USG ZyWALL Series

CLI Reference Guide

Version 3.00
2/2012
Edition 2

DEFAULT LOGIN	
User Name	**admin**
Password	**1234**

ZyXEL

www.zyxel.com

About This CLI Reference Guide

Intended Audience

This manual is intended for people who want to configure ZLD-based ZyWALLs via Command Line Interface (CLI). You should have at least a basic knowledge of TCP/IP networking concepts and topology. Generally, it is organized by feature as outlined in the web configurator.

Note: This guide is intended as a command reference for a series of products. Therefore many commands or command options in this guide may not be available in your product. See your User's Guide for a list of supported features and details about feature implementation.

Please refer to www.zyxel.com or your product's CD for product specific User Guides and product certifications.

How To Use This Guide

1 Read Chapter 1 on page 23 for how to access and use the CLI (Command Line Interface).

2 Read Chapter 2 on page 37 to learn about the CLI user and privilege modes.

3 Subsequent chapters are arranged by menu item as defined in the web configurator. Read each chapter carefully for detailed information on that menu item.

Note: Some features cannot be configured in both the web configurator and CLI.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

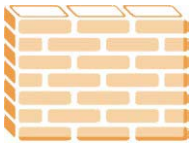
Syntax Conventions

- The ZLD-based ZyWALL may be referred to as the "ZyWALL", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyWALL icon is not an exact representation of your device.

ZyWALL	Computer	Notebook computer

Server	Firewall 	Telephone
Switch	Router	

Contents Overview

Introduction **21**

Command Line Interface 23
User and Privilege Modes 37

Reference **41**

Object Reference 43
Status 45
Registration 49
Interfaces 57
Trunks 97
Route 103
Routing Protocol 111
Zones 115
DDNS 119
Virtual Servers 123
HTTP Redirect 127
ALG 131
IP/MAC Binding 135
Firewall 137
IPSec VPN 145
SSL VPN 155
L2TP VPN 161
Application Patrol 167
Anti-Virus 177
IDP Commands 185
Content Filtering 203
Anti-Spam 215
Device HA 225
User/Group 233
Addresses 241
Services 247
Schedules 251
AAA Server 253
Authentication Objects 259
Certificates 263
ISP Accounts 268
SSL Application 270
Endpoint Security 273

DHCPv6 Objects 280
System 283
System Remote Management 289
File Manager 303
Logs 321
Reports and Reboot 327
Session Timeout 333
Diagnostics 335
Packet Flow Explore 337
Packet Flow Filter 341
Maintenance Tools 345
Watchdog Timer 351

Table of Contents

About This CLI Reference Guide 3

Document Conventions 4

Contents Overview 7

Table of Contents 9

Part I: Introduction 21

Chapter 1
Command Line Interface 23

1.1 Overview 23
1.1.1 The Configuration File 23
1.2 Accessing the CLI 23
1.2.1 Console Port 24
1.2.2 Web Configurator Console 24
1.2.3 Telnet 27
1.2.4 SSH (Secure SHell) 27
1.3 How to Find Commands in this Guide 27
1.4 How Commands Are Explained 28
1.4.1 Background Information (Optional) 28
1.4.2 Command Input Values (Optional) 28
1.4.3 Command Summary 28
1.4.4 Command Examples (Optional) 28
1.4.5 Command Syntax 28
1.4.6 Changing the Password 29
1.5 CLI Modes 29
1.6 Shortcuts and Help 30
1.6.1 List of Available Commands 30
1.6.2 List of Sub-commands or Required User Input 30
1.6.3 Entering Partial Commands 31
1.6.4 Entering a ? in a Command 31
1.6.5 Command History 31
1.6.6 Navigation 31
1.6.7 Erase Current Command 31
1.6.8 The no Commands 31
1.7 Input Values 32
1.8 Ethernet Interfaces 35

1.9 Saving Configuration Changes 35
1.10 Logging Out 36

Chapter 2
User and Privilege Modes 37

2.1 User And Privilege Modes 37
2.1.1 Debug Commands 38

Part II: Reference 41

Chapter 3
Object Reference 43

3.1 Object Reference Commands 43
3.1.1 Object Reference Command Example 44

Chapter 4
Status 45

Chapter 5
Registration 49

5.1 myZyXEL.com Overview 49
5.1.1 Subscription Services Available on the ZyWALL 49
5.2 Registration Commands 50
5.2.1 Command Examples 51
5.3 Country Code 52

Chapter 6
Interfaces 57

6.1 Interface Overview 57
6.1.1 Types of Interfaces 57
6.1.2 Relationships Between Interfaces 60
6.2 Interface General Commands Summary 61
6.2.1 Basic Interface Properties and IP Address Commands 61
6.2.2 DHCP Setting Commands 67
6.2.3 Interface Parameter Command Examples 71
6.2.4 RIP Commands 72
6.2.5 OSPF Commands 72
6.2.6 Connectivity Check (Ping-check) Commands 74
6.3 Ethernet Interface Specific Commands 75
6.3.1 MAC Address Setting Commands 75
6.3.2 Port Grouping Commands 76
6.4 Virtual Interface Specific Commands 77

6.4.1 Virtual Interface Command Examples 77
6.5 PPPoE/PPTP Specific Commands 78
6.5.1 PPPoE/PPTP Interface Command Examples 79
6.6 Cellular Interface Specific Commands 80
6.6.1 Cellular Status 82
6.6.2 Cellular Interface Command Examples 84
6.7 Tunnel Interface Specific Commands 85
6.7.1 Tunnel Interface Command Examples 86
6.8 USB Storage Specific Commands 86
6.8.1 USB Storage General Commands Example 87
6.9 WLAN Specific Commands 87
6.9.1 WLAN General Commands 88
6.9.2 WLAN Interface Commands 89
6.9.3 WLAN MAC Filter Commands 91
6.10 VLAN Interface Specific Commands 92
6.10.1 VLAN Interface Command Examples 93
6.11 Bridge Specific Commands 93
6.11.1 Bridge Interface Command Examples 94
6.12 Auxiliary Interface Specific Commands 94
6.12.1 Auxiliary Interface Command Examples 95

Chapter 7
Trunks 97

7.1 Trunks Overview 97
7.2 Trunk Scenario Examples 97
7.3 Trunk Commands Input Values 98
7.4 Trunk Commands Summary 98
7.5 Trunk Command Examples 99
7.6 Link Sticking 100
7.7 Link Sticking Commands Summary 101
7.8 Link Sticking Command Example 101

Chapter 8
Route 103

8.1 Policy Route 103
8.2 Policy Route Commands 103
8.2.1 Assured Forwarding (AF) PHB for DiffServ 108
8.2.2 Policy Route Command Example 108
8.3 IP Static Route 109
8.4 Static Route Commands 109
8.4.1 Static Route Commands Examples 110

Chapter 9
Routing Protocol 111

9.1 Routing Protocol Overview 111
9.2 Routing Protocol Commands Summary 111
9.2.1 RIP Commands 112
9.2.2 General OSPF Commands 112
9.2.3 OSPF Area Commands 113
9.2.4 Virtual Link Commands 113
9.2.5 Learned Routing Information Commands 114
9.2.6 show ip route Command Example 114

Chapter 10
Zones 115

10.1 Zones Overview 115
10.2 Zone Commands Summary 116
10.2.1 Zone Command Examples 117

Chapter 11
DDNS 119

11.1 DDNS Overview 119
11.2 DDNS Commands Summary 120

Chapter 12
Virtual Servers 123

12.1 Virtual Server Overview 123
12.1.1 1:1 NAT and Many 1:1 NAT 123
12.2 Virtual Server Commands Summary 123
12.2.1 Virtual Server Command Examples 125
12.2.2 Tutorial - How to Allow Public Access to a Server 126

Chapter 13
HTTP Redirect 127

13.1 HTTP Redirect Overview 127
13.1.1 Web Proxy Server 127
13.2 HTTP Redirect Commands 128
13.2.1 HTTP Redirect Command Examples 129

Chapter 14
ALG 131

14.1 ALG Introduction 131
14.2 ALG Commands 132
14.3 ALG Commands Example 133

Chapter 15
IP/MAC Binding 135

15.1 IP/MAC Binding Overview 135
15.2 IP/MAC Binding Commands 135
15.3 IP/MAC Binding Commands Example 136

Chapter 16
Firewall 137

16.1 Firewall Overview 137
16.2 Firewall Commands 138
16.2.1 Firewall Sub-Commands 141
16.2.2 Firewall Command Examples 142
16.3 Session Limit Commands 143

Chapter 17
IPSec VPN 145

17.1 IPSec VPN Overview 145
17.2 IPSec VPN Commands Summary 146
17.2.1 IKE SA Commands 147
17.2.2 IPSec SA Commands (except Manual Keys) 148
17.2.3 IPSec SA Commands (for Manual Keys) 151
17.2.4 VPN Concentrator Commands 151
17.2.5 VPN Configuration Provisioning Commands 152
17.2.6 SA Monitor Commands 153

Chapter 18
SSL VPN 155

18.1 SSL Access Policy 155
18.1.1 SSL Application Objects 155
18.1.2 SSL Access Policy Limitations 155
18.2 SSL VPN Commands 155
18.2.1 SSL VPN Commands 156
18.2.2 Setting an SSL VPN Rule Tutorial 157

Chapter 19
L2TP VPN 161

19.1 L2TP VPN Overview 161
19.2 IPSec Configuration 161
19.2.1 Using the Default L2TP VPN Connection 162
19.3 Policy Route 162
19.4 L2TP VPN Commands 163
19.4.1 L2TP VPN Commands 163
19.5 L2TP VPN Example 164
19.5.1 Configuring the Default L2TP VPN Gateway Example 165
19.5.2 Configuring the Default L2TP VPN Connection Example 165

19.5.3 Configuring the L2TP VPN Settings Example 165
19.5.4 Configuring the Policy Route for L2TP Example 166

Chapter 20
Application Patrol 167

20.1 Application Patrol Overview 167
20.2 Application Patrol Commands Summary 167
20.2.1 Pre-defined Application Commands 168
20.2.2 Rule Commands for Pre-defined Applications 168
20.2.3 Exception Commands for Pre-defined Applications 170
20.2.4 Other Application Commands 171
20.2.5 Rule Commands for Other Applications 171
20.2.6 General Commands for Application Patrol 172

Chapter 21
Anti-Virus 177

21.1 Anti-Virus Overview 177
21.2 Anti-virus Commands 177
21.2.1 General Anti-virus Commands 178
21.2.2 Zone to Zone Anti-virus Rules 178
21.2.3 White and Black Lists 180
21.2.4 Signature Search Anti-virus Command 181
21.3 Update Anti-virus Signatures 182
21.3.1 Update Signature Examples 183
21.4 Anti-virus Statistics 183
21.4.1 Anti-virus Statistics Example 184

Chapter 22
IDP Commands 185

22.1 Overview 185
22.2 General IDP Commands 185
22.2.1 IDP Activation 185
22.3 IDP Profile Commands 186
22.3.1 Global Profile Commands 186
22.3.2 IDP Zone to Zone Rules 187
22.3.3 Editing/Creating IDP Signature Profiles 188
22.3.4 Editing/Creating Anomaly Profiles 188
22.3.5 Editing System Protect 192
22.3.6 Signature Search 192
22.4 IDP Custom Signatures 195
22.4.1 Custom Signature Examples 196
22.5 Update IDP Signatures 199
22.5.1 Update Signature Examples 200

22.6 IDP Statistics 200
22.6.1 IDP Statistics Example 201

Chapter 23
Content Filtering 203

23.1 Content Filtering Overview 203
23.2 Content Filtering Policies 203
23.3 External Web Filtering Service 203
23.4 Content Filtering Reports 203
23.5 Content Filter Command Input Values 204
23.6 General Content Filter Commands 205
23.7 Content Filter Filtering Profile Commands 207
23.8 Content Filter URL Cache Commands 209
23.9 Content Filtering Statistics 210
23.9.1 Content Filtering Statistics Example 211
23.10 Content Filtering Commands Example 211

Chapter 24
Anti-Spam 215

24.1 Anti-Spam Overview 215
24.2 Anti-Spam Commands 215
24.2.1 General Anti-Spam Commands 215
24.2.2 Zone to Zone Anti-spam Rules 216
24.2.3 White and Black Lists 218
24.2.4 DNSBL Anti-Spam Commands 220
24.3 Anti-Spam Statistics 223
24.3.1 Anti-Spam Statistics Example 223

Chapter 25
Device HA 225

25.1 Device HA Overview 225
25.1.1 Before You Begin 226
25.2 General Device HA Commands 226
25.3 Active-Passive Mode Device HA 226
25.4 Active-Passive Mode Device HA Commands 227
25.4.1 Active-Passive Mode Device HA Commands 227
25.4.2 Active-Passive Mode Device HA Command Example 229
25.5 Legacy Mode (VRRP) Device HA 229
25.6 Legacy Mode (VRRP) Device HA Commands 229
25.6.1 VRRP Group Commands 230
25.6.2 VRRP Synchronization Commands 230
25.6.3 Link Monitoring Commands 231

Chapter 26
User/Group 233

26.1 User Account Overview 233
26.1.1 User Types 233
26.2 User/Group Commands Summary 234
26.2.1 User Commands 234
26.2.2 User Group Commands 235
26.2.3 User Setting Commands 235
26.2.4 Force User Authentication Commands 237
26.2.5 Additional User Commands 239

Chapter 27
Addresses 241

27.1 Address Overview 241
27.2 Address Commands Summary 241
27.2.1 Address Object Commands 242
27.2.2 Address Group Commands 244

Chapter 28
Services 247

28.1 Services Overview 247
28.2 Services Commands Summary 247
28.2.1 Service Object Commands 247
28.2.2 Service Group Commands 248

Chapter 29
Schedules 251

29.1 Schedule Overview 251
29.2 Schedule Commands Summary 251
29.2.1 Schedule Command Examples 252

Chapter 30
AAA Server 253

30.1 AAA Server Overview 253
30.2 Authentication Server Command Summary 253
30.2.1 ad-server Commands 253
30.2.2 ldap-server Commands 254
30.2.3 radius-server Commands 255
30.2.4 radius-server Command Example 255
30.2.5 aaa group server ad Commands 255
30.2.6 aaa group server ldap Commands 256
30.2.7 aaa group server radius Commands 257
30.2.8 aaa group server Command Example 258

Chapter 31
Authentication Objects 259

31.1 Authentication Objects Overview 259
31.2 aaa authentication Commands 259
31.2.1 aaa authentication Command Example 260
31.3 test aaa Command 260
31.3.1 Test a User Account Command Example 260

Chapter 32
Certificates 263

32.1 Certificates Overview 263
32.2 Certificate Commands 263
32.3 Certificates Commands Input Values 263
32.4 Certificates Commands Summary 264
32.5 Certificates Commands Examples 267

Chapter 33
ISP Accounts 268

33.1 ISP Accounts Overview 268
33.1.1 PPPoE and PPTP Account Commands 268
33.1.2 Cellular Account Commands 269

Chapter 34
SSL Application 270

34.1 SSL Application Overview 270
34.1.1 SSL Application Object Commands 270
34.1.2 SSL Application Command Examples 272

Chapter 35
Endpoint Security 273

35.1 Endpoint Security Overview 273
35.1.1 Endpoint Security Commands Summary 274
35.1.2 Endpoint Security Object Commands 274
35.1.3 Endpoint Security Object Command Example 277

Chapter 36
DHCPv6 Objects 280

36.1 DHCPv6 Object Commands Summary 280
36.1.1 DHCPv6 Object Commands 280
36.1.2 DHCPv6 Object Command Examples 281

Chapter 37
System 283

37.1 System Overview 283
37.2 Customizing the WWW Login Page 283
37.3 Host Name Commands 285
37.4 Time and Date 285
37.4.1 Date/Time Commands 286
37.5 Console Port Speed 286
37.6 DNS Overview 287
37.6.1 Domain Zone Forwarder 287
37.6.2 DNS Commands 287
37.6.3 DNS Command Example 288

Chapter 38
System Remote Management 289

38.1 Remote Management Overview 289
38.1.1 Remote Management Limitations 289
38.1.2 System Timeout 289
38.2 Common System Command Input Values 290
38.3 HTTP/HTTPS Commands 290
38.3.1 HTTP/HTTPS Command Examples 292
38.4 SSH 292
38.4.1 SSH Implementation on the ZyWALL 292
38.4.2 Requirements for Using SSH 292
38.4.3 SSH Commands 293
38.4.4 SSH Command Examples 293
38.5 Telnet 294
38.6 Telnet Commands 294
38.6.1 Telnet Commands Examples 294
38.7 Configuring FTP 295
38.7.1 FTP Commands 295
38.7.2 FTP Commands Examples 296
38.8 SNMP 296
38.8.1 Supported MIBs 296
38.8.2 SNMP Traps 296
38.8.3 SNMP Commands 297
38.8.4 SNMP Commands Examples 297
38.9 ICMP Filter 298
38.10 Dial-in Management 298
38.10.1 AT Command Strings 299
38.10.2 DTR Signal 299
38.10.3 Response Strings 299
38.10.4 Dial-in Management Commands 299
38.11 Vantage CNM 300
38.11.1 Vantage CNM Commands 300

38.12 Language Commands 301
38.13 IPv6 Commands 302

Chapter 39
File Manager 303

39.1 File Directories 303
39.2 Configuration Files and Shell Scripts Overview 303
39.2.1 Comments in Configuration Files or Shell Scripts 304
39.2.2 Errors in Configuration Files or Shell Scripts 305
39.2.3 ZyWALL Configuration File Details 305
39.2.4 Configuration File Flow at Restart 306
39.3 File Manager Commands Input Values 306
39.4 File Manager Commands Summary 307
39.5 File Manager Command Examples 308
39.6 FTP File Transfer 308
39.6.1 Command Line FTP File Upload 308
39.6.2 Command Line FTP Configuration File Upload Example 309
39.6.3 Command Line FTP File Download 309
39.6.4 Command Line FTP Configuration File Download Example 310
39.7 ZyWALL File Usage at Startup 310
39.8 Notification of a Damaged Recovery Image or Firmware 311
39.9 Restoring the Recovery Image 312
39.10 Restoring the Firmware 314
39.11 Restoring the Default System Database 316
39.11.1 Using the atkz -u Debug Command 318

Chapter 40
Logs 321

40.1 Log Commands Summary 321
40.1.1 Log Entries Commands 322
40.1.2 System Log Commands 322
40.1.3 Debug Log Commands 323
40.1.4 E-mail Profile Commands 324
40.1.5 Console Port Logging Commands 326

Chapter 41
Reports and Reboot 327

41.1 Report Commands Summary 327
41.1.1 Report Commands 327
41.1.2 Report Command Examples 328
41.1.3 Session Commands 328
41.1.4 Packet Size Statistics Commands 328
41.2 Email Daily Report Commands 329

41.2.1 Email Daily Report Example 330
41.3 Reboot 332

Chapter 42
Session Timeout 333

Chapter 43
Diagnostics 335

43.1 Diagnostics 335
43.2 Diagnosis Commands 335
43.3 Diagnosis Commands Example 335

Chapter 44
Packet Flow Explore 337

44.1 Packet Flow Explore 337
44.2 Packet Flow Explore Commands 337
44.3 Packet Flow Explore Commands Example 338

Chapter 45
Packet Flow Filter 341

45.1 Packet Flow Filter 341
45.2 Packet Flow Filter Commands 341
45.3 Packet Flow Filter Commands Examples 342

Chapter 46
Maintenance Tools 345

46.1 Maintenance Command Examples 347
46.1.1 Packet Capture Command Example 348

Chapter 47
Watchdog Timer 351

47.1 Hardware Watchdog Timer 351
47.2 Software Watchdog Timer 351
47.3 Application Watchdog 352
47.3.1 Application Watchdog Commands Example 352

List of Commands (Alphabetical) 355

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, 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 and possibly render it unusable.

1.1.1 The Configuration File

When you configure the ZyWALL 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. You can store more than one configuration file on the ZyWALL. However, only one configuration file is used at a time.

You can perform the following with a configuration file:

- Back up ZyWALL configuration once the ZyWALL is set up to work in your network.
- Restore ZyWALL configuration.
- Save and edit a configuration file and upload it to multiple ZyWALLs (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 using Telnet or SSH (Secure SHell).

Note: The ZyWALL might force you to log out of your session if reauthentication time, lease time, or idle timeout is reached. See Chapter 26 on page 233 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: Console Port

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

When you turn on your ZyWALL, 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's.
- No text displays if the speed is set higher than the ZyWALL's.
- If changing your terminal emulation program's speed does not get anything to display, restart the ZyWALL.
- If restarting the ZyWALL 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 20W

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. Follow the steps below to access the web console.

1 Log into the web configurator.

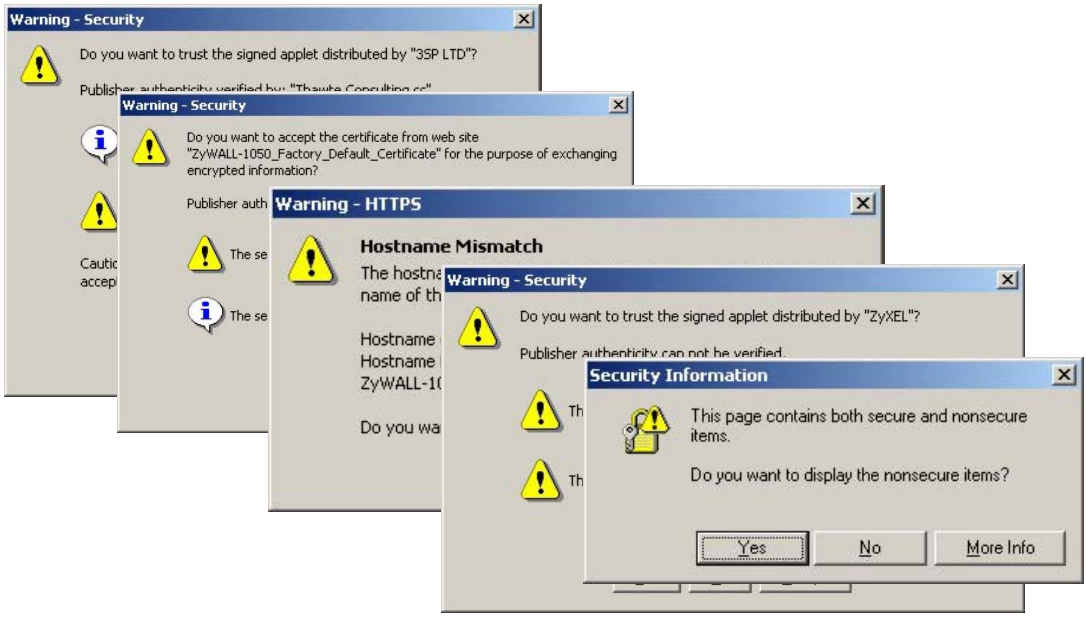
2 Click the **Console** icon in the top-right corner of the web configurator screen.

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.

