* [ server *rating_server* ] [ timeout *query_timeout* ] ..... 238
*url* timeout *query_timeout* ..... 238
usb-storage mount ..... 101
usb-storage umount ..... 101
usb-storage warn *number* <*percentage*|megabyte> ..... 101
use-defined-mac ..... 90
user *username* ..... 184
username rename *username username* ..... 266
username *username* [no] description *description* ..... 266
username *username* [no] logon-lease-time <0..1440> ..... 267
username *username* [no] logon-re-auth-time <0..1440> ..... 267
username *username* [no] logon-time-setting <default | manual> ..... 266
username *username* nopassword user-type {admin | guest | limited-admin | user} ..... 266
username *username* password *password* user-type {admin | guest | limited-admin | user} ... 266
username *username* user-type ext-group-user associated-aaa-server *server_profile* group-id *id* 266

username *username* user-type ext-user ..... 266
users default-setting [no] logon-lease-time <0..1440> ..... 267
users default-setting [no] logon-re-auth-time <0..1440> ..... 267
users default-setting [no] user-type <admin |ext-user|guest|limited-admin|user|ext-group-user> 267
users default-setting [no] user-type <admin |ext-user|guest|limited-admin|user|ext-group-user> logon-lease-time <0..1440> ..... 267
users default-setting [no] user-type <admin |ext-user|guest|limited-admin|user|ext-group-user> logon-re-auth-time <0..1440> ..... 268
users force-logout *username* | *ip* | *ipv6_addr* ..... 271
vlan <1..4094> {tag | untag} ..... 56
vlan-id <1..4094> ..... 64
vpn-concentrator rename *profile_name profile_name* ..... 184
vpn-configuration-provision authentication *auth_method* ..... 184
vpn-configuration-provision rule { append | *conf_index* | insert *conf_index* } ..... 184
vpn-configuration-provision rule { delete *conf_index* | move *conf_index* to *conf_index* } .184
vrpt send device information interval <15..3600> ..... 356
vrpt send interface statistics interval <15..3600> ..... 356
vrpt send system status interval <15..3600> ..... 356
web-auth [no] exceptional-service *service_name* ..... 169
web-auth default-rule authentication {required | unnecessary} {no log | log [alert]} ...169
web-auth login setting ..... 169
web-auth method {portal | user-agreement} ..... 169
web-auth policy <1..1024> ..... 169
web-auth policy append ..... 170
web-auth policy delete <1..1024> ..... 170
web-auth policy flush ..... 170
web-auth policy insert <1..1024> ..... 170
web-auth policy move <1..1024> to <1..1024> ..... 170
web-auth user-agreement ..... 170
wep <64 | 128> default-key <1..4> ..... 66
wep-auth-type {open | share} ..... 66
wep-key <1..4> *key* ..... 106
windows-version {windows-2000 | windows-xp | windows-2003 | windows-2008 | windows-vista | windows-7 | windows-2008r2} ..... 308
wlan mac-filter associate <allow | deny> ..... 107
wlan *slot_name* ..... 103
wlan-macfilter-profile rename *macfilter_profile_name1 macfilter_profile_name2* ..... 67
wlan-radio-profile rename *radio_profile_name1 radio_profile_name2* ..... 59
wlan-security-profile rename *security_profile_name1 security_profile_name2* ..... 65
wlan-ssid-profile rename *ssid_profile_name1 ssid_profile_name2* ..... 64
wpa-encrypt {tkip | aes | auto} ..... 66
wpa-psk {*wpa_key* | *wpa_key_64*} ..... 66
write ..... 340
write ..... 36
zone *profile_name* ..... 134