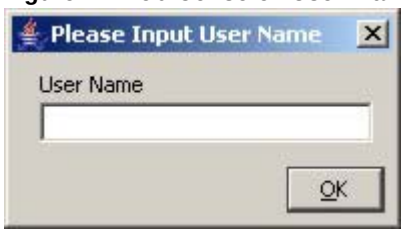
4 The web console starts. This might take a few seconds. One or more security screens may display. Click **Yes** or **Always**.

Figure 3 Web Console: Security Warnings



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

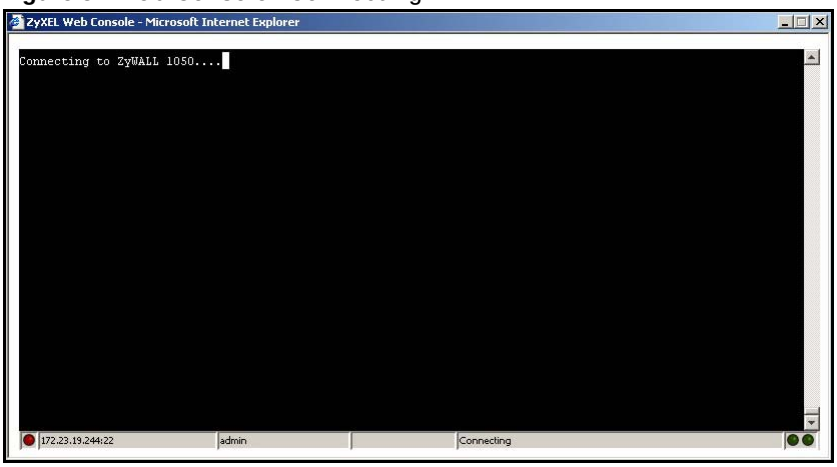
Figure 4 Web Console: User Name



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

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

Figure 5 Web Console: Connecting

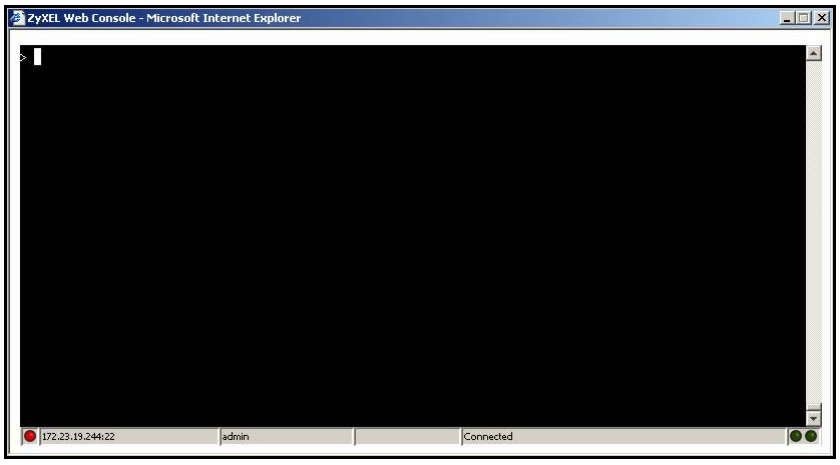


Then, the **Password** screen appears.

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.

1 If your computer is connected to the ZyWALL over the Internet, skip to the next step. Make sure your computer IP address and the ZyWALL 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'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. See Section 26.2 on page 234 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) • Run basic diagnostics	• Look at system information (like **Status** screen) • Run basic diagnostics	Unable to access	Unable to access
What **Admin** users can do	• Look at system information (like **Status** screen) • Run basic diagnostics	• Look at system information (like **Status** screen) • Run basic diagnostics	• Configure simple features (such as an address object) • Create or remove complex parts (such as an interface)	• Configure complex parts (such as an interface) in the ZyWALL
How you enter it	Log in to the ZyWALL	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)
				`Router(zone)#`
				`Router(config-if-ge)#`
				`...`

How you exit it	Type **exit**	Type **disable**	Type **exit**	Type **exit**

See Chapter 26 on page 233 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 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 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 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 treating it as a help query.

1.6.5 Command History

The ZyWALL 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 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 16-20	“0x” or “0X” + 32-40 hexadecimal values 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 .- first character: alphanumeric or -
connection_id	1+	alphanumeric or -_:
contact	1-61	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-.
country code	0 or 2	alphanumeric
custom signature file name	0-30	alphanumeric or _-. first character: letter
description	Used in keyword criteria for log entries	
	1-64	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-.
	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 .- first character: alphanumeric or -
	Used in domainname, ip dhcp pool, and ip domain	
	0-254	alphanumeric or ._- first character: alphanumeric or -
email	1-63	alphanumeric or .@_-
e-mail	1-64	alphanumeric or .@_-
encryption key	16-64 8-32	“0x” or “0X” + 16-64 hexadecimal values 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 .- first character: alphanumeric or -
	Used in ip ddns, time server, device HA, VPN, certificates, and interface ping check	
	0-254	alphanumeric or .- first character: alphanumeric or -
full file name	0-256	alphanumeric or _/.-
hostname	Used in hostname command	
	0-63	alphanumeric or .-_ first character: alphanumeric or -
	Used in other commands	
	0-252	alphanumeric or .- first character: alphanumeric or -
import configuration file	1-26+”.conf”	alphanumeric or ;`~!@#$%^&()_+[]{}',.=- add “.conf” at the end
import shell script	1-26+”.zysh”	alphanumeric or ;`~!@#$%^&()_+[]{}',.=- 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. IPv6 addresses can be abbreviated in two ways: 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. 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 alphanumeric or ;|`~!@#$%^&*()_+\{}':,./<>=-
profile name	0-30	alphanumeric or _- first character: letters or _-
proto name	1-16	lower-case letters, numbers, or -
protocol name	0-30	alphanumeric or _- first character: letters or _-
quoted string less than 127 chars	1-255	alphanumeric, spaces, or ;/?:@&=+$\.-_!~*'()%,
quoted string less than 63 chars	1-63	alphanumeric, spaces, or ;/?:@&=+$\.-_!~*'()%
quoted string	0+	alphanumeric, spaces, or punctuation marks enclosed in double quotation marks (“) 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 '()+,/:.=?;!*#@$_%-
url	Used in content filtering redirect	
	"http://"+ "https://"+	alphanumeric or ;/?:@&=+$\.-_!~*'()%, starts with "http://" or "https://" may contain one pound sign (#)
	Used in other content filtering commands	
	"http://"+	alphanumeric or ;/?:@&=+$\.-_!~*'()%, starts with "http://" may contain one pound sign (#)
user name	Used in VPN extended authentication	
	1-31	alphanumeric or _-
	Used in other commands	
	0-30	alphanumeric or _- first character: letters or _-
username	6-20	alphanumeric or .@_- registration
user name	1+	alphanumeric or -_. logging commands
user@domainname	1-80	alphanumeric or .@_-
vrrp group name: less than 15 chars	1-15	alphanumeric or _-
week-day sequence, i.e. 1=first,2=second	1	1-4
xauth method	1-31	alphanumeric or _-
xauth password	1-31	alphanumeric or ;|`~!@#$%^&*()_+\{}':,./<>=-
mac address	0-12 (even number)	hexadecimal for example: aa aabbcc aabbccddeeff

1.8 Ethernet Interfaces

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

- For the ZyWALL USG 300 and above, use ge*x*, *x* = 1~N, where N equals the highest numbered Ethernet interface for your ZyWALL model.
- The ZyWALL 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.

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 uses. See Chapter 26 on page 233 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 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. 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. 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. All unsaved changes are lost after the ZyWALL 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'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's current operational state.

Table 7 Status Show Commands

COMMAND	DESCRIPTION
show boot status	Displays details about the ZyWALL'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.
show mac	Displays the ZyWALL's MAC address.
show mem status	Displays what percentage of the ZyWALL's memory is currently being used.
show ram-size	Displays the size of the ZyWALL's on-board RAM.
show redundant-power status	Displays the status of the ZyWALL's power modules. The ZyWALL 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.
show socket listen	Displays the ZyWALL's listening ports
show socket open	Displays the ports that are open on the ZyWALL.
show system uptime	Displays how long the ZyWALL has been running since it last restarted or was turned on.
show version	Displays the ZyWALL'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 100
firmware version: 2.20(AQQ.0)b3
BM version      : 1.08
build date      : 2009-11-21 01:18:06
```

This example shows the current LED states on the ZyWALL. 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 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 and manage subscription services available for the ZyWALL.

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 and activate a service using the **Licensing > Registration** screens. Alternatively, go to http://www.myZyXEL.com with the ZyWALL'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, you need to access myZyXEL.com via that ZyWALL.

5.1.1 Subscription Services Available on the ZyWALL

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

- The ZyWALL's anti-virus packet scanner uses the signature files on the ZyWALL to detect virus files. Your ZyWALL 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 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 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. 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 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 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 accesses an external database that has millions of web sites categorized based on content. You can have the ZyWALL 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 and activate the corresponding service at myZyXEL.com (through the ZyWALL).

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. *country_code*: see Table 10 on page 52
`service-register checkexpire`	Gets information of all service subscriptions from myZyXEL.com and updates the status table.

Table 9 Command Summary: Registration (continued)

COMMAND	DESCRIPTION
`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 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 is set to use for content filtering.
`service-register content-filter-engine { bluecoat | commtouch }`	Sets whether the ZyWALL 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'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.

```
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
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

Table 10 Country Codes (continued)

COUNTRY CODE	COUNTRY NAME	COUNTRY CODE	COUNTRY NAME
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
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

Table 10 Country Codes (continued)

COUNTRY CODE	COUNTRY NAME	COUNTRY CODE	COUNTRY NAME
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
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

Table 10 Country Codes (continued)

COUNTRY CODE	COUNTRY NAME	COUNTRY CODE	COUNTRY NAME
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

Interfaces

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

6.1 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.

6.1.1 Types of Interfaces

You can create several types of interfaces in the ZyWALL. The types supported vary by ZyWALL 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 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. 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. 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 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 11 Characteristics of Ethernet, VLAN, Bridge, PPPoE/PPTP, and Virtual Interface (ZyWALL 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 12 Ethernet, VLAN, Bridge, PPP, and Virtual Interface Characteristics (ZyWALL 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 12 Ethernet, VLAN, Bridge, PPP, and Virtual Interface Characteristics (ZyWALL 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 13 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.

6.1.2 Relationships Between Interfaces

In the ZyWALL, 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 14 Relationships Between Different Types of Interfaces

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

6.2 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 15 Input Values for General Interface Commands

LABEL	DESCRIPTION
interface_name	The name of the interface. Ethernet interface: For the ZyWALL USG 300 and above, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL model. ZyWALL USG 200 and below models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. 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 VLAN interface: vlan*x*, *x* = 0 - 4094 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 4 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ZyWALL model supports. virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL 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 6.6 on page 80 for the unique commands for each type of interface.

6.2.1 Basic Interface Properties and IP Address Commands

This table lists basic properties and IP address commands.

Table 16 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 6.6.1 on page 82 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 16 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 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. *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. 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 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 16 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 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 obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. *dhcp6_profile*: Specify the DHCPv6 request object to use. *dhcp6_suffix_128*: Specify the ending part of the IPv6 address, a slash (/), and the prefix length. The ZyWALL appends it to the delegated prefix. 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 16 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. *dhcp6_profile*: Specify the DHCPv6 request object to use for generating the network prefix for the network. *dhcp6_suffix_64*: Specify the ending part of the IPv6 network address plus a slash (/) and the prefix length. The ZyWALL appends it to the selected delegated prefix. The combined address is the network prefix for the network. 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. 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 16 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 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 not get this interface's IPv6 address from the DHCPv6 server.
dhcp6 rapid-commit	Has the ZyWALL use the full four-step DHCPv6 message exchange process. 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 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. *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. *user_defined_name*: • This name cannot be one of the follows: "ethernet", "ppp", "vlan", "bridge", "virtual", "wlan", "cellular", "aux", "tunnel", "status", "summary", "all" • This name cannot begin with one of the follows either: "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.

6.2.1.1 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. 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. 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)#
```

6.2.2 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 17 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. About the sub-command settings: • If you use the `host` command, the ZyWALL treats this DHCP pool as a static DHCP entry. • If you do not use the `host` command and use the `network` command, the ZyWALL treats this DHCP pool as a pool of IP addresses. • 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. The `no` command removes the specified DHCP pool.
`show`	Shows information about the specified DHCP pool.
	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.

Table 17 interface Commands: DHCP Settings (continued)

COMMAND	DESCRIPTION
[no] host *ip*	Specifies the static IP address the ZyWALL should assign. Use this command, along with hardware-address, to create a static DHCP entry. Note: The IP address must be in the same subnet as the interface to which you plan to bind the DHCP pool. When this command is used, the ZyWALL 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. *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. *text*: String of up to 250 characters *hex*: String of up to 250 hexadecimal pairs. *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. *enterprise_id*: Number <0..4294967295>. *hex_s*: String of up to 120 hexadecimal pairs. *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> network *ip mask* 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. Note: The DHCP pool must have the same subnet as the interface to which you plan to bind it. 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.
[no] domain-name *domain_name*	Specifies the domain name assigned to DHCP clients. The no command clears this field.

Table 17 interface Commands: DHCP Settings (continued)

COMMAND	DESCRIPTION
[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. Note: You must specify the network number first, and the start address must be in the same subnet. 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 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 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 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.

6.2.2.1 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
```

6.2.2.2 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
```

6.2.3 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 18 Examples for Different Interface Parameters

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

Table 18 Examples for Different Interface Parameters

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

6.2.4 RIP Commands

This table lists the commands for RIP settings.

Table 19 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 9 on page 111 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.

6.2.5 OSPF Commands

This table lists the commands for OSPF settings.

Table 20 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 20 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. *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. *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 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 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 waits for an acknowledgment in response to a link state advertisement before it re-sends the advertisement. Link state advertisements (LSA) are used to share the link state and routing information between routers.

6.2.6 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 stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway passes the connectivity check.

This table lists the ping-check commands

Table 21 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. 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 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 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 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 pings for the ping check and sets the number of seconds the ZyWALL waits for a response.
ping-check {*domain_name* | *ip* | default-gateway} fail-tolerance <1..10>	Specifies what the ZyWALL pings for the ping check and sets the number of times the ZyWALL times out before it stops routing through the specified interface.
ping-check {*domain_name* | *ip* | default-gateway} method {icmp | tcp}	Sets how the ZyWALL checks the connection to the gateway. icmp: ping the gateway you specify to make sure it is still available. 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.

6.2.6.1 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)#
```

6.3 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 22 Input Values for Ethernet Interface Commands

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

6.3.1 MAC Address Setting Commands

This table lists the commands you can use to set the MAC address of an interface. On the ZyWALL USG 200 and below models, these commands only apply to a WAN or OPT interface.

Table 23 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 23 interface Commands: MAC Setting (continued)

COMMAND	DESCRIPTION
type {internal | external | general}	Sets which type of network you will connect this interface. The ZyWALL automatically adds default route and SNAT settings for traffic it routes from internal interfaces to external interfaces; for example LAN to WAN traffic. internal: Set this to connect to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The ZyWALL automatically adds default SNAT settings for traffic flowing from this interface to an external interface. external: Set this to connect to an external network (like the Internet). The ZyWALL automatically adds this interface to the default WAN trunk. 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.

6.3.2 Port Grouping Commands

This section covers commands that are specific to port grouping.

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

Table 24 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. *representative_interface*: ge*x* in a ZyWALL USG 300 or above. A dmz, ext-wlan, or lan1 interface in a ZyWALL USG 100 or 200. <1..*x*> where *x* equals the highest numbered port for your ZyWALL 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.

6.3.2.1 Port Grouping Command Examples

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

```
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    yes
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    no
```

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
```

6.4 Virtual Interface Specific Commands

Virtual interfaces use many of the general interface commands discussed at the beginning of Section 6.2 on page 61. There are no additional commands for virtual interfaces.

6.4.1 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
```

6.5 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 6.2 on page 61.

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 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 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 26 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.
`[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 get the IP address of the PPPoE/PPTP server automatically when it establishes the connection.

Table 26 interface Commands: PPPoE/PPTP Interfaces (continued)

COMMAND	DESCRIPTION
[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 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 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. *dhcp6_profile*: Specify the DHCPv6 request object to use. *dhcp6_suffix_128*: Specify the ending part of the IPv6 address, a slash (/), and the prefix length. The ZyWALL appends it to the delegated prefix. 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 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.
show interface ppp user-define	Displays all PPP interfaces that were manually configured on the ZyWALL.

6.5.1 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
```

6.6 Cellular Interface Specific Commands

Use a 3G (Third Generation) cellular device with the ZyWALL 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 27 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. auto has the ZyWALL always use the fastest network that is in range. 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 does not spend time looking for a WCDMA network. 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 27 Cellular Interface Commands (continued)

COMMAND	DESCRIPTION
[no] network-selection {auto|home}	Home network is the network to which you are originally subscribed. Home has the 3G device connect only to the home network. If the home network is down, the ZyWALL's 3G Internet connection is also unavailable. 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 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 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. download: set a limit on the downstream traffic (from the ISP to the ZyWALL). upload: set a limit on the upstream traffic (from the ZyWALL to the ISP). download-upload: set a limit on the total traffic in both directions. If you change the value, the ZyWALL resets the statistics. Use the no command to disable data budget control.
budget reset-day <0..31>	Sets the date on which the ZyWALL resets the budget every month. If the date you selected is not available in a month, such as 30th or 31st, the ZyWALL 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 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 to not create a log when the time or data limit is exceeded. Specify recursive to have the ZyWALL 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. If you set budget new-connection to disallow and budget current-connection to keep, the ZyWALL allows you to transmit data using the current connection, but you cannot build a new connection if the existing connection is disconnected.

Table 27 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 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 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. You can also set how often (from 1 to 65535 minutes) to send the log or alert.
no budget log-percentage	Sets the ZyWALL 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 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 can support.
show interface cellular budget-auto-save	Displays how often (in minutes) the ZyWALL 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 6.6.1 on page 82 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.

6.6.1 Cellular Status

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

Table 28 Cellular Status

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

Table 28 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's test of the 3G device failed.
Probe device ok	the ZyWALL's test of the 3G device failed.
Init device fail	the ZyWALL was not able to initialize the 3G device.
Init device ok	the ZyWALL initialized the 3G card.
Check lock fail	the ZyWALL'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 cannot get cellular device information.
Get dev-info ok	The ZyWALL 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 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.
Correct device	The ZyWALL detected a compatible 3G device.
Set band fail	Applying your band selection was not successful.
Set band ok	The ZyWALL successfully applied your band selection.
Set profile fail	Applying your ISP settings was not successful.
Set profile ok	The ZyWALL successfully applied your ISP settings.
PPP fail	The ZyWALL 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 successfully applied all of your configuration and you can use the 3G connection.

6.6.2 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.

```
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. 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!-----------------------------------------------
```

6.7 Tunnel Interface Specific Commands

The ZyWALL 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 6.2 on page 61.

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 6.2.6 on page 74 for more on ping check.

Table 29 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. *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. _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 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. manual: Use for a point-to-point manual tunnel for IPv6 transition. You must also configure a policy route for the tunnel. 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.

6.7.1 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
```

6.8 USB Storage Specific Commands

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

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

Table 30 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 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 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 30 USB Storage General Commands (continued)

COMMAND	DESCRIPTION
`[no] diag-info copy usb-storage`	Sets to have the ZyWALL 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 saves the current system diagnostics information to the connected USB storage device.
`[no] corefile copy usb-storage`	Sets to have the ZyWALL 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 saves core dump files to the connected USB storage device.

6.8.1 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
```

6.9 WLAN Specific Commands

You can install a compatible WLAN card to use the ZyWALL 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 31 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 33 on page 89

6.9.1 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 32 WLAN General Commands

COMMAND	DESCRIPTION
`wlan slot_name`	Specifies the slot the WLAN card is installed in and enters sub-command mode. *slot_name*: The name of the slot where the WLAN card is installed in the ZyWALL. 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. • b • g • b or g • b, g, or n • g or n.
`channel <wireless_channel | auto>`	Sets the wireless operating channel of an IEEE 802.11n interface. *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. short: increases data throughput but may make data transfer more prone to errors. 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. none: Apply no priority to traffic. 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 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.
`qos [none | wmm}`	Applies Wi-Fi Multimedia Quality of Service (QoS) or no wireless QoS.

Table 32 WLAN General Commands (continued)

COMMAND	DESCRIPTION
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.

6.9.1.1 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)#
```

6.9.2 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 33 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. *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 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 33 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 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. none: applies no security. wep: WEP security (extremely weak). wpa: WPA security. wpa-wpa2: WPA/WPA2-Enterprise or WPA/WPA2-PSK security. 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 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 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 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.
[no] security external acct *ip* port <1..65535>	Sets the IP address and port number of an external accounting server.

Table 33 WLAN Interface Commands (continued)

COMMAND	DESCRIPTION
[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 must have the same SSID. *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. 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. 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.

6.9.2.1 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
```

6.9.3 WLAN MAC Filter Commands

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

Table 34 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. The no command removes the entry. *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.

Table 34 WLAN General Commands (continued)

COMMAND	DESCRIPTION
`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, MAC addresses not listed will be blocked. 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.

6.9.3.1 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 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
```

6.10 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 6.2 on page 61.

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

Table 35 Input Values for VLAN Interface Commands

LABEL	DESCRIPTION
interface_name	VLAN interface: vlan*x*, *x* = 0 - 4094 Ethernet interface: For the ZyWALL USG 300 and above, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL model. The ZyWALL 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 36 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.

Table 36 interface Commands: VLAN Interfaces (continued)

COMMAND	DESCRIPTION
[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.

6.10.1 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
```

6.11 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 6.2 on page 61.

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

Table 37 Input Values for Bridge Interface Commands

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

This table lists the bridge interface commands.

Table 38 interface Commands: Bridge Interfaces

COMMAND	DESCRIPTION
interface *interface_name*	Creates the specified interface if necessary and enters sub-command mode.

Table 38 interface Commands: Bridge Interfaces (continued)

COMMAND	DESCRIPTION
[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.

6.11.1 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
```

6.12 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 39 interface Commands: Auxiliary Interface

COMMAND	DESCRIPTION
interface dial aux 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”. *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. *password*: You can use up to 63 printable ASCII characters. Spaces are not allowed.

Table 39 interface Commands: Auxiliary Interface (continued)

COMMAND	DESCRIPTION
[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. *username*: You can use alphanumeric, underscores (_), dashes (-), periods (.), and /@$ characters, and it can be up to 64 characters long.

6.12.1 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
```

7

Trunks

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

7.1 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 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 can balance the load between multiple connections. If one interface's connection goes down, the ZyWALL 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 can still send its traffic through another interface.

7.2 Trunk Scenario Examples

Suppose one of the ZyWALL'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.

7.3 Trunk Commands Input Values

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

Table 40 interface-group Command Input Values

LABEL	DESCRIPTION
group-name	A descriptive name for the trunk. For the ZyWALL 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. The ZyWALL 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. Ethernet interface: For the ZyWALL USG 300 and above, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL model. The ZyWALL USG 200 and lower models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL model supports. VLAN interface: vlan*x*, *x* = 0 - 4094 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ZyWALL model supports.
num	The interface's position in the trunk's list of members <1..8>.
<CR>	Carriage Return (the "enter" key).

7.4 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 40 on page 98 for details about the values you can input with these commands.

Table 41 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 41 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. Set either inbound, outbound, or total (outbound and inbound) traffic to which the ZyWALL 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 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 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 enable SNAT or not. The ZyWALL performs SNAT by default for traffic going to or from the WAN interfaces.
show system default-interface-group	Displays the WAN trunk the ZyWALL first attempts to use.

7.5 Trunk Command Examples

The following example creates a weighted round robin trunk for Ethernet interfaces ge1 and ge2. The ZyWALL 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 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)#
```

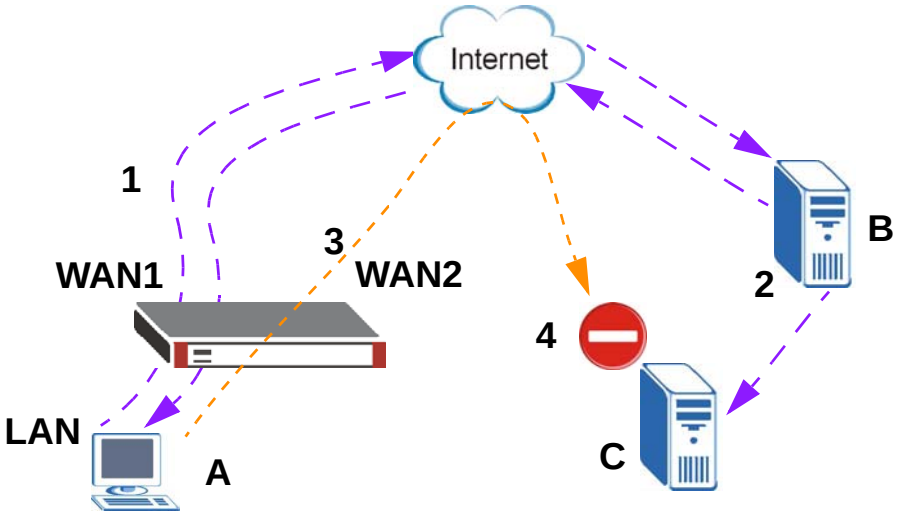
The following example creates a spill-over trunk for Ethernet interfaces ge1 and ge3, which will apply to both incoming and outgoing traffic through the trunk.. The ZyWALL sends traffic through ge1 until it hits the limit of 1000 kbps. The ZyWALL sends anything over 1000 kbps through ge3.

```
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)#
```

7.6 Link Sticking

You can have the ZyWALL 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 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 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 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**.

7.7 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's load balancing behavior.) You must use the `configure terminal` command to enter the configuration mode before you can use these commands. See Table 40 on page 98 for details about the values you can input with these commands.

Table 42 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 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.

7.8 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
```

8

Route

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

8.1 Policy Route

Traditionally, routing is based on the destination address only and the ZyWALL 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.

8.2 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 43 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.
interface_name	The name of the interface. Ethernet interface: For the ZyWALL USG 300 and above, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL model. The ZyWALL USG 200 and lower models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. 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 VLAN interface: vlan*x*, *x* = 0 - 4094 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 12 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ZyWALL model supports. virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL model supports.

Table 43 Input Values for General Policy Route Commands (continued)

LABEL	DESCRIPTION
policy_number	The number of a policy route. 1 - *X* where *X* is the highest number of policy routes the ZyWALL model supports. See the ZyWALL'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 44 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.
`[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 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 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.

Table 44 Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
[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. 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 108 for more details.
dscp-marking <0..63>	Sets a DSCP value to have the ZyWALL apply that DSCP value to the route's outgoing packets.
dscp-marking class {default | *dscp_class*}	Sets how the ZyWALL handles the DSCP value of the outgoing packets that match this route. Set this to default to have the ZyWALL 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 108 for more details.
no dscp-marking	Use this command to have the ZyWALL 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).
[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.

Table 44 Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
[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. 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 108 for more details.
dscp-marking <0..63>	Sets a DSCP value to have the ZyWALL apply that DSCP value to the route’s outgoing packets.
dscp-marking class {default | *dscp_class*}	Sets how the ZyWALL handles the DSCP value of the outgoing packets that match this route. Set this to default to have the ZyWALL 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 108 for more details.
no dscp-marking	Use this command to have the ZyWALL 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.

Table 44 Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
[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 to use policy routes to manually specify the destination addresses of dynamic IPSec rules. You must manually create these policy routes. The ZyWALL automatically obtains source and destination addresses for dynamic IPSec rules that do not match any of the policy routes. The no command has the ZyWALL 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 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 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 is enabled.
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 checks policy routes first before IPSec dynamic rules.
show policy-route override-direct-route	Displays whether or not the ZyWALL 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 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.
show policy-route underlayer-rules	Displays all policy route rule details for advanced debugging.

8.2.1 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 45 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)

8.2.2 Policy Route Command Example

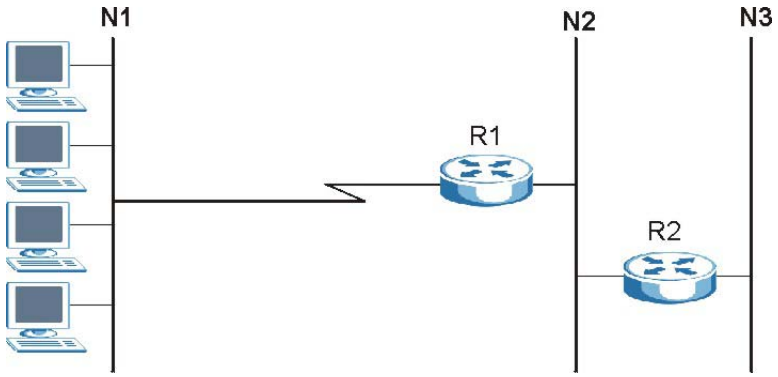
The following commands create two address objects (TW_SUBNET and GW_1) and insert a policy that routes the packets (with the source IP address TW_SUBNET and any destination IP address) through the interface ge1 to the next-hop router GW_1. This route uses the IP address of the outgoing interface as the 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)#
```

8.3 IP Static Route

The ZyWALL has no knowledge of the networks beyond the network that is directly connected to the ZyWALL. For instance, the ZyWALL knows about network **N2** in the following figure through gateway **R1**. However, the ZyWALL 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 about the networks beyond the network connected to the ZyWALL directly.

Figure 15 Example of Static Routing Topology



8.4 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 43 on page 103 for information on input values.

Table 46 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 9.2.5 on page 114.
`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.

Table 46 Command Summary: Static Route (continued)

COMMAND	DESCRIPTION
[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).

8.4.1 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
```

9

Routing Protocol

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

9.1 Routing Protocol Overview

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

The ZyWALL supports two standards, RIP and OSPF, for routing protocols. RIP and OSPF are compared in Table 47 on page 111, and they are discussed further in the next two sections.

Table 47 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

9.2 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 48 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(_). text password: 1-8 characters long MD5 password: 1-16 characters long

The following sections list the routing protocol commands.

9.2.1 RIP Commands

This table lists the commands for RIP.

Table 49 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”.

9.2.2 General OSPF Commands

This table lists the commands for general OSPF configuration.

Table 50 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. The no command resets it to “default”, or the highest available IP address.

9.2.3 OSPF Area Commands

This table lists the commands for OSPF areas.

Table 51 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.

9.2.4 Virtual Link Commands

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

Table 52 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.

9.2.5 Learned Routing Information Commands

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

Table 53 ip route Commands: Learned Routing Information

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

9.2.6 show ip route Command Example

The following example shows learned routing information on the ZyWALL.

```
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      -
```

10

Zones

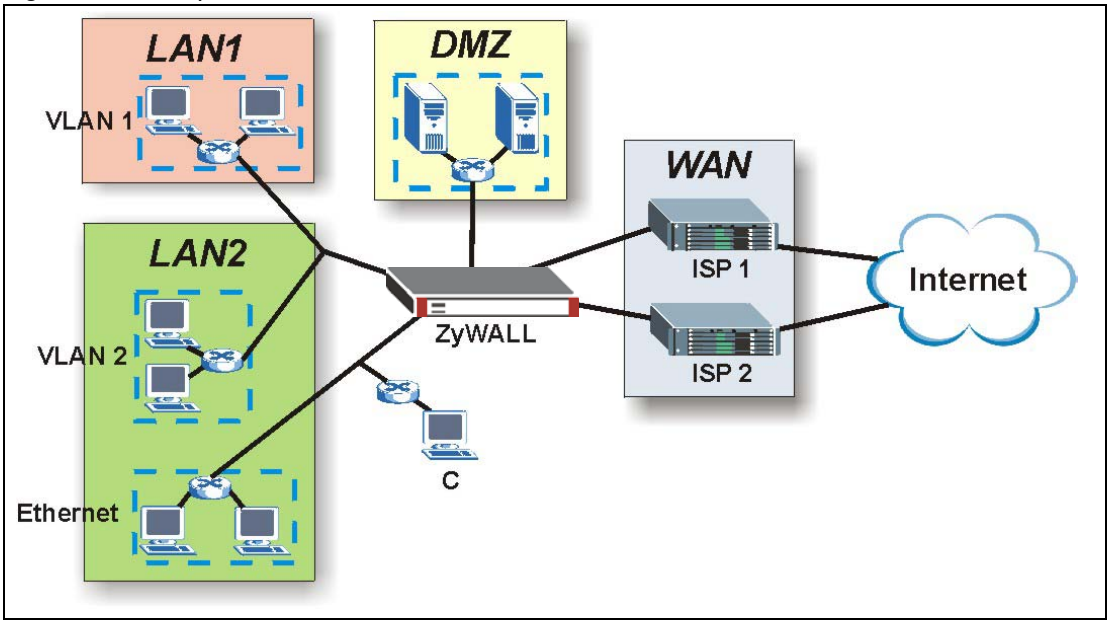
Set up zones to configure network security and network policies in the ZyWALL.

10.1 Zones Overview

A zone is a group of interfaces and VPN tunnels. The ZyWALL 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



10.2 Zone Commands Summary

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

Table 54 Input Values for Zone Commands

LABEL	DESCRIPTION
profile_name	The name of a zone, or the name of a VPN tunnel. For the ZyWALL 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. About the pre-defined zones in the ZyWALL USG 200 and below models: • The lan1 interface always belongs to the LAN1 zone. • The lan2 interface always belongs to the LAN2 zone. • The dmz interface always belongs to the DMZ zone. • The wan1, wan2, wan1_ppp, or wan2_ppp interfaces always belong to the WAN zone. • An opt_ppp interface can be added to the WAN or OPT zone.

This table lists the zone commands.

Table 55 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.
`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.
`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 6.2 on page 61 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.

10.2.1 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
```

11

DDNS

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

11.1 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. When registration is complete, the DNS service provider gives you a password or key. At the time of writing, the ZyWALL supports the following DNS service providers. See the listed websites for details about the DNS services offered by each.

Table 56 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

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

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

11.2 DDNS Commands Summary

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

Table 57 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 58 ip ddns Commands

COMMAND	DESCRIPTION
show ddns [*profile_name*]	Displays information about the specified DDNS profile or about all DDNS profiles.
[no] ip ddns profile *profile_name*	Creates the specified DDNS profile if necessary and enters sub-command mode. The no command deletes it.
[no] service-type {dyndns | dyndns_static | dyndns_custom | dynu-basic | dynu-premium | no-ip | peanut-hull | 3322-dyn | 3322-static}	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. *username*: You can use up to 31 alphanumeric characters and the underscore (_). *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. *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.
[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. *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.

Table 58 ip ddns Commands (continued)

COMMAND	DESCRIPTION
[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.

12

Virtual Servers

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

12.1 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 that you want to make available outside the private network. If the ZyWALL 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.

12.1.1 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 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 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.

12.2 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 59 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 60 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. Select what kind of NAT this rule is to perform. `nat-1-1-map`: means the NAT type is either 1:1 NAT or many 1:1 NAT. See Section 12.1.1 on page 123 for more information. 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 available to a public network outside the ZyWALL (like the Internet). 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. `nat-1-1-map`: means the NAT type is either 1:1 NAT or many 1:1 NAT. See Section 12.1.1 on page 123 for more information. 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 available to a public network outside the ZyWALL (like the Internet). 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. `nat-1-1-map`: means the NAT type is either 1:1 NAT or many 1:1 NAT. See Section 12.1.1 on page 123 for more information. 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 available to a public network outside the ZyWALL (like the Internet). The `deactivate` command disables the virtual server rule.

Table 60 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. nat-1-1-map: means the NAT type is either 1:1 NAT or many 1:1 NAT. See Section 12.1.1 on page 123 for more information. 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 available to a public network outside the ZyWALL (like the Internet). 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*.

12.2.1 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)#
```

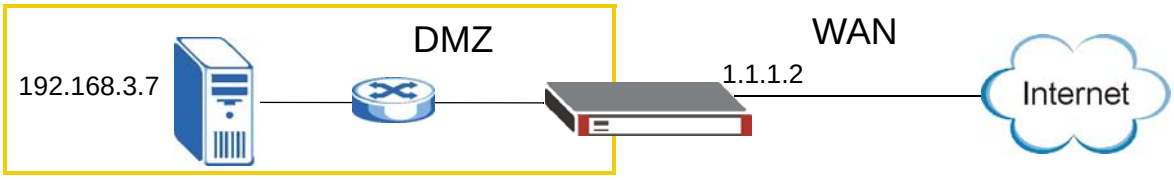
The following command shows information about all the virtual servers in the ZyWALL.

```
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)#
```

12.2.2 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 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.

13

HTTP Redirect

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

13.1 HTTP Redirect Overview

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

13.1.1 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.

13.2 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 61 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. Ethernet interface: For the ZyWALL USG 300 and above, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL model. The ZyWALL USG 200 and lower models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. 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 VLAN interface: vlan*x*, *x* = 0 - 4094 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 4 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ZyWALL model supports. virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL 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 62 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.

13.2.1 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
```

14

ALG

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

14.1 ALG Introduction

The ZyWALL can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as SIP) to operate properly through the ZyWALL'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 examines and uses IP address and port number information embedded in the VoIP traffic's data stream. When a device behind the ZyWALL uses an application for which the ZyWALL has VoIP pass through enabled, the ZyWALL 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 only needs to use the ALG feature for traffic that goes through the ZyWALL'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 when you enable the SIP ALG.

14.2 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 63 alg Commands

COMMAND	DESCRIPTION
`[no] alg sip [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. Use `inactivity-timeout` to have the ZyWALL apply SIP media and signaling inactivity time out limits. Use `signal-port` with a listening port number (1025 to 65535) if you are using SIP on a port other than UDP 5060. 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. 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. 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. Use `transformation` to have the ZyWALL 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. The `no` command turns off the SIP ALG or removes the settings that you specify.
`[no] alg <h323 | ftp> [signal-port <1025..65535> | signal-extra-port <1025..65535> | transformation]`	Turns on or configures the H.323 or FTP ALG. 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. 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. Use `transformation` to have the ZyWALL 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. The `no` command turns off the H.323 or FTP ALG or removes the settings that you specify.
`[no] alg sip defaultport <1..65535>`	Adds (or removes) a custom UDP port number for SIP traffic.
`show alg <sip | h323 | ftp>`	Displays the specified ALG's configuration.

14.3 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
```

15

IP/MAC Binding

15.1 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 uses DHCP to assign IP addresses and records to MAC address it assigned each IP address. The ZyWALL 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.

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.

15.2 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 64 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.

15.3 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)#
```

16

Firewall

This chapter introduces the ZyWALL's firewall and shows you how to configure your ZyWALL's firewall.

16.1 Firewall Overview

The ZyWALL's firewall is a stateful inspection firewall. The ZyWALL 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'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'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's default settings. The ZyWALL checks the schedule, user name (user's login name on the ZyWALL), 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 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, 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 and will be disabled after the user logs out of the ZyWALL.

16.2 Firewall Commands

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

Table 65 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 ZyWALL 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. The ZyWALL 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 model supports. See the ZyWALL'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.

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 66 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 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 67 on page 141 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 67 on page 141 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 67 on page 141 for the sub-commands.

Table 66 Command Summary: Firewall (continued)

COMMAND	DESCRIPTION
`firewall zone_object {zone_object|ZyWALL} delete <1..5000>`	Removes a direction specific through-ZyWALL rule or to-ZyWALL rule. <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 67 on page 141 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. 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 67 on page 141 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.
`firewall insert rule_number`	Enters the firewall sub-command mode to add a firewall rule before the specified rule number. See Table 67 on page 141 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 will permit a host to have at one time.
`show firewall`	Displays all firewall settings.
`show firewall rule_number`	Displays a firewall rule's settings.
`show firewall zone_object {zone_object|ZyWALL}`	Displays all firewall rules settings for the specified packet direction.
`show firewall zone_object {zone_object|ZyWALL} rule_number`	Displays a specified firewall rule's settings for the specified packet direction.
`show firewall 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 firewall rules.
`[no] connlimit6 max-per-host <1..8192>`	Sets the highest number of IPv6 sessions that the ZyWALL 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 67 on page 141 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 67 on page 141 for the sub-commands.

Table 66 Command Summary: Firewall (continued)

COMMAND	DESCRIPTION
`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 67 on page 141 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. <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 67 on page 141 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. 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 67 on page 141 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.
`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 67 on page 141 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 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 firewall rules.
`[no] firewall6 asymmetrical-route activate`	Allows or disallows asymmetrical route topology for IPv6 traffic.

16.2.1 Firewall Sub-Commands

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

Table 67 firewall Sub-commands

COMMAND	DESCRIPTION
`action {allow|deny|reject}`	Sets the action the ZyWALL 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's WAN network from being forwarded to an internal network according to a virtual server rule. Use snat to block packets sent from a computer on the ZyWALL's internal network from being forwarded to the WAN network according to a 1:1 NAT or Many 1:1 NAT rule. 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.
`[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 to create a log (and optionally an alert) when packets match this rule. The no command sets the ZyWALL 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.

Table 67 firewall Sub-commands (continued)

COMMAND	DESCRIPTION
[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.

16.2.2 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 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 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 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
```

16.3 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 68 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.
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 69 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.

Table 69 Command Summary: Session Limit (continued)

COMMAND	DESCRIPTION
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.
[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.

17

IPSec VPN

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

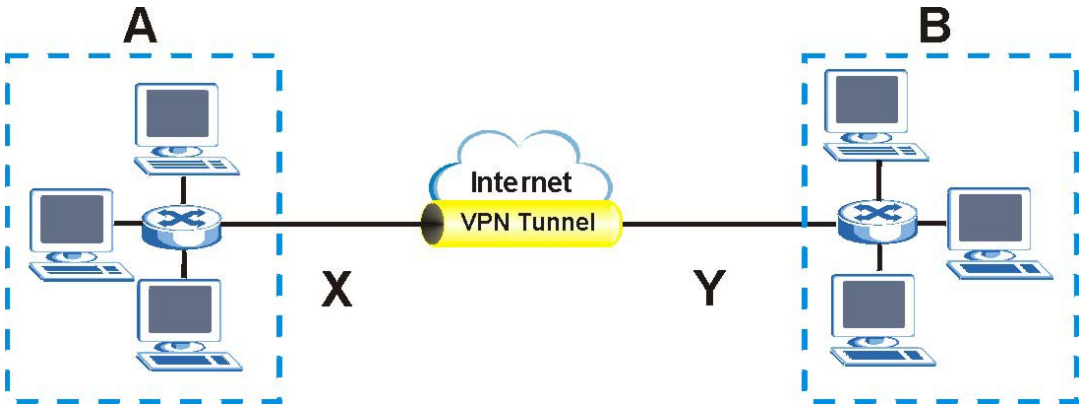
17.1 IPSec VPN Overview

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 19 VPN: Example

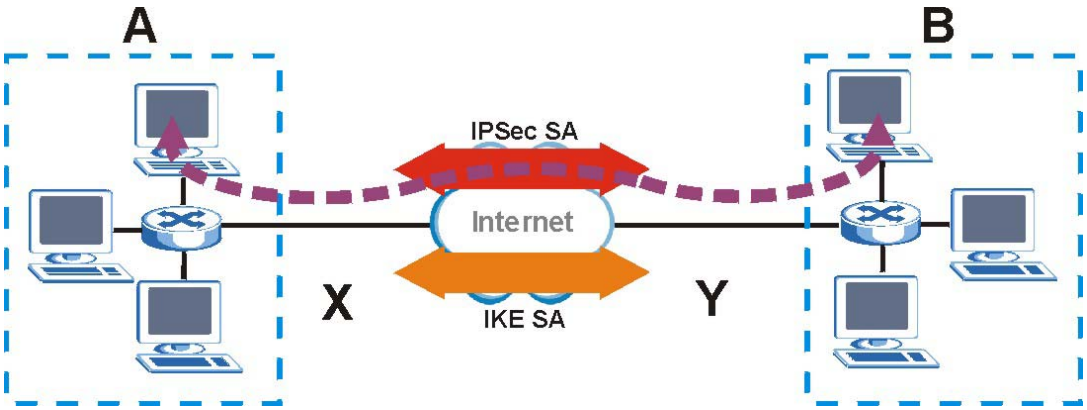


The VPN tunnel connects the ZyWALL (**X**) and the remote IPSec router (**Y**). These routers then connect the local network (**A**) and remote network (**B**).

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

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

Figure 20 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.

17.2 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 70 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 70 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. algorithm encapsulation inbound name outbound policy timeout uptime

The following sections list the IPSec VPN commands.

17.2.1 IKE SA Commands

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

Table 71 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 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 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 changes to using the secondary connection. Users will lose their VPN connection briefly while the ZyWALL 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 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. *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}
lifetime <180..3000000>	Sets the IKE SA life time to the specified value.

Table 71 isakmp Commands: IKE SAs (continued)

COMMAND	DESCRIPTION
group1 group2 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: • 8 - 32 alphanumeric characters or ,;|`~!@#$%^&*()_+\{}':./<>=-". • 16 - 64 hexadecimal (0-9, A-F) characters, preceded by "0x". 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 is the server or client. If the ZyWALL is the server, it also specifies the extended authentication method (aaa authentication *profile_name*); if the ZyWALL is the client, it also specifies the username and password to provide to the remote IPSec router. The no command disables extended authentication. *username*: You can use alphanumeric characters, underscores (_), and dashes (-), and it can be up to 31 characters long. *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*).

17.2.2 IPSec SA Commands (except Manual Keys)

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

Table 72 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 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.
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.

Table 72 crypto Commands: IPSec SAs (continued)

COMMAND	DESCRIPTION
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 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. *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. *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. Site-to-site: The remote IPSec router has a static IP address or a domain name. This ZyWALL can initiate the VPN tunnel. site-to-site-dynamic: The remote IPSec router has a dynamic IP address. Only the remote IPSec router can initiate the VPN tunnel. 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. remote-access-client: Choose this to connect to an IPSec server. This ZyWALL 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).
[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. 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.

Table 72 crypto Commands: IPSec SAs (continued)

COMMAND	DESCRIPTION
[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).

17.2.3 IPSec SA Commands (for Manual Keys)

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

Table 73 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). *auth_key*: You can use any alphanumeric characters or ,;|`~!@#$%^&*()_+\{}':./<>=-". The length of the key depends on the algorithm. md5 - 16-20 characters sha - 20 characters sha256 - 32 characters sha512 - 64 characters *enc_key*: You can use any alphanumeric characters or ,;\|`~!@#$%^&*()_+\{}':./<>=-". The length of the key depends on the algorithm. des - 8-32 characters 3des - 24-32 characters aes128 - 16-32 characters aes192 - 24-32 characters aes256 - 32 characters 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. The ZyWALL 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 only uses 12345678. The ZyWALL 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.

17.2.4 VPN Concentrator Commands

This table lists the commands for the VPN concentrator.

Table 74 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 74 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*).

17.2.5 VPN Configuration Provisioning Commands

This table lists the commands for VPN configuration provisioning.

Table 75 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. *conf_index*: The index number of a VPN configuration provisioning rule, 1 to the ZyWALL'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 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 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.

17.2.6 SA Monitor Commands

This table lists the commands for the SA monitor.

Table 76 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. *`regexp`*: A keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:?|{}[]<>/ characters. 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. 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. A * in the middle of a VPN connection or policy name has the ZyWALL 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. The whole VPN connection or policy name has to match if you do not use a question mark or asterisk. See Table 70 on page 146 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. *`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.

18

SSL VPN

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

18.1 SSL Access Policy

An SSL access policy allows the ZyWALL 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.

18.1.1 SSL Application Objects

SSL application objects specify an application type and server that users are allowed to access through an SSL tunnel. See Chapter 34 on page 270 for how to configure SSL application objects.

18.1.2 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.

18.2 SSL VPN Commands

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

Table 77 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 77 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.

18.2.1 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 78 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 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 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 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 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 grants access and stops checking. 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 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.
`[no] eps periodical-check activate`	Sets whether to have the ZyWALL repeat the endpoint security check at a regular interval configured using the next command. The no command disables this setting.

Table 78 SSL VPN Commands

COMMAND	DESCRIPTION
[no] eps periodical-check <1..1440>	Sets the number of minutes to have the ZyWALL 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. ip-pool: specify the name of the pool of IP addresses to assign to the user computers for the VPN connection. 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. 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.
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.

18.2.2 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 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 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'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
```

19

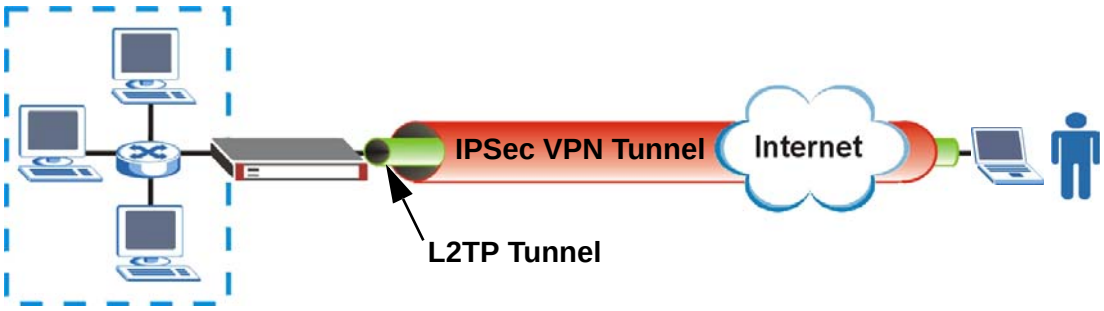
L2TP VPN

This chapter explains how to set up and maintain L2TP VPNs in the ZyWALL.

19.1 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. The remote users do not need their own IPSec gateways or VPN client software.

Figure 21 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 17 on page 145 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).

19.2 IPSec Configuration

You must configure an IPSec VPN connection for L2TP VPN to use (see Chapter 17 on page 145 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.

19.2.1 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.

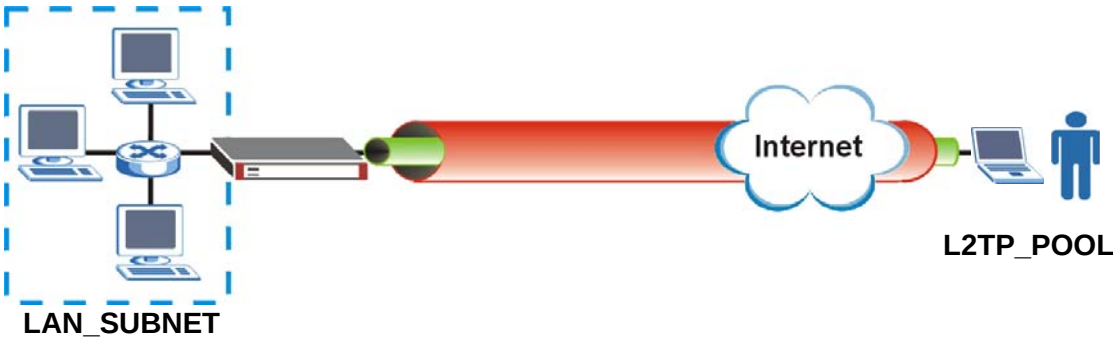
- Configure the **My Address** setting according to your requirements.
- Replace the default **Pre-Shared Key**.

19.3 Policy Route

You must configure a policy route to let remote users access resources on a network behind the ZyWALL.

- 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 assigns to the remote users (**L2TP_POOL** in the following figure).

Figure 22 Policy Route for L2TP VPN



19.4 L2TP VPN Commands

The following table describes the values required for some L2TP VPN commands. Other values are discussed with the corresponding commands.

Table 79 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. Ethernet interface: For the ZyWALL USG 300 and above, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL model. The ZyWALL USG 200 and lower models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. VLAN interface: vlan*x*, *x* = 0 - 4094 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ZyWALL model supports.
ppp_interface	PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL 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.

19.4.1 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 80 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 uses for L2TP VPN. It must meet the requirements listed in Section 19.2 on page 161. 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 uses to assign to the L2TP VPN clients.
`l2tp-over-ipsec authentication` *aaa authentication profile_name*	Specifies how the ZyWALL authenticates a remote user before allowing access to the L2TP VPN tunnel. The authentication method has the ZyWALL check a user's user name and password against the ZyWALL's local database, a remote LDAP, RADIUS, a Active Directory server, or more than one of these.

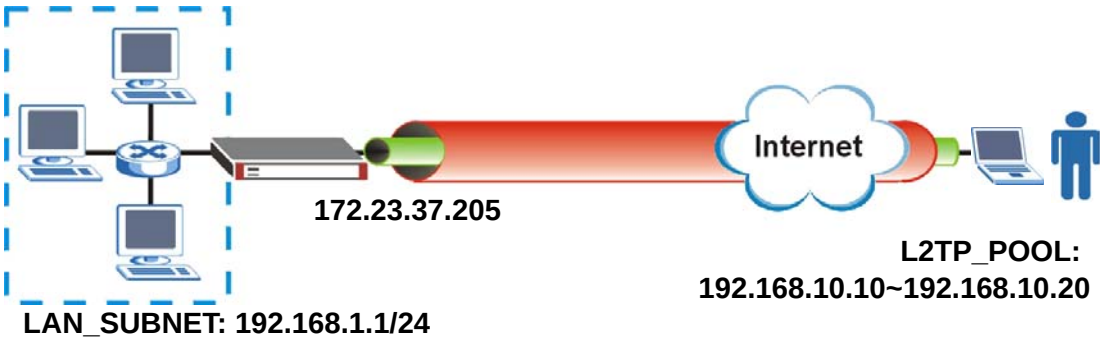
Table 80 L2TP VPN Commands

COMMAND	DESCRIPTION
`certificate cert_name`	Select the certificate to use to identify the ZyWALL 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 to log in. The no command removes the user name setting.
`[no] l2tp-over-ipsec keepalive-timer <1..180>`	The ZyWALL sends a Hello message after waiting this long without receiving any traffic from the remote user. The ZyWALL 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.

19.5 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 23 L2TP VPN Example



- The ZyWALL 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.

19.5.1 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)#
```

19.5.2 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)#
```

19.5.3 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’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:
```

19.5.4 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 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
```

20

Application Patrol

This chapter describes how to set up application patrol for the ZyWALL.

20.1 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 checks firewall rules before application patrol rules for traffic going through the ZyWALL. To use a service, make sure both the firewall and application patrol allow the service's packets to go through the ZyWALL.

Application patrol examines every TCP and UDP connection passing through the ZyWALL and identifies what application is using the connection. Then, you can specify, by application, whether or not the ZyWALL continues to route the connection.

20.2 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 81 Input Values for Application Patrol Commands

LABEL	DESCRIPTION
protocol_name	The name of a pre-defined application. These are listed by category. general: ftp | smtp | pop3 | irc | http im: msn | aol-icq | yahoo | qq p2p: bittorrent | eDonkey | fasttrack | gnutella | napster | h323 | sip | soulseek stream: rtsp
rule_number	The number of an application patrol rule. 1 - *X* where *X* is the highest number of rules the ZyWALL model supports. See the ZyWALL's User's Guide for details.

Table 81 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.

20.2.1 Pre-defined Application Commands

This table lists the commands for each pre-defined application.

Table 82 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 should take when it identifies this application.
`app protocol_name mode {portless | portbase}`	Specifies how the ZyWALL 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.

20.2.2 Rule Commands for Pre-defined Applications

This table lists the commands for rules in each pre-defined application.

Table 83 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 84 on page 169 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 84 on page 169 for the sub-commands.

`app protocol_name rule rule_number`
or
`app protocol_name rule modify rule_number`
	Enters sub-command mode for editing the rule at the specified row. See Table 84 on page 169 for the sub-commands.

Table 83 app Commands: Rules in Pre-Defined Applications (continued)

COMMAND	DESCRIPTION
app *protocol_name* rule default or app *protocol_name* rule modify default	Enters sub-command mode for editing the default rule for the application. See Table 84 on page 169 for the sub-commands.
no app *protocol_name* rule *rule_number*	Deletes the specified rule.

20.2.2.1 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 84 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 handles the DSCP value of the outgoing packets to a connection’s initiator that match this policy. Enter a DSCP value to have the ZyWALL apply that DSCP value. Set this to the class default to have the ZyWALL 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 handles the DSCP value of the outgoing packets from a connection’s initiator that match this policy. Enter a DSCP value to have the ZyWALL apply that DSCP value. Set this to the class default to have the ZyWALL 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.

20.2.3 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 85 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 86 on page 170 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 86 on page 170 for the sub-commands.
app *protocol_name* exception *rule_number*	Enters sub-command mode for editing the rule at the specified row. See Table 86 on page 170 for the sub-commands.
app *protocol_name* exception *rule_number* or app *protocol_name* exception modify *rule_number*	Enters sub-command mode for editing the rule at the specified row. See Table 86 on page 170 for the sub-commands.
app *protocol_name* exception default or app *protocol_name* exception modify default	Enters sub-command mode for editing the default rule for the application. See Table 86 on page 170 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.

20.2.3.1 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 86 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 handles the DSCP value of the outgoing packets to a connection’s initiator that match this policy. Enter a DSCP value to have the ZyWALL apply that DSCP value. Set this to the class default to have the ZyWALL 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 86 app patrol exception rule Sub-commands (continued)

COMMAND	DESCRIPTION
[no] outbound-dscp-mark {<0..63> | class {default | *dscp_class*}}	This is how the ZyWALL handles the DSCP value of the outgoing packets from a connection's initiator that match this policy. Enter a DSCP value to have the ZyWALL apply that DSCP value. Set this to the class default to have the ZyWALL 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.

20.2.4 Other Application Commands

This table lists the commands for other applications in application patrol.

Table 87 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.

20.2.5 Rule Commands for Other Applications

This table lists the commands for rules in other applications.

Table 88 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.

20.2.5.1 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 89 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 handles the DSCP value of the outgoing packets to a connection’s initiator that match this policy. Enter a DSCP value to have the ZyWALL apply that DSCP value. Set this to the class default to have the ZyWALL 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 handles the DSCP value of the outgoing packets from a connection’s initiator that match this policy. Enter a DSCP value to have the ZyWALL apply that DSCP value. Set this to the class default to have the ZyWALL set the DSCP value to 0.
show	Displays the rule’s configuration

20.2.6 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 49.

This table lists the general commands for application patrol.

Table 90 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 90 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 is enabled.

20.2.6.1 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
```

21

Anti-Virus

This chapter introduces and shows you how to configure the anti-virus scanner.

21.1 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.

21.2 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 91 Input Values for General Anti-Virus Commands

LABEL	DESCRIPTION
zone_object	The name of the zone. For the ZyWALL 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. The ZyWALL 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. 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. 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. A * in the middle of a pattern has the ZyWALL 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. The whole file name has to match if you do not use a question mark or asterisk. If you do not use a wildcard, the ZyWALL checks up to the first 80 characters of a file name.

21.2.1 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 49).

Table 92 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 cannot identify a type.
`show anti-virus skip-unknown-file-type activation`	Displays whether or not anti-virus checks files for which the ZyWALL cannot identify a type.
`anti-virus mail-infect-ext activate`	Has the ZyWALL 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 not add a notification text file to an e-mail after destroying a virus-infected e-mail attachment.

21.2.1.1 Activate/Deactivate Anti-Virus Example

This example shows how to activate and deactivate anti-virus on the ZyWALL.

```
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)#
```

21.2.2 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 93 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 93 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 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 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 detects a virus in a file. The file can be destroyed (filled with zeros from the point where the virus was found). The ZyWALL 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 not check files against a pattern list.
`[no] file-decompression [unsupported destroy]`	Enable file decompression to have the ZyWALL 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.

21.2.2.1 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
```

21.2.3 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 94 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 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 94 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.

21.2.3.1 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
```

21.2.4 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 95 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. all: displays all signatures. category: select whether you want to see virus signatures or spyware signatures. *id*: type the ID or part of the ID of the signature you want to find. *name*: type the name or part of the name of the signature(s) you want to find. This search is not case-sensitive. *severity*: type the severity level of the signatures you want to find (high, medium, or low).

21.2.4.1 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
```

21.3 Update Anti-virus Signatures

Use these commands to update new signatures. You should have already registered for anti-virus service.

Table 96 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.

21.3.1 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
```

21.4 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 97 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. `source`: lists the source IP addresses of the most virus-infected files. `destination`: lists the most common destination IP addresses for virus-infected files.

21.4.1 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
```

22

IDP Commands

This chapter introduces IDP-related commands.

22.1 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 98 Input Values for IDP Commands

LABEL	DESCRIPTION
zone_profile	The name of a zone. For the ZyWALL 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. The ZyWALL 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.

22.2 General IDP Commands

22.2.1 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 49.

This table shows the IDP signature, anomaly, and system-protect activation commands.

Table 99 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.

22.2.1.1 Activate/Deactivate IDP Example

This example shows how to activate and deactivate signature-based IDP on the ZyWALL.

```
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
```

22.3 IDP Profile Commands

22.3.1 Global Profile Commands

Use these commands to rename or delete existing profiles and show IDP base profiles.

Table 100 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.

22.3.1.1 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)#
```

22.3.2 IDP Zone to Zone Rules

Use the following rules to apply IDP profiles to specific directions of packet travel.

Table 101 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.

22.3.2.1 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
```

22.3.3 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 102 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.

22.3.4 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 103 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 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 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 103 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 103 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.

22.3.4.1 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)#
```

22.3.5 Editing System Protect

Use these commands to edit the system protect profiles.

Table 104 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.

22.3.6 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 105 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.

22.3.6.1 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 106 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 107 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		

22.3.6.2 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
```

22.4 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 108 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.

22.4.1 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.

```
Router(config)# show idp signatures custom-signature number
signatures:  1
```

22.5 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 109 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

22.5.1 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
```

22.6 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 110 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. `signature-name`: lists the most commonly detected signatures. `source`: lists the source IP addresses from which the ZyWALL has detected the most intrusion attempts. `destination`: lists the most common destination IP addresses for detected intrusion attempts.

22.6.1 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
```

23

Content Filtering

This chapter covers how to use the content filtering feature to control web access.

23.1 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.

23.2 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.

23.3 External Web Filtering Service

When you register for and enable the external web filtering service, your ZyWALL accesses an external database that has millions of web sites categorized based on content. You can have the ZyWALL block, block and/or log access to web sites based on these categories.

23.4 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.

23.5 Content Filter Command Input Values

The following table explains the values you can input with the `content-filter` commands.

Table 111 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 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. {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-). You can enter a single IP address in dotted decimal notation like 192.168.2.5. 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. 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). An example is 192.168.2.1/24 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 111 Content Filter Command Input Values (continued)

LABEL	DESCRIPTION
forbid_hosts	The IP address or domain name of a forbidden web site. 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-). You can enter a single IP address in dotted decimal notation like 192.168.2.5. 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. 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). An example is 192.168.2.1/24 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. 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.

23.6 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 111 on page 204 for details about the values you can input with these commands.

Table 112 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 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 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'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 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 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. 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 112 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. *ipv4*: IPv4 address <W.X.Y.Z> *ipv4_cidr*: IPv4 subnet in CIDR format, i.e. 192.168.1.0/32 <W.X.Y.Z>/<1..32> *ipv4_range*: Range of IPv4 addresses. <W.X.Y.Z>-<W.X.Y.Z> *wildcard_domainname*: wildcard domain name, i.e. zyxel*.co* (([*a-z0-9\-]){1,63}\.)+([*a-z0-9\-]){1,63} *tld*: top level domain.
exit	Leaves the sub-command mode.
show content-filter passed warning	Displays the ZyWALL'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.

23.7 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 111 on page 204 for details about the values you can input with these commands.

Table 113 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 113 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. 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. 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. 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. 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 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 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 not log access to web pages if the external content filtering database is unavailable.
no content-filter profile *filtering_profile* url unrate {log}	Has the ZyWALL not log access to web pages that the external web filtering service has not categorized.

Table 113 content-filter Filtering Profile Commands Summary (continued)

COMMAND	DESCRIPTION
[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 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. 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. 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. 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. 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 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 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 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 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.

23.8 Content Filter URL Cache Commands

The following table lists the commands that you can use to view and configure your ZyWALL'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 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 111 on page 204 for details about the values you can input with these commands.

Table 114 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's database of restricted web pages.
`url`	Tests whether or not a web site is saved in the ZyWALL's database of restricted web pages.
`exit`	Leaves the sub-command mode.

23.9 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 115 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.

23.9.1 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
```

23.10 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 49).
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!-----------------------------------------
```

24

Anti-Spam

This chapter introduces and shows you how to configure the anti-spam scanner.

24.1 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.

24.2 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 116 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 model supports. See the ZyWALL's User's Guide for details.
zone_object	The name of the zone. The ZyWALL 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.

24.2.1 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 117 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.

24.2.1.1 Activate/Deactivate Anti-Spam Example

This example shows how to activate and deactivate anti-spam on the ZyWALL.

```
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)#
```

24.2.2 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 118 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 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 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 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 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 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 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 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 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.
`[no] anti-spam {smtp | pop3} defaultport` *`port_number`*	Specify a custom SMTP or POP3 TCP port to check.

Table 118 Commands for Zone to Zone Anti-Spam Rules (continued)

COMMAND	DESCRIPTION
show anti-spam {smtp | pop3} defaultport	Display the SMTP or POP3 TCP ports the ZyWALL 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 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 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 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 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 forwards when queries to the mail scan servers time out.
show anti-spam mail-scan query-timeout smtp	Display the action the ZyWALL 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 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 waits for a reply from the mail scan server before taking the relevant timeout action.
show anti-spam mail-scan status	Displays the ZyWALL's settings for IP reputation, mail content, and virus outbreak checking.
show anti-spam tag query-timeout	Display the label the ZyWALL 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 adds to e-mails that it tags and forwards when queries to the mail scan servers time out.

24.2.2.1 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 logs the event when an e-mail matches the DNSBL (see Section 24.2.4 on page 220 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
```

24.2.3 White and Black Lists

The following table identifies values used in these commands. Other input values are discussed with the corresponding commands.

Table 119 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. 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. 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. See Section 24.2.3.2 on page 220 for more details.

Table 119 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 model supports. See the ZyWALL'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 24.2.3.2 on page 220 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 120 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'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's spam white list or black list.

24.2.3.1 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
```

24.2.3.2 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 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 checks the first one.

24.2.4 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 121 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 122 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 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 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. • 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. • 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. dnsbl-timeout configures the message or label to add to the mail subject of e-mails that the ZyWALL forwards if queries to the DNSBL domains time out. 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'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 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. dnsbl-timeout displays the message or label to add to the mail subject of e-mails that the ZyWALL 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 waits for a reply from the DNSBL domains.
show anti-spam dnsbl query-timeout time	Displays how long the ZyWALL waits for a reply from the DNSBL domains.

Table 122 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'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's list

24.2.4.1 DNSBL Example

This example:

- Sets the ZyWALL to use "DNSBL-example.com" as a DNSBL.
- Turns DNSBL checking on.
- Sets the ZyWALL to forward POP3 mail with a tag if the queries to the DNSBL domains time out.
- Sets the ZyWALL to check up to 4 sender and relay server IP addresses in e-mail headers against the DNSBL.
- Sets the ZyWALL 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
```

24.3 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 123 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. `source`: lists the source IP addresses of the most spam. `mail-address`: lists the most common source mail address for spam.
`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.

24.3.1 Anti-Spam Statistics Example

This example shows how to collect anti-spam statistics and display a summary.

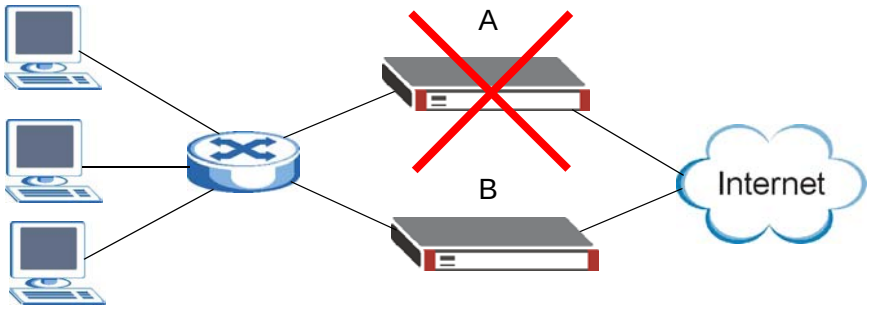
```
Router(config)# anti-spam statistics  collect
Router(config)# show anti-spam statistics collect
collect statistics: yes
collect statistics time: since 2008-03-11 07:16:01 to 2008-03-11 07:16:13
Router(config)# show anti-spam statistics summary
total mails scanned: 0
total clear mails: 0
clear mail 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
```

25

Device HA

Use device HA to increase network reliability. Device HA lets a backup ZyWALL (**B**) automatically take over if a master ZyWALL (**A**) fails.

Figure 24 Device HA Backup Taking Over for the Master



25.1 Device HA Overview

Active-Passive Mode and Legacy Mode

- Active-passive mode lets a backup ZyWALL take over if the master ZyWALL fails.
- Legacy mode uses VRRP (Virtual Router Redundancy Protocol) groups and allows for more complex relationships between the master and backup ZyWALLs, such as active-active or using different ZyWALLs as the master ZyWALL for individual interfaces. Legacy mode configuration involves a greater degree of complexity. Active-passive mode is recommended for general failover deployments.
- The ZyWALLs 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 for management whether the ZyWALL 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 copy the master ZyWALL's configuration, signatures (anti-virus, IDP/application patrol, and system protect), and certificates.

Note: Only ZyWALLs of the same model and firmware version can synchronize.

Otherwise you must manually configure the master ZyWALL's settings on the backup (by editing copies of the configuration files in a text editor for example).

25.1.1 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 before synchronizing it with the master ZyWALL.

- Synchronization includes updates for services to which the master and backup ZyWALLs 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 ZyWALLs to the same services.

25.2 General Device HA Commands

This table lists the general commands for device HA.

Table 124 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 to use active-passive or legacy (VRRP group based) device HA.

25.3 Active-Passive Mode Device HA

Virtual Router

The master and backup ZyWALL form a single 'virtual router'.

Cluster ID

You can have multiple ZyWALL 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 loses its connection, device HA has the backup ZyWALL take over.

Enable monitoring for the same interfaces on the master and backup ZyWALLs. 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.

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 regardless of whether it is the master or the backup.

25.4 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 125 Input Values for device-ha Commands

LABEL	DESCRIPTION
interface_name	The name of the interface. This depends on the ZyWALL model. For the ZyWALL USG 300 and above, use ge*x*, *x* = 1 ~ N, where N equals the highest numbered Ethernet interface for your ZyWALL model. For the ZyWALL USG 200 and below, use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. Besides, in HA AP mode, the interface can also be a bridge interface. In HA Legacy mode, the interface can also be a VLAN interface.

The following sections list the `device-ha` commands.

25.4.1 Active-Passive Mode Device HA Commands

This table lists the commands for configuring active-passive mode device HA.

Table 126 device-ha ap-mode Commands

COMMAND	DESCRIPTION
`[no] device-ha ap-mode preempt`	Turn on preempt if this ZyWALL should become the master ZyWALL if a lower-priority ZyWALL is the master when this ZyWALL is enabled.
`device-ha ap-mode role {master|backup}`	Sets the ZyWALL 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 and all of its backup ZyWALLs. If you have multiple ZyWALL virtual routers on your network, use a different cluster ID for each virtual router.
`device-ha ap-mode priority <1..254>`	Sets backup ZyWALL's priority. The backup ZyWALL with the highest value takes over the role of the master ZyWALL if the master ZyWALL becomes unavailable. The priority must be between 1 and 254. (The master interface has priority 255.)
`[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. `string`: Use a plain text password for authentication. *key* - Use up to eight characters including alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ ()). `ah-md5`: Use an encrypted MD5 password for authentication. *key* - Use up to eight characters including alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ ()).

Table 126 device-ha ap-mode Commands (continued)

COMMAND	DESCRIPTION
[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. It specifies the password to require from synchronizing backup ZyWALLs. 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). *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 uses when synchronizing with the master. The no command sets the password setting to blank (which means this backup ZyWALL cannot synchronize with the master). *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 synchronizes with the master.
[no] device-ha ap-mode backup sync from *master_address* port *port*	Sets the address of the master ZyWALL with which this backup ZyWALL is to synchronize. *master_address*: The master ZyWALL's IP address or fully-qualified domain name (FQDN). *port*: The master ZyWALL'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 will synchronize with the master.
show device-ha ap-mode status	Displays the ZyWALL's key device HA settings.
show device-ha ap-mode master sync	Displays the master ZyWALL's synchronization settings.
show device-ha ap-mode backup sync	Displays the backup ZyWALL's synchronization settings.
show device-ha ap-mode backup sync status	Displays the backup ZyWALL's current synchronization status.
show device-ha ap-mode backup sync summary	Displays the backup ZyWALL'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, 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 goes down. *interface_name*: This is a bridge interface, For example, brx.

25.4.2 Active-Passive Mode Device HA Command Example

This example configures a ZyWALL to be a master ZyWALL 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
```

25.5 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 uses a custom VRRP implementation and is not compatible with standard VRRP.

VRRP Group Overview

In the ZyWALL, 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.

25.6 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 127 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.

25.6.1 VRRP Group Commands

This table lists the commands for VRRP groups.

Table 128 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 preempt lower-priority routers in the virtual router. The no command prevents the ZyWALL 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. *password*: You may use alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ ()), and it can be up to eight characters long.
`[no] description` *description*	Specifies the description for the specified VRRP group. The no command clears the description. *description*: You can use alphanumeric and ()+/:=?!*#@$_%- 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.

25.6.2 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 129 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 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 router. Usually, this is the IP address or FQDN of the virtual router. The no command clears this field. *hostname*: You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.

Table 129 device-ha Commands: Synchronization (continued)

COMMAND	DESCRIPTION
[no] device-ha sync port <1..65535>	Specifies the port number to use to synchronize with the specified ZyWALL 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". *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 automatically synchronizes with the specified ZyWALL router. The no command resets the interval to five minutes.
[no] device-ha sync now	Synchronize now.

25.6.3 Link Monitoring Commands

This table lists the commands for link monitoring. Link monitoring has the master ZyWALL shut down all of its VRRP interfaces if one of its VRRP interface links goes down. This way the backup ZyWALL takes over all of the master ZyWALL's functions.

Table 130 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 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 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 is set to have the master ZyWALL shut down any 3G or wireless LAN interfaces if one of its VRRP interface links goes down.

26

User/Group

This chapter describes how to set up user accounts, user groups, and user settings for the ZyWALL. You can also set up rules that control when users have to log in to the ZyWALL before the ZyWALL routes traffic for them.

26.1 User Account Overview

A user account defines the privileges of a user logged into the ZyWALL. User accounts are used in firewall rules and application patrol, in addition to controlling access to configuration and services in the ZyWALL.

26.1.1 User Types

There are the types of user accounts the ZyWALL uses.

Table 131 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
Admin	Change ZyWALL configuration (web, CLI)	WWW, TELNET, SSH, FTP
Limited-Admin	Look at ZyWALL configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH
Access Users		
User	Access network services 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 31 on page 259 for more information about authentication methods.)

26.2 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 132 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.

26.2.1 User Commands

The first table lists the commands for users.

Table 133 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.
`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. *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. *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 133 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).

26.2.2 User Group Commands

This table lists the commands for groups.

Table 134 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.
[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*).

26.2.3 User Setting Commands

This table lists the commands for user settings, except for forcing user authentication.

Table 135 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 135 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.

26.2.3.1 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
```

26.2.4 Force User Authentication Commands

This table lists the commands for forcing user authentication.

Table 136 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 before the ZyWALL 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 uses on traffic that does not match any exceptional service or other authentication policy. `required`: Users need to be authenticated. They must manually go to the ZyWALL's login screen. The ZyWALL will not redirect them to the login screen. `unnecessary`: Users do not need to be authenticated. `no log | log [alert]`: Select whether to have the ZyWALL 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 137 on page 238 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 137 on page 238 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 137 on page 238 for the sub-commands.
`force-auth policy delete <1..1024>`	Deletes the specified condition. 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.

26.2.4.1 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 137 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. force: Users need to be authenticated and the ZyWALL automatically display the login screen when users who have not logged in yet try to send HTTP traffic. required: Users need to be authenticated. They must manually go to the login screen. The ZyWALL will not redirect them to the login screen.
[no] description *description*	Sets the description for the specified condition. The no command clears the description. *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 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. 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 has to repeat the endpoint security check. The no command means that the ZyWALL only perform the endpoint security check when users log in to the ZyWALL.
[no] force	Forces users to log in to the ZyWALL if the specified condition is satisfied. The no command means that users do not log in to the ZyWALL.
[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.

26.2.4.2 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
```

26.2.5 Additional User Commands

This table lists additional commands for users.

Table 138 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.

26.2.5.1 Additional User Command Examples

The following commands display the users that are currently logged in to the ZyWALL 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
================================================================================
```

27

Addresses

This chapter describes how to set up addresses and address groups for the ZyWALL.

27.1 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 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 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.

27.2 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 139 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 model. For the USG 300 and above, use ge*x*, *x* = 1 ~ N, where N equals the highest numbered Ethernet interface for your ZyWALL model. For the ZyWALL USG 200 and below, use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.

The following sections list the address object and address group commands.

27.2.1 Address Object Commands

This table lists the commands for address objects.

Table 140 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. *ip_range*: <1..255>.<0..255>.<0..255>.<1..255>-<1..255>.<0..255>.<0..255>.<1..255> *ip_subnet*: <1..255>.<0..255>.<0..255>.<0..255>/<1..32> *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. *ipv6_address*: IPv6 address *ipv6_range*: IPv6 address range. For example: fe80:1234::1-fe80:1234::ffff *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.

27.2.1.1 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
```

27.2.2 Address Group Commands

This table lists the commands for address groups.

Table 141 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 141 object-group Commands: Address Groups (continued)

COMMAND	DESCRIPTION
[no] description *description*	Sets the description to the specified value. The no command clears the description. *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*.

27.2.2.1 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
```

28

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.

28.1 Services Overview

See the appendices in the web configurator's User Guide for a list of commonly-used services.

28.2 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 142 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.

28.2.1 Service Object Commands

The first table lists the commands for service objects.

Table 143 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 143 service-object Commands: Service Objects (continued)

COMMAND	DESCRIPTION
service-object *object_name* icmp *icmp_value*	Creates the specified ICMP message using the specified parameters. *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.

28.2.1.1 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
```

28.2.2 Service Group Commands

The first table lists the commands for service groups.

Table 144 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 144 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. *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*.

28.2.2.1 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
```

29

Schedules

Use schedules to set up one-time and recurring schedules for policy routes, firewall rules, application patrol, and content filtering.

29.1 Schedule Overview

The ZyWALL 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.

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.

29.2 Schedule Commands Summary

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

Table 145 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 146 schedule Commands

COMMAND	DESCRIPTION
`show schedule-object`	Displays information about the schedules in the ZyWALL.
`no schedule-object` *object_name*	Deletes the schedule object.

Table 146 schedule Commands (continued)

COMMAND	DESCRIPTION
schedule-object *object_name date time date time*	Creates or updates a one-time schedule. *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. *day*: 3-character day of the week; sun | mon | tue | wed | thu | fri | sat

29.2.1 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
```

30

AAA Server

This chapter introduces and shows you how to configure the ZyWALL to use external authentication servers.

30.1 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 supports.

- Local user database

  The ZyWALL uses the built-in local user database to authenticate administrative users logging into the ZyWALL's web configurator or network access users logging into the network through the ZyWALL. 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.

30.2 Authentication Server Command Summary

This section describes the commands for authentication server settings.

30.2.1 ad-server Commands

The following table lists the `ad-server` commands you use to set the default AD server.

Table 147 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 147 ad-server Commands (continued)

COMMAND	DESCRIPTION
[no] ad-server binddn *binddn*	Sets the user name the ZyWALL 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 to establish a secure connection to the AD server. The no command disables this feature.

30.2.2 ldap-server Commands

The following table lists the ldap-server commands you use to set the default LDAP server.

Table 148 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 uses to log into the default LDAP server. The no command clears this setting.
[no] ldap-server cn-identifier *uid*	Sets the unique common name (cn) to identify a record. 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 to establish a secure connection to the LDAP server. The no command disables this feature.

30.2.3 radius-server Commands

The following table lists the `radius-server` commands you use to set the default RADIUS server.

Table 149 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. 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.

30.2.4 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)#
```

30.2.5 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 150 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. 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. 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 150 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 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 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 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. 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 to establish a secure connection to the AD server. The no command disables this feature.

30.2.6 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 151 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. 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. 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 151 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 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 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 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. 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 to establish a secure connection to the LDAP server. The no command disables this feature.

30.2.7 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 152 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. 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 152 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 is used to determine to which group a user belongs. 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. 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. 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.

30.2.8 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
```

31

Authentication Objects

This chapter shows you how to select different authentication methods for user authentication using the AAA servers or the internal user database.

31.1 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 uses to authenticate users (using VPN or managing through HTTP/HTTPS).

31.2 aaa authentication Commands

The following table lists the `aaa authentication` commands you use to configure an authentication profile.

Table 153 aaa authentication Commands

COMMAND	DESCRIPTION
`aaa authentication rename` *`profile-name-old profile-name-new`*	Changes the profile name. *`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. 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. *`member`* = group ad, group ldap, group radius, or local. Note: You must specify at least one member for each profile. Each type of member can only be used once in a profile. The `no` command clears the specified authentication method(s) for the profile.

Table 153 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. *member* = group ad, group ldap, group radius, or local. Note: You must specify at least one member for each profile. Each type of member can only be used once in a profile. 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.

31.2.1 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)#
```

31.3 test aaa Command

The following table lists the `test aaa` command you use to teat a user account on an authentication server.

Table 154 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.

31.3.1 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 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!-----------------------------------------
```

32

Certificates

This chapter explains how to use the **Certificates**.

32.1 Certificates Overview

The ZyWALL 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 to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

32.2 Certificate Commands

This section describes the commands for configuring certificates.

32.3 Certificates Commands Input Values

The following table explains the values you can input with the `certificate` commands.

Table 155 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 155 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 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;|`~!@#$%^&*()_+\{}':,./<>=-
ca_name	When you have the ZyWALL enroll for a certificate immediately online, you must have the certification authority's certificate already imported as a trusted certificate. Specify the name of the certification authority's certificate. It can be up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
url	When you have the ZyWALL 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'()+,/:.=?;!*#@$_%-

32.4 Certificates Commands Summary

The following table lists the commands that you can use to display and manage the ZyWALL'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 156 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 156 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 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 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. *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. 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. The ZyWALL 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. 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;|`~!@#$%^&*()_+\{}':,./<>=-
ocsp {activate|deactivate}	Has the ZyWALL check (or not check) incoming certificates that are signed by this certificate against a directory server that uses OCSP (Online Certificate Status Protocol).
ocsp url *url* [id *name* password *password*] [deactivate]	Sets the validation configuration for the specified remote (trusted) certificate where the directory server uses OCSP. *url*: Type the protocol, IP address and pathname of the OCSP server. name: The ZyWALL may need to authenticate itself in order to access the OCSP server. Type the login name (up to 31 characters) from the entity maintaining the server (usually a certification authority). You can use alphanumeric characters, the underscore and the dash. password: Type the password (up to 31 characters) from the entity maintaining the OCSP server (usually a certification authority). You can use the following characters: a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
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 156 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.

32.5 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
```

33

ISP Accounts

Use ISP accounts to manage Internet Service Provider (ISP) account information for PPPoE, PPTP and cellular interfaces.

33.1 ISP Accounts Overview

An ISP account is a profile of settings for Internet access using PPPoE, PPTP, or cellular.

33.1.1 PPPoE and PPTP Account Commands

The following table lists the PPPoE and PPTP ISP account commands.

Table 157 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. *`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. *`username`*: You can use alphanumeric, underscores (_), dashes (-), commas (,), and `/@$` characters, and it can be up to 64 characters long.
`[no] password` *`password`*	Sets the password for the specified ISP account. The `no` command clears the password. *`password`*: You can use up to 63 printable ASCII characters. Spaces are not allowed.
`[no] authentication {chap-pap | chap | pap | mschap | mschap-v2}`	Sets the authentication for the specified ISP account. The `no` command sets the authentication to chap-pap.
`[no] compression {yes | no}`	Turns compression on or off for the specified ISP account. The `no` command turns off compression.
`[no] idle <0..360>`	Sets the idle timeout for the specified ISP account. The `no` command sets the idle timeout to zero.
`[no] service-name {`*`ip`* `|` *`hostname`* `|` *`service_name`*`}`	Sets the service name for the specified PPPoE ISP account. The `no` command clears the service name. *`hostname`*: You may up to 63 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period. *`service_name`*: You can use up to 63 alphanumeric characters, underscores (_), dashes (-), and `@$./` characters.

Table 157 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. *connection_id*: You can use up to 31 alphanumeric characters, underscores (_), dashes (-), and colons (:).

33.1.2 Cellular Account Commands

The following table lists the cellular ISP account commands.

Table 158 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. *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. *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. *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. *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. *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.

34

SSL Application

This chapter describes how to configure SSL application objects for use in SSL VPN.

34.1 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.

34.1.1 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 159 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. `file-sharing`: create a file share application for VPN SSL. `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 supports one OWA object. `web-server`: to allow access to the specified web site hosted on the local network. `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. *`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 159 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. "\\<IP address>\<share name>" "\\<domain name>\<share name>" "\\<computer name>\<share name>" 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. Specify the listening ports of the LAN computer(s) running remote desktop server software. The ZyWALL uses a port number from this range to send traffic to the LAN computer that is being remotely managed. *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. Specify the listening ports of the LAN computer(s) running remote desktop server software. The ZyWALL 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. *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. 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.

34.1.2 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
```

35

Endpoint Security

This chapter describes how to configure endpoint security objects for use in authentication policy and SSL VPN.

35.1 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 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.

35.1.1 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 160 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.

35.1.2 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 161 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. `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. 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 can also detect whether or not the anti-virus software is activated; in those cases it must also be activated.

Table 161 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. 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. The user's computer must have one of the listed personal firewalls to pass this checking item. For some personal firewalls the ZyWALL 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. The user's computer must not have any of the forbidden applications running to pass this checking item. 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. The user's computer must have all of the trusted applications running to pass this checking item. 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. 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. 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 161 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. The status command displays the EPS signature version, release date and the total number of software packages for which the ZyWALL'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. 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 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. 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. 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. 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. The status command displays the EPS signature version, release date and the total number of software packages for which the ZyWALL's endpoint security can check.
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.

Table 161 Endpoint Security Object Commands

COMMAND	DESCRIPTION
`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.

35.1.3 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. The following example shows how to check all available Anti-Virus software packages for which the ZyWALL'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. 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 18 on page 155 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)#
```

36

DHCPv6 Objects

This chapter describes how to configure and view DHCPv6 request and lease objects.

36.1 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 162 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 model. For the USG 300 and above, use ge*x*, *x* = 1 ~ N, where N equals the highest numbered Ethernet interface for your ZyWALL model. For the ZyWALL USG 200 and below, use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.

The following sections list the DHCPv6 object commands.

36.1.1 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 163 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 163 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.

36.1.2 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
```

37

System

This chapter provides information on the commands that correspond to what you can configure in the system screens.

37.1 System Overview

Use these commands to configure general ZyWALL 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 zones (if any) from which computers.

37.2 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 26 on page 233 for more on access user accounts.

The following figures identify the parts you can customize in the login and access pages.

Figure 25 Login Page Customization

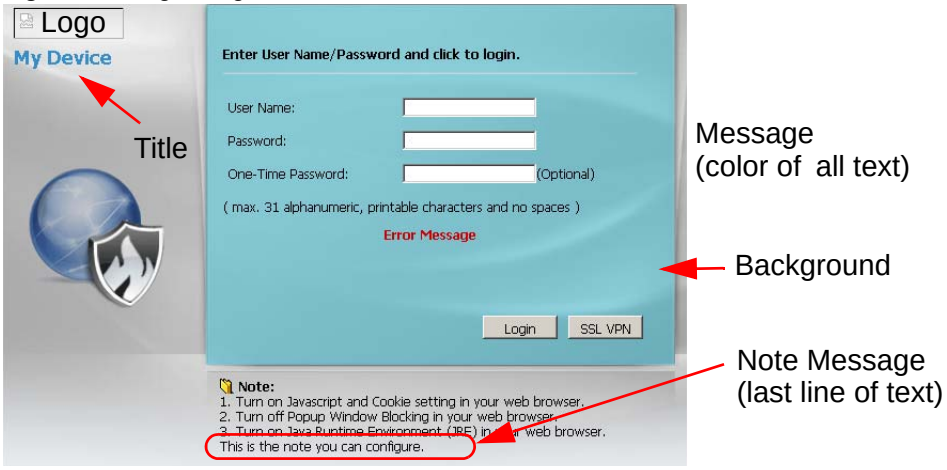
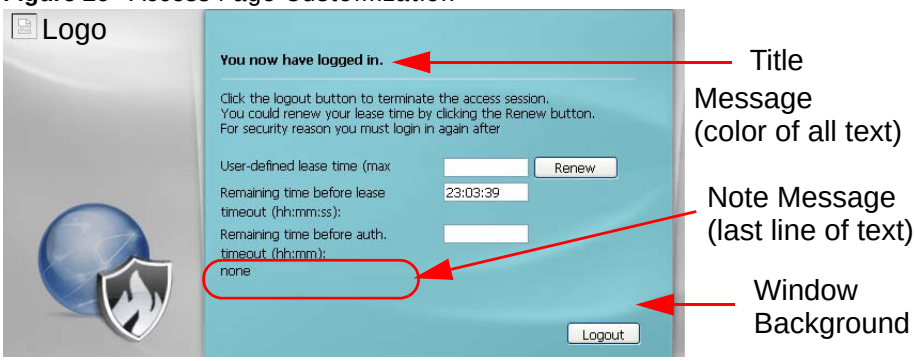


Figure 26 Access Page Customization



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 164 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 164 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 is set to use custom login and access pages or the default ones.

37.3 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 165 Command Summary: Host Name

COMMAND	DESCRIPTION
`[no] domainname domain_name`	Sets the domain name. The `no` command removes the domain name. *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. The `no` command removes the host name.
`show fqdn`	Displays the fully qualified domain name.

37.4 Time and Date

For effective scheduling and logging, the ZyWALL system time must be accurate. The ZyWALL'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.

37.4.1 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 166 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. 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.
`show clock status`	Displays your time zone and daylight saving settings.
`show clock time`	Displays the current time of your ZyWALL.
`show ntp server`	Displays time server settings.

37.5 Console Port Speed

This section shows you how to set the console port speed when you connect to the ZyWALL 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 167 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). *baud_rate*: 9600, 19200, 38400, 57600 or 115200.
`show console`	Displays console port speed.

37.6 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.

37.6.1 Domain Zone Forwarder

A domain zone forwarder contains a DNS server's IP address. The ZyWALL 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.

37.6.2 DNS Commands

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

Table 168 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. Ethernet interface: For the ZyWALL USG 300 and above, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL model. The ZyWALL USG 200 and lower models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. 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 VLAN interface: vlan*x*, *x* = 0 - 4094 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 12 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ZyWALL model supports. virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL 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 169 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 -flush`	Clears the DNS .

Table 169 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). *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 receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address. *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. 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. private | interface: Use private if the ZyWALL connects to the DNS server through a VPN tunnel. Otherwise, use the interface command to set the interface through which the ZyWALL sends DNS queries to a DNS server. The auto means any interface that the ZyWALL 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.

37.6.3 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
```

38

System Remote Management

This chapter shows you how to determine which services/protocols can access which ZyWALL zones (if any) from which computers.

Note: To access the ZyWALL from a specified computer using a service, make sure no service control rules or to-ZyWALL firewall rules block that traffic.

38.1 Remote Management Overview

You may manage your ZyWALL 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.

38.1.1 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 will disconnect the session immediately.
3. There is a firewall rule that blocks it.

38.1.2 System Timeout

There is a lease timeout for administrators. The ZyWALL 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 for authentication again when the reauthentication time expires.

38.2 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 170 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 model supports.
zone_object	The name of the zone. For the ZyWALL 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. The ZyWALL USG 200 and lower models use pre-defined zone names like DMZ, LAN1, SSL VPN, WLAN, IPSec VPN, OPT, and WAN.

38.3 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 171 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`). *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 web configurator. The `no` command disables HTTPS access to the ZyWALL 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 171 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). *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 uses for the SSL in HTTPS connections and the sequence in which it uses them. The *cipher_algorithm* can be any of the following. rc4: RC4 (RC4 may impact the ZyWALL's CPU performance since the ZyWALL's encryption accelerator does not support it). aes: AES des: DES 3des: Triple DES.
no ip http secure-server cipher-suite {*cipher_algorithm*}	Has the ZyWALL not use the specified encryption algorithm for the SSL in HTTPS connections.
[no] ip http server	Allows HTTP access to the ZyWALL web configurator. The no command disables HTTP access to the ZyWALL 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.

38.3.1 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
```

38.4 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.

38.4.1 SSH Implementation on the ZyWALL

Your ZyWALL 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 for remote management on port 22 (by default).

38.4.2 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 over SSH.

38.4.3 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 172 Command Summary: SSH

COMMAND	DESCRIPTION
`[no] ip ssh server`	Allows SSH access to the ZyWALL CLI. The no command disables SSH access to the ZyWALL CLI.
`[no] ip ssh server cert` *certificate_name*	Sets a certificate whose corresponding private key is to be used to identify the ZyWALL for SSH connections. The no command resets the certificate used by the SSH server to the factory default (`default`). *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. *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. *zone_object*: The name of the zone. For the ZyWALL 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. The ZyWALL 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 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.

38.4.4 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.

```
Router# configure terminal
Router(config)# ip ssh server cert Default
```

38.5 Telnet

You can configure your ZyWALL for remote Telnet access.

38.6 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 173 Command Summary: Telnet

COMMAND	DESCRIPTION
`[no] ip telnet server`	Allows Telnet access to the ZyWALL CLI. The `no` command disables Telnet access to the ZyWALL 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. *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. *zone_object*: The name of the zone. For the ZyWALL 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. The ZyWALL 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.

38.6.1 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)#
```

38.7 Configuring FTP

You can upload and download the ZyWALL's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

38.7.1 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 174 Command Summary: FTP

COMMAND	DESCRIPTION
`[no] ip ftp server`	Allows FTP access to the ZyWALL. The `no` command disables FTP access to the ZyWALL.
`[no] ip ftp server cert` *`certificate_name`*	Sets a certificate to be used to identify the ZyWALL. 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. *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. *zone_object*: The name of the zone. For the ZyWALL 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. The ZyWALL 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.

38.7.2 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
================================================================================
```

38.8 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your ZyWALL supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL through the network. The ZyWALL supports SNMP version one (SNMPv1) and version two (SNMPv2c).

38.8.1 Supported MIBs

The ZyWALL supports MIB II that is defined in RFC-1213 and RFC-1215. The ZyWALL 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's MIBs from www.zyxel.com.

38.8.2 SNMP Traps

The ZyWALL will send traps to the SNMP manager when any one of the following events occurs:

Table 175 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 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.
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.

38.8.3 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 176 Command Summary: SNMP

COMMAND	DESCRIPTION
`[no] snmp-server`	Allows SNMP access to the ZyWALL. The `no` command disables SNMP access to the ZyWALL.
`[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. The `no` command removes the contact information for the person in charge of the ZyWALL.
`[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. The `no` command removes the geographic location for the ZyWALL.
`[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. *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. *zone_object*: The name of the zone. For the ZyWALL 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. The ZyWALL 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.

38.8.4 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
```

38.9 ICMP Filter

The ip icmp-filter commands are obsolete. See Chapter 16 on page 137 to configure firewall rules for ICMP traffic going to the ZyWALL to discard or reject ICMP packets destined for the ZyWALL.

Configure the ICMP filter to help keep the ZyWALL hidden from probing attempts. You can specify whether or not the ZyWALL 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 177 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. 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. 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.

38.10 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's other WAN connections are down. This is like an auxiliary interface, except it is used for management connections coming into the ZyWALL instead of as a backup WAN connection.

38.10.1 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.

38.10.2 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 uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command ATH.

38.10.3 Response Strings

The response strings tell the ZyWALL 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.

38.10.4 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 178 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 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. *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. *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.
`[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.

38.10.4.1 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
```

38.11 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 to be managed by the Vantage CNM server, then you should not do any configurations directly to the ZyWALL (using either the web configurator or commands) without notifying the Vantage CNM administrator.

38.11.1 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 179 Command Summary: Vantage CNM

COMMAND	DESCRIPTION
`[no] cnm-agent manager` *`url`*	Sets up the URL of the Vantage server that the ZyWALL 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.
`[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 to authenticate the server using HTTP digest authentication. `No` removes the username of the ACS connection request.

Table 179 Command Summary: Vantage CNM

COMMAND	DESCRIPTION
[no] cnm-agent acs password <password for ACS connection request>	Configure the password of the ACS (Auto-Configuration Server) connection request for the ZyWALL to authenticate the server using HTTP digest authentication. No removes the password of the ACS connection request.
[no] cnm-agent username <TR-069 username>	Configure the username of the ZyWALLfor the ACS server to authenticate the ZyWALL using HTTP digest authentication. No removes the password of the ACS server authentication request.
[no] cnm-agent password <TR-069 password>	Configure the password of the ZyWALL for the ACS server to authenticate the ZyWALL using HTTP digest authentication. 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.

38.11.1.1 Vantage CNM Command Examples

The following example turns on Vantage CNM management and sets the ZyWALL 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
```

38.12 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 180 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. all displays the available languages.

38.13 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 181 Command Summary: IPv6

COMMAND	DESCRIPTION
`[no] ipv6 activate`	Enables or disables IPv6 support.
`show ipv6 status`	Displays whether IPv6 support is enabled or disabled.

39

File Manager

This chapter covers how to work with the ZyWALL's firmware, certificates, configuration files, custom IDP signatures, packet trace results, shell scripts and temporary files.

39.1 File Directories

The ZyWALL stores files in the following directories.

Table 182 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.

39.2 Configuration Files and Shell Scripts Overview

You can store multiple configuration files and shell script files on the ZyWALL.

When you apply a configuration file, the ZyWALL 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 and run when you need them. When you run a shell script, the ZyWALL 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. 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 27 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 applies configuration files differently than it runs shell scripts. This is explained below.

Table 183 Configuration Files and Shell Scripts in the ZyWALL

Configuration Files (.conf)	Shell Scripts (.zysh)
• Resets to default configuration. • Goes into CLI **Configuration** mode. • Runs the commands in the configuration file.	• Goes into CLI **Privilege** mode. • Runs the commands in the shell script.

You have to run the example in Table 27 on page 304 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 29 for more information about CLI modes.)

39.2.1 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 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 exit sub command mode.

Note: “exit” or “!’” must follow sub commands if it is to make the ZyWALL 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
!
```

39.2.2 Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the ZyWALL processes the file line-by-line. The ZyWALL checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the ZyWALL 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 ignores any errors in the configuration file or shell script and applies all of the valid commands. The ZyWALL still generates a log for any errors.

39.2.3 ZyWALL Configuration File Details

You can store multiple configuration files on the ZyWALL. You can also have the ZyWALL use a different configuration file without the ZyWALL restarting.

- When you first receive the ZyWALL, it uses the **system-default.conf** configuration file of default settings.
- When you change the configuration, the ZyWALL creates a **startup-config.conf** file of the current configuration.
- The ZyWALL checks the **startup-config.conf** file for errors when it restarts. If there is an error in the **startup-config.conf** file, the ZyWALL 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 reboots, if the **startup-config.conf** file passes the error check, the ZyWALL 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.

39.2.4 Configuration File Flow at Restart

If there is not a **startup-config.conf** when you restart the ZyWALL (whether through a management interface or by physically turning the power off and back on), the ZyWALL uses the **system-default.conf** configuration file with the ZyWALL's default settings.

If there is a **startup-config.conf**, the ZyWALL checks it for errors and applies it. If there are no errors, the ZyWALL uses it and copies it to the **lastgood.conf** configuration file. If there is an error, the ZyWALL 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 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 ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The ZyWALL still generates a log for any errors.

39.3 File Manager Commands Input Values

The following table explains the values you can input with the file manager commands.

Table 184 File Manager Command Input Values

LABEL	DESCRIPTION
file_name	The name of a file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-).

39.4 File Manager Commands Summary

The following table lists the commands that you can use for file management.

Table 185 File Manager Commands Summary

COMMAND	DESCRIPTION
apply /conf/*file_name.conf* [ignore-error] [rollback]	Has the ZyWALL 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. 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. 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 apply most of your configuration and you can refer to the logs for what to fix. 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 with a fully valid configuration file. Use rollback without ignore-error: this gets the ZyWALL started with a fully valid configuration file as quickly as possible. You can use the "apply /conf/system-default.conf" command to reset the ZyWALL 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 from the source file name to the target file name. 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 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 restarts.
copy running-config /conf/*file_name.conf*	Saves a duplicate of the configuration file that the ZyWALL 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. 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 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.
schedule-run 1 *file_name.zysh* {daily | monthly | weekly} time {*date* | sun | mon | tue | wed | thu | fri | sat}	Has the ZyWALL 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.

Table 185 File Manager Commands Summary (continued)

COMMAND	DESCRIPTION
`show running-config`	Displays the settings of the configuration file that the system is using.
`setenv-startup stop-on-error off`	Has the ZyWALL 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 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 immediately uses configuration changes made via commands, but if you do not use the `write` command, the changes will be lost when the ZyWALL restarts.

39.5 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)#
```

39.6 FTP File Transfer

You can use FTP to transfer files to and from the ZyWALL for advanced maintenance and support.

39.6.1 Command Line FTP File Upload

1. Connect to the ZyWALL.
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.[1] For example:

   In the conf directory, use "put config.conf today.conf” to upload the configuration file (config.conf) to the ZyWALL and rename it “today.conf”.

   "put 1.00(XL.0).bin” transfers the firmware (1.00(XL.0).bin) to the ZyWALL.

The firmware update can take up to five minutes. Do not turn off or reset the ZyWALL while the firmware update is in progress! If you lose power during the firmware upload, you may need to refer to Section 39.8 on page 311 to recover the firmware.

39.6.2 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 as next.conf.

Note: Uploading a custom signature file named "custom.rules", overwrites all custom signatures on the ZyWALL.

Figure 28 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.
```

39.6.3 Command Line FTP File Download

1. Connect to the ZyWALL.
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.
5. Use "get” to download files. For example:

   “get vpn_setup.zysh vpn.zysh” transfers the vpn_setup.zysh configuration file on the ZyWALL to your computer and renames it “vpn.zysh.”

1. When you upload a custom signature, the ZyWALL appends it to the existing custom signatures stored in the "custom.rules” file.

39.6.4 Command Line FTP Configuration File Download Example

The following example gets a configuration file named today.conf from the ZyWALL and saves it on the computer as current.conf.

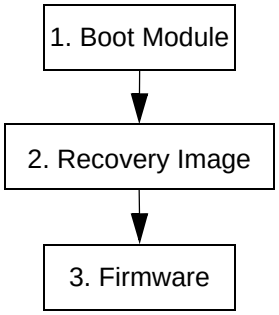
Figure 29 FTP Configuration File Download Example

```
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.
```

39.7 ZyWALL File Usage at Startup

The ZyWALL uses the following files at system startup.

Figure 30 ZyWALL 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 notifies you if the recovery image is damaged.
2. The recovery image checks and loads the firmware. The ZyWALL notifies you if the firmware is damaged.

39.8 Notification of a Damaged Recovery Image or Firmware

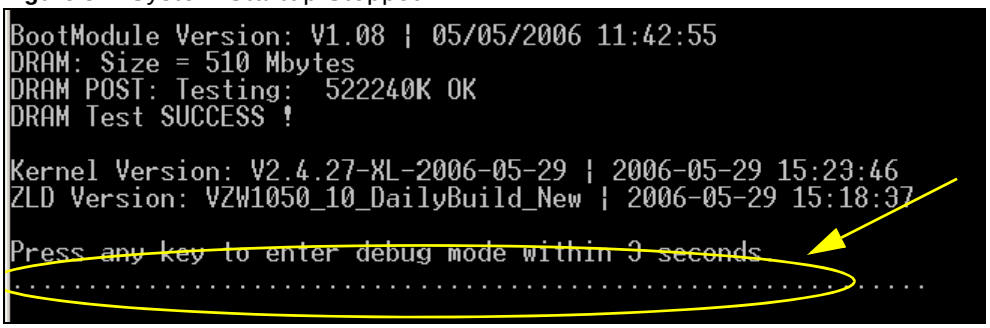
The ZyWALL's recovery image and/or firmware could be damaged, for example by the power going off during a firmware upgrade. This section describes how the ZyWALL notifies you of a damaged recovery image or firmware file. Use this section if your device has stopped responding for an extended period of time and you cannot access or ping it. Note that the ZyWALL 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 via a terminal emulation program (such as HyperTerminal). Your console session displays the ZyWALL's startup messages. If you cannot see any messages, check the terminal emulation program's settings (see Section 1.2.1 on page 24) and restart the ZyWALL.

2 The system startup messages display followed by "Press any key to enter debug mode within 3 seconds."

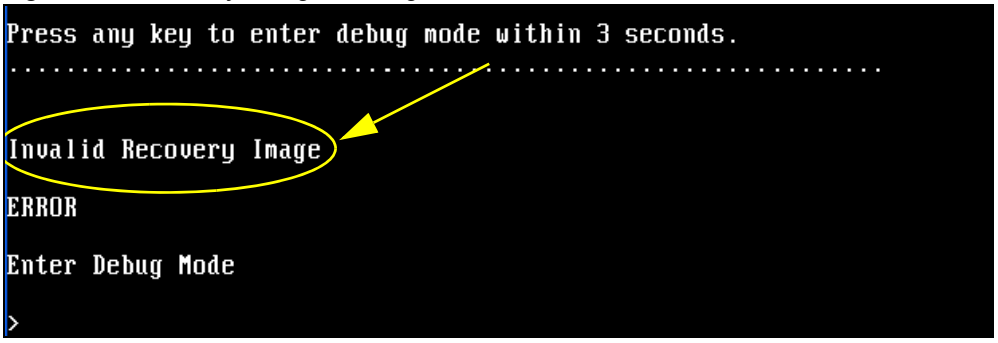
Note: Do not press any keys at this point. Wait to see what displays next.

Figure 31 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 39.9 on page 312 to restore the recovery image.

Figure 32 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 39.10 on page 314 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 33 Firmware Damaged

```
Building ...

Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file.
```

39.9 Restoring the Recovery Image

This procedure requires the ZyWALL’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.

2 When “Press any key to enter debug mode within 3 seconds.” displays, press a key to enter debug mode.

Figure 34 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 35 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)
```

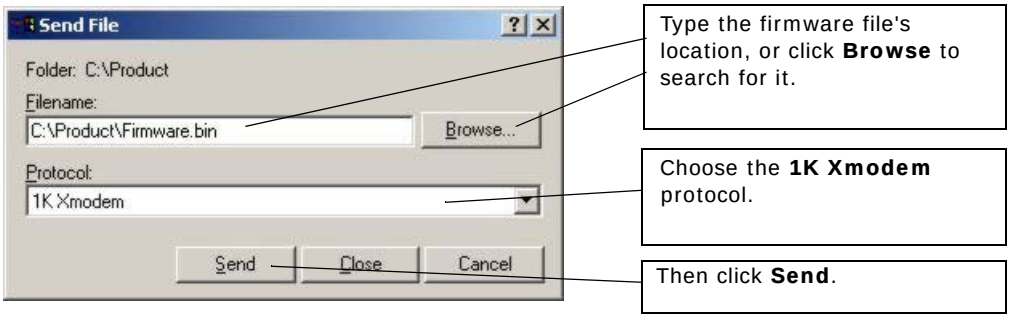
4 Enter Y and wait for the “Starting XMODEM upload” message before activating XMODEM upload on your terminal.

Figure 36 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 37 Example Xmodem Upload



6 Wait for about three and a half minutes for the Xmodem upload to finish.

Figure 38 Recovery Image Upload Complete

```
Total  1867264 bytes received.
programming ..................................................
..............................................................
..............................................................
..............................................................
..............................................................
..............................................................

OK

>
```

7 Enter `atgo`. The ZyWALL 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 39.10 on page 314 to recover the firmware.

Figure 39 atgo Debug Command

```
> atgo
Booting...
```

39.10 Restoring the Firmware

This procedure requires the ZyWALL’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’s port **1** (only port **1** can be used).

2 The ZyWALL’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. 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. 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 40 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 41 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 recovers the firmware.

Figure 42 Firmware Received and Recovery Started

```
Firmware received ...

[Update Filesystem]
       Updating Code
       ..
```

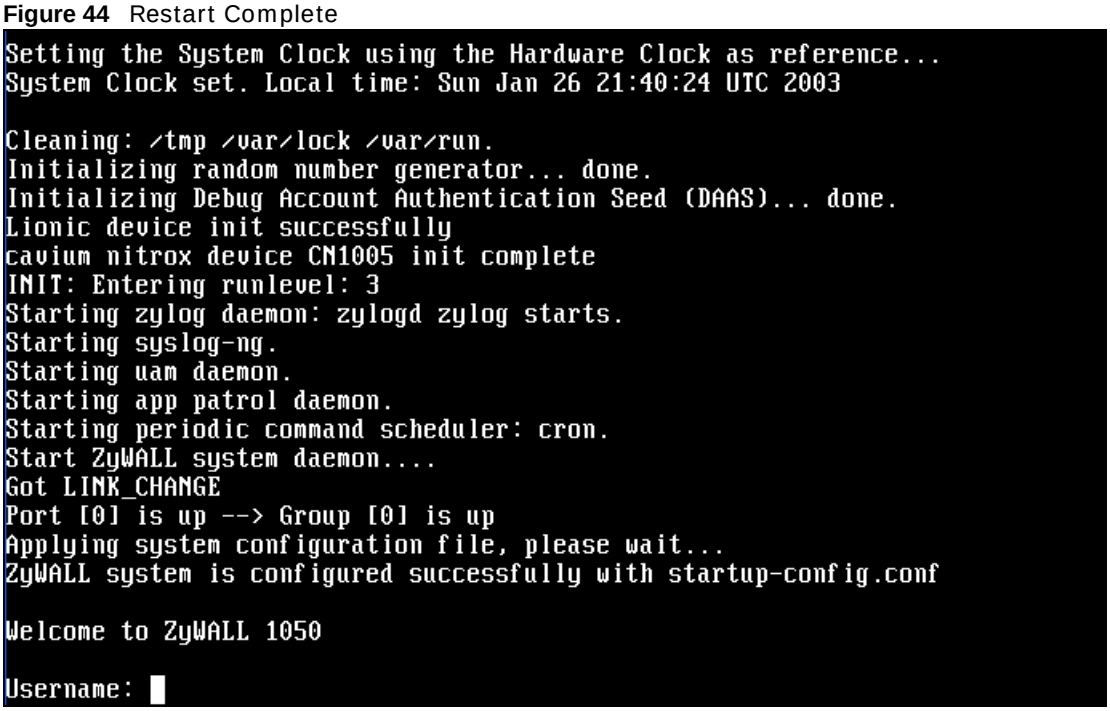
9 The console session displays “done” when the firmware recovery is complete. Then the ZyWALL automatically restarts.

Figure 43 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 starts up successfully. The firmware recovery process is now complete and the ZyWALL is ready to use.

Figure 44 Restart Complete



39.11 Restoring the Default System Database

The default system database stores information such as the default anti-virus or IDP signatures. The ZyWALL 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 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's default system database.

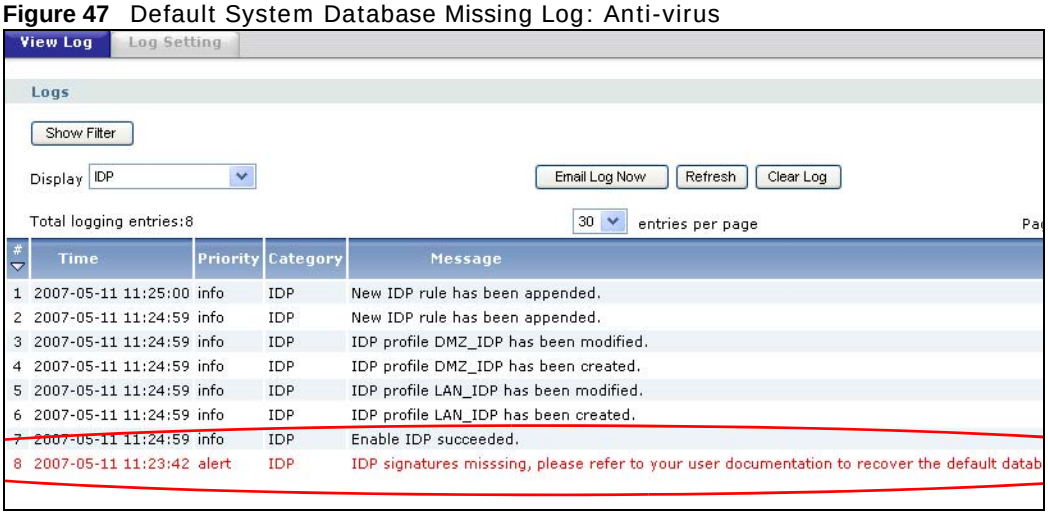
Figure 45 Default System Database Console Session Warning at Startup: Anti-virus

```
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 46 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 47 Default System Database Missing Log: Anti-virus



This procedure requires the ZyWALL'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.

39.11.1 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.
2. When “Press any key to enter debug mode within 3 seconds.” displays, press a key to enter debug mode.

Figure 48 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 `atkz -u` to start the recovery process.

Figure 49 atkz -u Command for Restoring the Default System Database

```
> atkz -u
-u
OK

> atgo
Booting...
```

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’s port **1** (only port **1** can be used).

Figure 50 Use FTP with Port 1 and IP 192.168.1.1 to Upload File

```
Checking CODE ... Done

Updating ...

Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file.
```

5. The ZyWALL’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. 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. 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 51 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 52 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 53 Default System Database Received and Recovery Complete

```
Default System Database received ...

[Update Filesystem]
        Updating Database
        .
        done
```

12 The username prompt displays after the ZyWALL starts up successfully. The default system database recovery process is now complete and the ZyWALL IDP and anti-virus features are ready to use again.

Figure 54 Startup Complete

```
nothing was mounted
Hostname: localhost.

Setting the System Clock using the Hardware Clock as reference...
System Clock set. Local time: Wed May  9 03:26:53 UTC 2007

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 CN505 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 [1] is up --> Group [1] is up
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:
```

40

Logs

This chapter provides information about the ZyWALL'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.

40.1 Log Commands Summary

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

Table 186 Input Values for Log Commands

LABEL	DESCRIPTION
interface_name	The name of the interface. Ethernet interface: For the ZyWALL USG 300 and above, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL model. The ZyWALL USG 200 and lower models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. 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 VLAN interface: vlan*x*, *x* = 0 - 4094 Virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 12 Bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your ZyWALL model supports. Virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL 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.

40.1.1 Log Entries Commands

This table lists the commands to look at log entries.

Table 187 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. *pri*: alert | crit | debug | emerg | error | info | notice | warn *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. *field*: time | msg | src | dst | note | pri | cat | all

40.1.2 System Log Commands

This table lists the commands for the system log settings.

Table 188 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 generate a log for each connectivity check. The no command has the ZyWALL only log the first connectivity check.
show connectivity-check continuous-log status	Displays whether or not the ZyWALL generates a log for each connectivity check.
clear logging system-log buffer	Clears the system log.

40.1.2.1 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    ,
```

40.1.3 Debug Log Commands

This table lists the commands for the debug log settings.

Table 189 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. *`pri`*: alert | crit | debug | emerg | error | info | notice | warn *`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. *`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 190 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. *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. cef: Common Event Format, syslog-compatible format. 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 191 logging Commands: VRPT Settings

COMMAND	DESCRIPTION
vrpt send device information interval <15..3600>	Sets the interval (in seconds) for how often the ZyWALL 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 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 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 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 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 sends a system status log to the VRPT server.

40.1.4 E-mail Profile Commands

This table lists the commands for the e-mail profile settings.

Table 192 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 192 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. *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. *username*: You can use alphanumeric characters, underscores (_), and dashes (-), and it can be up to 31 characters long. *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. *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 mails to the specified e-mail profile. The no command clears this field. *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. *day*: sun | mon | tue | wed | thu | fri | sat

40.1.4.1 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
```

40.1.5 Console Port Logging Commands

This table lists the commands for the console port settings.

Table 193 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.

41

Reports and Reboot

This chapter provides information about the report associated commands and how to restart the ZyWALL using commands. It also covers the daily report e-mail feature.

41.1 Report Commands Summary

The following sections list the report, session, and packet size statistics commands.

41.1.1 Report Commands

This table lists the commands for reports.

Table 194 report Commands

COMMAND	DESCRIPTION
`[no] report`	Begins data collection. The `no` command stops data collection.
`show report status`	Displays whether or not the ZyWALL 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: `ip` - traffic by IP address and direction `service` - traffic by service and direction `url` - hits by URL

41.1.2 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
```

41.1.3 Session Commands

This table lists the commands to display the current sessions for debugging or statistical analysis.

Table 195 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). any means all users, services and IP addresses respectively. 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.

41.1.4 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 196 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 196 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. *interval*: 128, 256, or 512 (bytes)
report packet size statistics clear	Clears the packet size statistics data for all interface.

41.2 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 197 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 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 198 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 sends the report e-mails (up to five recipients).
[no] mail-to-2 *e_mail*	See above.

Table 198 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.

41.2.1 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 not use the second and third mail-to options.
- Sets my-email@example.com as the fourth mail-to option.
- Has the ZyWALL not use the fifth mail-to option.

- Has the ZyWALL provide username 12345 and password 12345 to the SMTP server for authentication.
- Sets the ZyWALL to send the report at 1:57 PM.
- Has the ZyWALL 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 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
```

41.3 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.

42

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 199 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
```

43

Diagnostics

This chapter covers how to use the diagnostics feature.

43.1 Diagnostics

The diagnostics feature provides an easy way for you to generate a file containing the ZyWALL's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting.

43.2 Diagnosis Commands

The following table lists the commands that you can use to have the ZyWALL collect diagnostics information. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

Table 200 diagnosis Commands

COMMAND	DESCRIPTION
`diag-info collect`	Has the ZyWALL 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.

43.3 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
```

44

Packet Flow Explore

This chapter covers how to use the packet flow explore feature.

44.1 Packet Flow Explore

Use this to get a clear picture on how the ZyWALL 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.

44.2 Packet Flow Explore Commands

The following table lists the commands that you can use to have the ZyWALL display routing and SNAT related settings.

Table 201 Packet Flow Explore Commands

COMMAND	DESCRIPTION
`show route order`	Displays the order of routing related functions the ZyWALL checks for packets. Once a packet matches the criteria of a routing rule, the ZyWALL 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 checks for packets. Once a packet matches the criteria of an SNAT rule, the ZyWALL 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.

44.3 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>
```

45

Packet Flow Filter

This chapter covers how to use the packet flow filter feature.

45.1 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 do not.

45.2 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 202 Packet Flow Filter Command Input Values

LABEL	DESCRIPTION
pf_filter_num_range	The filter number to be displayed. 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 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 203 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 203 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.

45.3 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#
```

46

Maintenance Tools

Use the maintenance tool commands to check the conditions of other devices through the ZyWALL. The maintenance tools can help you to troubleshoot network problems.

Here are maintenance tool commands that you can use in privilege mode.

Table 204 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. If you specify `file`, the ZyWALL dumps the traffic to `/packet_trace/packet_trace_interface`. Use FTP to retrieve the files (see Section 39.6 on page 308). If you do not assign the duration, the ZyWALL keeps dumping traffic until you use Ctrl-C. Use the extension filter to extend the use of this command. *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. *hostname*: You can use up to 252 alphanumeric characters, dashes (-), or periods (.). The first character cannot be a period. *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. The no command stops the running packet capture on the ZyWALL. 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 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 204 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. 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. The ZyWALL 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 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 only store packet capture entries on the ZyWALL (internal) or on a USB storage connected to the ZyWALL.
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 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. size: specifies the number of data bytes to be sent count: Stop after sending this number of ECHO_REQUEST packets. 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. *interface_name*: specifies interface through which to send the ECHO_REQUEST packets. *filter_extension*: You can use 1-256 alphanumeric characters, spaces, or '()+,/:=?;!*#@$_%.- characters.
show packet-capture status	Displays whether a packet capture is ongoing.
tracepath6 {*ipv6* | *hostname*}	Displays the path MTU for the target address.

Table 204 Maintenance Tools Commands in Privilege Mode (continued)

COMMAND	DESCRIPTION
`show ipv6 neighbor-list`	Displays the ZyWALL'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 205 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.

46.1 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 206 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
```

46.1.1 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'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 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).

47

Watchdog Timer

This chapter provides information about the ZyWALL's watchdog timers.

47.1 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 207 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.

47.2 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 208 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.

47.3 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 209 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 starts sending alerts when CPU usage exceeds the maximum (the second threshold you enter). The ZyWALL 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 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 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 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 starts sending alerts when disk usage exceeds the maximum (the second threshold you enter). The ZyWALL 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 starts sending alerts when memory usage exceeds the maximum (the second threshold you enter). The ZyWALL 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.

47.3.1 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>] 346
[no] {anti-virus | personal-firewall} activate 274
[no] {*ipv4* | *ipv4_cidr* | *ipv4_range* | *wildcard_domainname* | *tld*} 207
[no] aaa authentication default *member1* [*member2*] [*member3*] [*member4*] 259
[no] aaa authentication *profile-name* 259
[no] aaa authentication *profile-name member1* [*member2*] [*member3*] [*member4*] 260
[no] aaa group server ad *group-name* 255
[no] aaa group server ldap *group-name* 256
[no] aaa group server radius *group-name* 257
[no] access-page color-window-background 284
[no] access-page message-text *message* 284
[no] account {pppoe | pptp} *profile_name* 268
[no] account cellular *profile_name* 269
[no] account *profile_name* 78
[no] account *profile_name* 80
[no] action-block {login|message|audio|video|file-transfer} 169
[no] action-block {login|message|audio|video|file-transfer} 170
[no] action-block {login|message|audio|video|file-transfer} 172
[no] activate 141
[no] activate 143
[no] activate 144
[no] activate 152
[no] activate 156
[no] activate 169
[no] activate 170
[no] activate 172
[no] activate 179
[no] activate 187
[no] activate 216
[no] activate 230
[no] activate 238
[no] activate 299
[no] activate 329
[no] activate 88
[no] address *address6_object* 144
[no] address *address_object* 143
[no] address6-object *object_name* {*ipv6_address* | *ipv6_range* | *ipv6_subnet*} 242
[no] address6-object *object_name* interface-ip *interface* {dhcpv6 | link-local | slaac | static} {*addr_index*} 242
[no] address6-object *object_name* interface-subnet *interface* {dhcpv6 | slaac | static} {*addr_index*} 242
[no] address-object *object_name* 244
[no] ad-server basedn *basedn* 253
[no] ad-server binddn *binddn* 254
[no] ad-server cn-identifier *uid* 254
[no] ad-server host *ad_server* 254
[no] ad-server password *password* 254
[no] ad-server password-encrypted *password* 254
[no] ad-server port *port_no* 254
[no] ad-server search-time-limit *time* 254

[no] ad-server ssl 254
[no] ampdu 88
[no] ampdu 89
[no] amsdu 88
[no] amsdu 89
[no] answer-rings 299
[no] anti-spam {smtp | pop3} defaultport *port_number* 216
[no] anti-spam activate 215
[no] anti-spam black-list [*rule_number*] e-mail *email* {activate|deactivate} 219
[no] anti-spam black-list [*rule_number*] ip-address *ip subnet_mask* {activate|deactivate} 219
[no] anti-spam black-list [*rule_number*] mail-header *mail-header mail-header-value* {activate|deactivate} 219
[no] anti-spam black-list [*rule_number*] subject *subject* {activate|deactivate} 219
[no] anti-spam black-list activate 219
[no] anti-spam dnsbl activate 221
[no] anti-spam ip-reputation activate 217
[no] anti-spam ip-reputation private-check activate 217
[no] anti-spam mail-content activate 217
[no] anti-spam statistics collect 223
[no] anti-spam virus-outbreak activate 217
[no] anti-spam white-list [*rule_number*] e-mail *email* {activate|deactivate} 219
[no] anti-spam white-list [*rule_number*] ip-address *ip subnet_mask* {activate|deactivate} 219
[no] anti-spam white-list [*rule_number*] mail-header *mail-header mail-header-value* {activate|deactivate} 219
[no] anti-spam white-list [*rule_number*] subject *subject* {activate|deactivate} 219
[no] anti-spam white-list activate 219
[no] anti-spam xheader {mail-content | virus-outbreak} *xheader-name xheader-value* 217
[no] anti-spam xheader {white-list | black-list} *mail-header mail-header-value* 219
[no] anti-spam xheader dnsbl *mail-header mail-header-value* 222
[no] anti-spam xheader query-timeout *xheader-name xheader-value* 217
[no] anti-virus activate 178
[no] anti-virus *anti_virus_software_name* detect-auto-protection {enable | disable | ignore} 274
[no] anti-virus black-list activate 180
[no] anti-virus black-list file-pattern *av_file_pattern* {activate|deactivate} 181
[no] anti-virus eicar activate 178
[no] anti-virus skip-unknown-file-type activate 178
[no] anti-virus statistics collect 183
[no] anti-virus update auto 182
[no] anti-virus white-list activate 180
[no] anti-virus white-list file-pattern *av_file_pattern* {activate|deactivate} 180
[no] apn *access_point_name* 269
[no] app activate 173
[no] app highest sip bandwidth priority 173
[no] app other log [alert] 171
[no] app other *protocol_name* bandwidth-graph 173
[no] app *protocol_name* activate 168
[no] app *protocol_name* allowport <1..65535> 168
[no] app *protocol_name* bandwidth-graph 173
[no] app *protocol_name* bwm 168
[no] app *protocol_name* defaultport <1..65535> 168
[no] app *protocol_name* log [alert] 168
[no] application *application_object* 156
[no] application forbidden-process *process_name* 275
[no] application trusted-process *process_name* 275
[no] app-watch-dog activate 352
[no] app-watch-dog alert 352
[no] app-watch-dog auto-recover 352
[no] app-watch-dog console-print {always|once} 352

[no] app-watch-dog cpu-threshold min <1..100> max <1..100> 352
[no] app-watch-dog disk-threshold min <1..100> max <1..100> 352
[no] app-watch-dog interval <6..300> 352
[no] app-watch-dog mem-threshold min <1..100> max <1..100> 352
[no] app-watch-dog retry-count <1..5> 352
[no] app-watch-dog sys-reboot 352
[no] area IP [{stub | nssa}] 113
[no] area IP authentication 113
[no] area IP authentication authentication-key *authkey* 113
[no] area IP authentication message-digest 113
[no] area IP authentication message-digest-key <1..255> md5 *authkey* 113
[no] area IP virtual-link IP 113
[no] area IP virtual-link IP authentication 113
[no] area IP virtual-link IP authentication authentication-key *authkey* 113
[no] area IP virtual-link IP authentication message-digest 113
[no] area IP virtual-link IP authentication message-digest-key <1..255> md5 *authkey* 113
[no] area IP virtual-link IP authentication same-as-area 113
[no] area IP virtual-link IP authentication-key *authkey* 113
[no] authentication {chap-pap | chap | pap | mschap | mschap-v2} 268
[no] authentication {chap-pap | chap | pap | mschap | mschap-v2} 94
[no] authentication {force | required} 238
[no] authentication {none | pap | chap} 269
[no] authentication {string *password* | ah-md5 *password*} 230
[no] authentication mode {md5 | text} 112
[no] authentication string *authkey* 112
[no] auto-destination 104
[no] auto-disable 104
[no] backmx 121
[no] backup-custom *ip* 120
[no] backup-iface *interface_name* 121
[no] band {auto|wcdma|gsm} 80
[no] bandwidth <1..1048576> priority <1..1024> [maximize-bandwidth-usage] 104
[no] bandwidth <1..1048576> priority <1..1024> [maximize-bandwidth-usage] 106
[no] bandwidth excess-usage 169
[no] bandwidth excess-usage 170
[no] bandwidth excess-usage 172
[no] bind *interface_name* 78
[no] block 116
[no] block-ack 88
[no] block-ack 89
[no] block-intra 89
[no] budget active 81
[no] budget data active {download-upload|download|upload} <1..100000> 81
[no] budget time active <1..672> 81
[no] bwm activate 104
[no] bwm activate 173
[no] bypass {ip-reputation | mail-content | virus-outbreak} 216
[no] bypass {white-list | black-list | dnsbl} 216
[no] bypass {white-list | black-list} 179
[no] cache-clean activate 156
[no] case-sensitive 255
[no] case-sensitive 257
[no] case-sensitive 258
[no] client-identifier *mac_address* 68
[no] client-name *host_name* 68
[no] clock daylight-saving 286
[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 286
[no] clock time-zone {-|+*hh*} 286
[no] cnm-agent acs password <password for ACS connection request> 301
[no] cnm-agent acs username <username for ACS connection request> 300
[no] cnm-agent activate 300
[no] cnm-agent auth activate 300
[no] cnm-agent manager *url* 300
[no] cnm-agent password <TR-069 password> 301
[no] cnm-agent periodic-inform activate 300
[no] cnm-agent username <TR-069 username> 301
[no] compression {yes | no} 268
[no] connection-id *connection_id* 269
[no] connectivity {nail-up | dial-on-demand} 78
[no] connectivity-check continuous-log activate 322
[no] connectivity-check continuous-log activate 74
[no] connlimit max-per-host <1..8192> 138
[no] connlimit6 max-per-host <1..8192> 139
[no] console baud *baud_rate* 286
[no] content-filter active 206
[no] content-filter block message *message* 206
[no] content-filter block redirect *redirect_url* 206
[no] content-filter default block 206
[no] content-filter license *license* 206
[no] content-filter license *license* 207
[no] content-filter policy *policy_number address schedule filtering_profile* 206
[no] content-filter profile *filtering_profile* 207
[no] content-filter profile *filtering_profile* commtouch-url category {category_name} ...209
[no] content-filter profile *filtering_profile* custom 207
[no] content-filter profile *filtering_profile* custom activex 207
[no] content-filter profile *filtering_profile* custom cookie 207
[no] content-filter profile *filtering_profile* custom java 207
[no] content-filter profile *filtering_profile* custom proxy 208
[no] content-filter profile *filtering_profile* custom trust-allow-features 208
[no] content-filter profile *filtering_profile* custom trust-only 208
[no] content-filter profile *filtering_profile* url category {category_name} 208
[no] content-filter profile *filtering_profile* url url-server 209
[no] content-filter service-timeout *service_timeout* 209
[no] content-filter statistics collect 210
[no] content-filter -timeout *_timeout* 206
[no] content-filter -timeout *_timeout* 210
[no] corefile copy usb-storage 87
[no] crypto ignore-df-bit 148
[no] crypto map *map_name* 148
[no] crypto *map_name* 152
[no] crypto *profile_name* 116
[no] ctmatch {dnat | snat} 141
[no] ctsrts <256..2346> 88
[no] custom *ip* 120
[no] deactivate 104
[no] deactivate 106
[no] default-router *ip* 68
[no] description *description* 104
[no] description *description* 106
[no] description *description* 141
[no] description *description* 143
[no] description *description* 144
[no] description *description* 156
[no] description *description* 230
[no] description *description* 235

[no] description *description* 238
[no] description *description* 245
[no] description *description* 249
[no] description *description* 275
[no] description *description* 299
[no] description *description* 62
[no] description *description* 68
[no] destination {*address6_object*|any} 106
[no] destination {*address_object* | *group_name*} 238
[no] destination {*address_object*|any} 104
[no] destination {any|*ipv4*} 341
[no] destination *profile_name* 169
[no] destination *profile_name* 170
[no] destination *profile_name* 172
[no] destinationip *address_object* 141
[no] destinationip6 *address_object* 141
[no] device-ha activate 226
[no] device-ha ap-mode authentication {string *key* | ah-md5 *key*} 227
[no] device-ha ap-mode backup sync authentication password *password* 228
[no] device-ha ap-mode backup sync auto 228
[no] device-ha ap-mode backup sync from *master_address* port *port* 228
[no] device-ha ap-mode backup sync interval <1..1440> 228
[no] device-ha ap-mode *interface_name* activate 228
[no] device-ha ap-mode *interface_name* manage-ip *ip subnet_mask* 228
[no] device-ha ap-mode master sync authentication password *password* 228
[no] device-ha ap-mode preempt 227
[no] device-ha sync authentication password *password* 231
[no] device-ha sync auto 231
[no] device-ha sync from {*hostname* | *ip*} 230
[no] device-ha sync interval <5..1440> 231
[no] device-ha sync now 231
[no] device-ha sync port <1..65535> 231
[no] device-ha vrrp-group *vrrp_group_name* 230
[no] diag-info copy usb-storage 87
[no] dialing-type {tone | pulse} 94
[no] dial-string *isp_dial_string* 269
[no] dial-timeout <30..120> 94
[no] domainname *domain_name* 285
[no] domain-name *domain_name* 68
[no] downstream <0..1048576> 62
[no] downstream <0..1048576> 85
[no] dpd 147
[no] dscp {any | <0..63>} 105
[no] dscp {any | <0..63>} 106
[no] dscp class {default | *dscp_class*} 105
[no] dscp class {default | *dscp_class*} 106
[no] dst-port {any|<1..65535>} 341
[no] duplex <full | half> 76
[no] enable 277
[no] enable 341
[no] encryption {nomppe | mppe-40 | mppe-128} 269
[no] eps <1..8> *eps_object_name* 238
[no] eps <1..8> *eps_profile_name* 156
[no] eps activate 156
[no] eps activate 238
[no] eps failure-messages *failure_messages* 274
[no] eps periodical-check <1..1440> 157
[no] eps periodical-check <1..1440> 238
[no] eps periodical-check activate 156

[no] eps profile *profile_name* 274
[no] eps rename *profile_name new_profile_name* 277
[no] fall-back 147
[no] file-decompression [unsupported destroy] 179
[no] file-info file-path *file_path* 275
[no] file-info file-path *file_path* {eq | gt | lt | ge | le | neq} file-size <1..1073741824> 275
[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* 275
[no] file-info file-path *file_path* {eq | gt | lt | ge | le | neq} file-version *file_version* 275
[no] firewall activate 139
[no] firewall activate 140
[no] firewall asymmetrical-route activate 138
[no] firewall6 asymmetrical-route activate 140
[no] first-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns} | ZyWALL} 69
[no] first-wins-server *ip* 69
[no] flood-detection {tcp-flood | udp-flood | ip-flood | icmp-flood} {activate | log [alert] | block} 189
[no] *forbid_hosts* 207
[no] force 238
[no] force-auth activate 237
[no] frag <256..2346> 88
[no] from *zone_name* 169
[no] from *zone_name* 170
[no] from *zone_name* 172
[no] from *zone_object* 141
[no] from *zone_object* 179
[no] from-zone *zone_object* 216
[no] from-zone *zone_profile* 187
[no] groupname *groupname* 235
[no] groupname *groupname* 235
[no] ha-iface *interface_name* 121
[no] hardware-address *mac_address* 68
[no] hardware-watchdog-timer <4..37> 351
[no] hide 89
[no] host {any|*ipv4*} 341
[no] host *hostname* 120
[no] host *ip* 68
[no] hostname *hostname* 285
[no] http-inspection {http-xxx} action {drop | reject-sender | reject-receiver | reject-both}} 190
[no] http-inspection {http-xxx} activate 190
[no] icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} activate 190
[no] idle <0..360> 268
[no] idle <0..360> 269
[no] idle <0..360> 94
[no] idp 186
[no] idp {signature | system-protect} update auto 199
[no] idp statistics collect 200
[no] inbound-dscp-mark {<0..63> | class {default | *dscp_class*}} 169
[no] inbound-dscp-mark {<0..63> | class {default | *dscp_class*}} 170
[no] inbound-dscp-mark {<0..63> | class {default | *dscp_class*}} 172
[no] in-dnat activate 150
[no] infected-action {destroy | send-win-msg} 179
[no] initial-string *initial_string* 299
[no] initial-string *initial_string* 94
[no] in-snat activate 150

[no] interface {*num*|*interface-name*} 99
[no] interface *ap_interface* 89
[no] interface *interface_name* 105
[no] interface *interface_name* 106
[no] interface *interface_name* 116
[no] interface *interface_name* 230
[no] interface *interface_name* 62
[no] interface *interface_name* 80
[no] interface *tunnel_iface* 85
[no] interface-group *group-name* 98
[no] ip address dhcp 62
[no] ip address *ip subnet_mask* 62
[no] ip address *ip subnet_mask* 89
[no] ip ddns profile *profile_name* 120
[no] ip dhcp pool *profile_name* 67
[no] ip dhcp-pool *profile_name* 69
[no] ip dns server a-record *fqdn w.x.y.z* 287
[no] ip dns server mx-record *domain_name* {*w.x.y.z*|*fqdn*} 288
[no] ip dns server zone-forwarder {<1..32>|append|insert <1..32>} {*domain_zone_name*|*} inter-face *interface_name* 288
[no] ip ftp server 295
[no] ip ftp server cert *certificate_name* 295
[no] ip ftp server port <1..65535> 295
[no] ip ftp server tls-required 295
[no] ip gateway *ip* 62
[no] ip gateway *ip* [metric <0..15>] 89
[no] ip helper-address *ip* 69
[no] ip http authentication *auth_method* 290
[no] ip http port <1..65535> 290
[no] ip http secure-port <1..65535> 290
[no] ip http secure-server 290
[no] ip http secure-server auth-client 290
[no] ip http secure-server cert *certificate_name* 291
[no] ip http secure-server force-redirect 291
[no] ip http server 291
[no] ip load-balancing link-sticking activate 101
[no] ip load-balancing link-sticking timeout *timeout* 101
[no] ip ospf authentication-key *password* 73
[no] ip ospf cost <1..65535> 73
[no] ip ospf dead-interval <1..65535> 73
[no] ip ospf hello-interval <1..65535> 73
[no] ip ospf priority <0..255> 73
[no] ip ospf retransmit-interval <1..65535> 73
[no] ip rip {send | receive} version <1..2> 72
[no] ip rip v2-broadcast 72
[no] ip route {*w.x.y.z*} {*w.x.y.z*} {*interface*|*w.x.y.z*} <0..127> 109
[no] ip route control-virtual-server-rules activate 110
[no] ip ssh server 293
[no] ip ssh server cert *certificate_name* 293
[no] ip ssh server port <1..65535> 293
[no] ip ssh server v1 293
[no] ip telnet server 294
[no] ip telnet server port <1..65535> 294
[no] ip-select {iface | auto | custom} 120
[no] ip-select-backup {iface | auto | custom} 120
[no] ipv6 activate 302
[no] ipv6 address *dhcp6_profile dhcp6_suffix_128* 79
[no] ipv6 dhcp6 address-request 79
[no] ipv6 dhcp6 rapid-commit 79

[no] ipv6 dhcp6-request-object *dhcp6_profile* 79
[no] ipv6 enable 79
[no] ipv6 metric <0..15> 79
[no] ipv6 nd ra accept 79
[no] isakmp policy *policy_name* 147
[no] item as-report 330
[no] item av-report 330
[no] item cf-report 330
[no] item cpu-usage 330
[no] item idp-report 330
[no] item mem-usage 330
[no] item port-usage 330
[no] item session-usage 330
[no] item traffic-report 330
[no] join *interface_name* 94
[no] *keyword* 208
[no] l2tp-over-ipsec activate; 163
[no] l2tp-over-ipsec first-dns-server {*ip* | *interface_name*} {1st-dns|2nd-dns|3rd-dns}| {*ppp_interface*|aux}{1st-dns|2nd-dns}} 164
[no] l2tp-over-ipsec first-wins-server *ip* 164
[no] l2tp-over-ipsec keepalive-timer <1..180> 164
[no] l2tp-over-ipsec second-dns-server {*ip* | *interface_name*} {1st-dns|2nd-dns|3rd-dns}| {*ppp_interface*|aux}{1st-dns|2nd-dns}} 164
[no] l2tp-over-ipsec second-wins-server *ip* 164
[no] l2tp-over-ipsec user user_name 164
[no] ldap-server basedn *basedn* 254
[no] ldap-server binddn *binddn* 254
[no] ldap-server cn-identifier *uid* 254
[no] ldap-server host *ldap_server* 254
[no] ldap-server password *password* 254
[no] ldap-server password-encrypted *password* 254
[no] ldap-server port *port_no* 254
[no] ldap-server search-time-limit *time* 254
[no] ldap-server ssl 254
[no] lease {<0..365> [<0..23> [<0..59>]] | infinite} 69
[no] limit <0..8192> 143
[no] limit <0..8192> 144
[no] local-address <*ip*> 82
[no] local-address *ip* 78
[no] log [alert] 141
[no] log [alert] 169
[no] log [alert] 170
[no] log [alert] 172
[no] log [alert] 179
[no] log [alert] 216
[no] logging console 326
[no] logging console category *module_name* 326
[no] logging debug suppression 323
[no] logging debug suppression interval <10..600> 323
[no] logging mail <1..2> 324
[no] logging mail <1..2> {send-log-to | send-alerts-to} *e_mail* 325
[no] logging mail <1..2> address {*ip* | *hostname*} 325
[no] logging mail <1..2> authentication 325
[no] logging mail <1..2> authentication username *username* password *password* 325
[no] logging mail <1..2> category *module_name* level {alert | all} 325
[no] logging mail <1..2> port <1..65535> 325
[no] logging mail <1..2> schedule {full | hourly} 325
[no] logging mail <1..2> subject *subject* 325
[no] logging syslog <1..4> 324

[no] logging syslog <1..4> {disable | level normal | level all} 324
[no] logging syslog <1..4> address {*ip* | *hostname*} 324
[no] logging syslog <1..4> facility {local_1 | local_2 | local_3 | local_4 | local_5 | local_6 | local_7} 324
[no] logging syslog <1..4> format {cef | vrpt} 324
[no] logging system-log suppression 322
[no] logging system-log suppression interval <10..600> 322
[no] logging usb-storage 86
[no] login-page color-background 284
[no] login-page color-window-background 284
[no] login-page message-text % *message* 284
[no] mail-from *e_mail* 329
[no] mail-subject append date-time 329
[no] mail-subject append system-name 329
[no] mail-to-1 *e_mail* 329
[no] mail-to-2 *e_mail* 329
[no] mail-to-3 *e_mail* 330
[no] mail-to-4 *e_mail* 330
[no] mail-to-5 *e_mail* 330
[no] manage-ip IP 230
[no] match-action pop3 {forward | forward-with-tag} 216
[no] match-action smtp {drop | forward | forward-with-tag} 216
[no] message *eps_warning_message* 277
[no] metric <0..15> 62
[no] mss <536..1452> 79
[no] mss <536..1460> 62
[no] mtu <576..1480> 85
[no] mtu <576..1500> 62
[no] mtu <576..2304> 90
[no] mute 299
[no] mx {*ip* | *domain_name*} 120
[no] nail-up 150
[no] natt 148
[no] negotiation auto 76
[no] netbios-broadcast 150
[no] network *interface* area IP 113
[no] network *interface_name* 112
[no] network *interface_name* 72
[no] network *interface_name* area *ip* 72
[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*} 157
[no] network-extension traffic-enforcement 157
[no] network-selection {auto|home} 81
[no] next-hop {auto|gateway *address object* |interface *interface_name* |trunk *trunk_name*|tunnel *tunnel_name*} 105
[no] next-hop {auto|gateway *gatewayv6* |interface *interface_name* |trunk *trunk_name*|tunnel *tunnel_name*} 106
[no] ntp 286
[no] ntp server {*fqdn*|*w.x.y.z*} 286
[no] object-group address *group_name* 244
[no] object-group *group_name* 244
[no] object-group *group_name* 249
[no] object-group service *group_name* 248
[no] outbound-dscp-mark {<0..63> | class {default | *dscp_class*}} 169
[no] outbound-dscp-mark {<0..63> | class {default | *dscp_class*}} 171
[no] outbound-dscp-mark {<0..63> | class {default | *dscp_class*}} 172
[no] outonly-interface *interface_name* 112
[no] outonly-interface *interface_name* 72

[no] out-snat activate 150
[no] packet-capture activate 345
[no] packet-flow activate 342
[no] packet-flow ring-buffer activate 342
[no] passive-interface *interface_name* 112
[no] passive-interface *interface_name* 112
[no] passive-interface *interface_name* 72
[no] passive-interface *interface_name* 73
[no] password *password* 268
[no] password *password* 269
[no] password *password* 94
[no] personal-firewall *personal_firewall_software_name* detect-auto-protection {enable | disable | ignore} 275
[no] phone-number *phone* 95
[no] pin <*pin code*> 82
[no] ping-check activate 74
[no] policy controll-ipsec-dynamic-rules activate 107
[no] policy controll-virtual-server-rules activate 107
[no] policy override-direct-route activate 107
[no] policy6 override-direct-route activate 107
[no] policy-enforcement 149
[no] port <0..65535> 172
[no] port *interface_name* 92
[no] port-speed {9600 | 19200 | 38400 | 57600 | 115200} 299
[no] port-speed {9600 | 19200 | 38400 | 57600 | 115200} 95
[no] preempt 230
[no] priority <1..254> 230
[no] protocol {any|<1..255>} 341
[no] protocol {tcp | udp} 172
[no] radius-server host *radius_server* auth-port *auth_port* 255
[no] radius-server key *secret* 255
[no] radius-server timeout *time* 255
[no] redistribute {static | ospf} 112
[no] redistribute {static | rip} 112
[no] redistribute {static | rip} metric-type <1..2> metric <0..16777214> 112
[no] remote-address <*ip*> 82
[no] remote-address *ip* 78
[no] replay-detection 150
[no] report 327
[no] report packet size statistics 328
[no] reset-counter 330
[no] role {master | backup} 230
[no] router-id IP 112
[no] scan {http | ftp | imap4 | smtp | pop3} 179
[no] scan {smtp | pop3} 216
[no] scan-detection {icmp-sweep | icmp-filtered-sweep} {activate | log [alert] | block} 189
[no] scan-detection {ip-xxx} {activate | log [alert] | block} 189
[no] scan-detection {tcp-xxx} {activate | log [alert] | block} 189
[no] scan-detection {udp-xxx} {activate | log [alert] | block} 189
[no] scan-detection open-port {activate | log [alert] | block} 189
[no] schedule *profile_name* 169
[no] schedule *profile_name* 171
[no] schedule *profile_name* 172
[no] schedule *schedule_name* 238
[no] schedule *schedule_object* 105
[no] schedule *schedule_object* 106
[no] schedule *schedule_object* 141
[no] second-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns} | ZyWALL} 69
[no] second-wins-server *ip* 69

[no] security dot1x acct *ip* port <1..65535> 90
[no] security dot1x activate 90
[no] security dot1x auth *ip* port <1..65535> 90
[no] security external acct *ip* port <1..65535> 90
[no] security external auth *ip* port <1..65535> 91
[no] server alternative-cn-identifier *uid* 256
[no] server alternative-cn-identifier *uid* 257
[no] server basedn *basedn* 256
[no] server basedn *basedn* 257
[no] server binddn *binddn* 256
[no] server binddn *binddn* 257
[no] server cn-identifier *uid* 256
[no] server cn-identifier *uid* 257
[no] server description *description* 256
[no] server description *description* 257
[no] server description *description* 258
[no] server group-attribute <1-255> 258
[no] server group-attribute *group-attribute* 256
[no] server group-attribute *group-attribute* 257
[no] server host *ad_server* 256
[no] server host *ldap_server* 257
[no] server host *radius_server* 258
[no] server *ip* 269
[no] server key *secret* 258
[no] server password *password* 256
[no] server password *password* 257
[no] server port *port_no* 256
[no] server port *port_no* 257
[no] server search-time-limit *time* 256
[no] server search-time-limit *time* 257
[no] server ssl 256
[no] server ssl 257
[no] server timeout *time* 258
[no] service {*service_name*|any} 105
[no] service {*service_name*|any} 106
[no] service *service_name* 141
[no] service-name {*ip* | *hostname* | *service_name*} 268
[no] service-object *object_name* 248
[no] service-type {dyndns | dyndns_static | dyndns_custom | dynu-basic | dynu-premium | no-ip | peanut-hull | 3322-dyn | 3322-static} 120
[no] session-limit activate 143
[no] session-limit6 activate 144
[no] shutdown 62
[no] shutdown 85
[no] signature *sid* activate 188
[no] signature *sid* activate 192
[no] smtp-auth activate 329
[no] smtp-port <1..65535> 329
[no] snat {outgoing-interface|pool {*address_object*}} 105
[no] snmp-server 297
[no] snmp-server community *community_string* {ro|rw} 297
[no] snmp-server contact *description* 297
[no] snmp-server enable {informs|traps} 297
[no] snmp-server host {*w.x.y.z*} [*community_string*] 297
[no] snmp-server location *description* 297
[no] snmp-server port <1..65535> 297
[no] software-watchdog-timer <10..600> 351
[no] source {*address6_object*|any} 107
[no] source {*address_object* | *group_name*} 238

[no] source {*address_object*|any} 105
[no] source {any|*ipv4*} 341
[no] source *profile_name* 169
[no] source *profile_name* 171
[no] source *profile_name* 172
[no] sourceip *address_object* 141
[no] sourceip6 *address_object* 141
[no] sourceport {tcp|udp} {eq <1..65535>|range <1..65535> <1..65535>} 141
[no] speed <100,10> 76
[no] src-port {any|<1..65535>} 341
[no] sslvpn application *application_object* 270
[no] sslvpn *profile_name* 116
[no] sslvpn *tunnel_name* 105
[no] starting-address *ip* pool-size <1..65535> 69
[no] super 88
[no] system default-snat 99
[no] tcp-decoder {tcp-xxx} action {drop | reject-sender | reject-receiver | reject-both}} 190
[no] tcp-decoder {tcp-xxx} activate 190
[no] third-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns} | ZyWALL} 69
[no] to {*zone_object*|ZyWALL} 142
[no] to *zone_name* 169
[no] to *zone_name* 171
[no] to *zone_name* 172
[no] to *zone_object* 179
[no] to-zone *zone_object* 216
[no] to-zone *zone_profile* 187
[no] trigger <1..8> incoming *service_name* trigger *service_name* 105
[no] *trust_hosts* 208
[no] tunnel *tunnel_name* 106
[no] udp-decoder {truncated-header | undersize-len | oversize-len} activate 190
[no] upstream <0..1048576> 62
[no] usb-storage activate 86
[no] user *user_name* 106
[no] user *user_name* 107
[no] user *user_name* 142
[no] user *user_name* 143
[no] user *user_name* 144
[no] user *user_name* 157
[no] user *username* 169
[no] user *username* 171
[no] user *username* 172
[no] user *username* 235
[no] user *username* 268
[no] user *username* 269
[no] username *username* 95
[no] username *username* password *password* 120
[no] users idle-detection 236
[no] users idle-detection timeout <1..60> 236
[no] users lockout-period <1..65535> 236
[no] users retry-count <1..99> 236
[no] users retry-limit 236
[no] users simultaneous-logon {administration | access} enforce 236
[no] users simultaneous-logon {administration | access} limit <1..1024> 236
[no] users update-lease automation 236
[no] version <1..2> 112
[no] vlan-id <1..4094> 93
[no] vpn-concentrator *profile_name* 151
[no] vpn-configuration-provision activate 152
[no] vrid <1..254> 230

[no] wan-iface *interface_name* 120
[no] webpage-encrypt 271
[no] wildcard 121
[no] windows-auto-update {enable | disable | ignore} 276
[no] windows-registry *registry_key* {eq | gt | lt | ge | le | neq} *registry_value* 276
[no] windows-security-patch *security_patch* 276
[no] windows-service-pack <1..10> 276
[no] wlan mac-filter activate 91
[no] wlan mac-filter *mac_address* [description *description*] 91
[no] xauth type {server *xauth_method* | client name *username* password *password*} 148
[no] zone *profile_name* 116
[no]adderss6-object *object_name* interface-gateway *interface* { slaac | static} {*addr_index*} 242
{signature | anomaly | system-protect} activate 186
{signature | anomaly | system-protect} activation 186
| 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*] 68
aaa authentication [no] match-default-group 260
aaa authentication rename *profile-name-old profile-name-new* 259
aaa group server ad *group-name* 255
aaa group server ad rename *group-name group-name* 255
aaa group server ldap *group-name* 256
aaa group server ldap rename *group-name group-name* 256
aaa group server radius *group-name* 258
aaa group server radius rename {*group-name-old*} *group-name-new* 257
access {forward | drop | reject} 169
access {forward | drop | reject} 170
access {forward | drop | reject} 172
access-page message-color {*color-rgb* | *color-name* | *color-number*} 284
access-page title *title* 284
access-page window-color {*color-rgb* | *color-name* | *color-number*} 284
action {allow|deny|reject} 141
activate 147
activate 149
address *ipv6_addr_prefix* 62
address *ipv6_addr_prefix* 64
address-object *object_name* {*ip* | *ip_range* | *ip_subnet* | interface-ip | interface-subnet | interface-gateway} {*interface*} 242
address-object rename *object_name object_name* 242
adjust-mss {auto | <200..1500>} 149
algorithm {wrr|llf|spill-over} 98
anti-spam dnsbl [1..5] domain *dnsbl_domain* {activate|deactivate} 221
anti-spam dnsbl ip-check-order {forward | backward} 221
anti-spam dnsbl max-query-ip [1..5] 221
anti-spam dnsbl query-timeout pop3 {forward | forward-with-tag} 221
anti-spam dnsbl query-timeout smtp {drop | forward | forward-with-tag} 221
anti-spam dnsbl query-timeout time [1..10] 221
anti-spam dnsbl statistics flush 221
anti-spam ip-reputation query-timeout time [*timeout*] 217
anti-spam mail-scan query-timeout pop3 {forward | forward-with-tag} 217
anti-spam mail-scan query-timeout smtp {drop | forward | forward-with-tag} 217
anti-spam mail-scan query-timeout time [*timeout*] 217
anti-spam rule append 216
anti-spam rule delete *rule_number* 216
anti-spam rule insert *rule_number* 216
anti-spam rule move *rule_number* to *rule_number* 216
anti-spam rule *rule_number* 216
anti-spam statistics flush 223

anti-spam tag {dnsbl | dnsbl-timeout} [*tag*] 221
anti-spam tag {mail-content | virus-outbreak} [*tag*] 217
anti-spam tag black-list [*tag*] 219
anti-spam tag query-timeout [*tag*] 217
anti-virus black-list replace *old_av_file_pattern new_av_file_pattern* {activate|deactivate} 181
anti-virus mail-infect-ext activate 178
anti-virus reload signatures 178
anti-virus rule <1..32> 179
anti-virus rule append 178
anti-virus rule delete <1..32> 179
anti-virus rule insert <1..32> 178
anti-virus rule move <1..32> to <1..32> 179
anti-virus search signature {all | category *category* | id *id* | name *name* | severity *severity* [{from *id* to *id*}] 181
anti-virus statistics flush 183
anti-virus update daily <0..23> 182
anti-virus update hourly 182
anti-virus update signatures 182
anti-virus update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23> 182
anti-virus white-list replace *old_av_file_pattern new_av_file_pattern* {activate|deactivate} 180
app other {del | forward | drop | reject} 171
app other <1..64> 171
app other append 171
app other default 171
app other insert *rule_number* 171
app other move *rule_number* to *rule_number* 171
app *protocol_name* {forward | drop | reject} 168
app *protocol_name* bandwidth <0..102400> 168
app *protocol_name* exception append 170
app *protocol_name* exception default 170
app *protocol_name* exception insert *rule_number* 170
app *protocol_name* exception modify default 170
app *protocol_name* exception modify *rule_number* 170
app *protocol_name* exception move *rule_number* to *rule_number* 170
app *protocol_name* exception *rule_number* 170
app *protocol_name* exception *rule_number* 170
app *protocol_name* mode {portless | portbase} 168
app *protocol_name* rule append 168
app *protocol_name* rule default 169
app *protocol_name* rule insert *rule_number* 168
app *protocol_name* rule modify default 169
app *protocol_name* rule modify *rule_number* 168
app *protocol_name* rule *rule_number* 168
apply 37
apply /conf/*file_name.conf* [ignore-error] [rollback] 307
app-watch-dog reboot-log flush 352
area IP virtual-link IP message-digest-key <1..255> md5 *authkey* 113
arp IP *mac_address* 348
atse 37
authentication {pre-share | rsa-sig} 147
authentication key <1..255> key-string *authkey* 112
band <b | g | bg| bgn | gn> 88
bandwidth {inbound | outbound} <0..1048576> 170
bandwidth {inbound|outbound} <0..1048576> 169
bandwidth {inbound|outbound} <0..1048576> 172
bandwidth priority <1..7> 169
bandwidth priority <1..7> 170

bandwidth priority <1..7> 172
bandwidth-graph 168
bind *profile* 187
budget {log|log-alert}[recursive <1..65535>] 81
budget {log-percentage|log-percentage-alert} [recursive <1..65535>] 82
budget current-connection {keep|drop} 81
budget new-connection {allow|disallow} 81
budget percentage {ptime|pdata} <0..99> 82
budget reset-counters 81
budget reset-day <0..31> 81
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*; 264
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* 264
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* 264
ca generate pkcs12 name *name* password *password* 264
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* 264
ca rename category {local|remote} *old_name new_name* 264
ca validation *remote_certificate* 265
cdp {activate|deactivate} 265
certificate *certificate-name* 147
certificate *cert_name* 164
channel <*wireless_channel* | auto> 88
channel-width <auto | 20m | 40m> 88
clear 37
clear aaa authentication *profile-name* 259
clear aaa group server ad [*group-name*] 255
clear aaa group server ldap [*group-name*] 256
clear aaa group server radius *group-name* 257
clear ip dhcp binding {*ip* | *} 69
clear logging debug buffer 323
clear logging system-log buffer 322
clear report [*interface_name*] 327
clock date *yyyy-mm-dd* time *hh:mm:ss* 286
clock time *hh:mm:ss* 286
cnm-agent keepalive interval <10..90> 300
cnm-agent periodic-inform interval <10..86400> 300
cnm-agent server-type {vantage | tr069} 301
cnm-agent trigger-inform [interval] 300
configure 37
connectivity {nail-up | dial-on-demand} 82
content-filter common-list {trust|forbid} 206
content-filter passed warning flush 206
content-filter passed warning timeout <1..1440> 206
content-filter policy *policy_number* shutdown 206
content-filter profile *filtering_profile* commtouch-url match {block | log | warn | pass} 209
content-filter profile *filtering_profile* commtouch-url match-unsafe {block | log | pass} 209
content-filter profile *filtering_profile* commtouch-url offline {block | log | warn | pass} 209
content-filter profile *filtering_profile* commtouch-url unrate {block | log | warn | pass} 209
content-filter profile *filtering_profile* custom-list forbid 207
content-filter profile *filtering_profile* custom-list keyword 208
content-filter profile *filtering_profile* custom-list trust 208

content-filter profile *filtering_profile* url match {block | log | warn | pass} 208
content-filter profile *filtering_profile* url match-unsafe {block | log | pass} 208
content-filter profile *filtering_profile* url offline {block | log | warn | pass} 208
content-filter profile *filtering_profile* url unrate {block | log | warn | pass} 208
content-filter statistics flush 210
content-filter url-cache test 210
content-filter url-server test bluecoat 206
content-filter url-server test commtouch 206
content-filter zsb port <1..65535> 206
copy 37
copy {/cert | /conf | /idp | /packet_trace | /script | /tmp}*file_name-a.conf* {/cert | /conf | /idp | /packet_trace | /script | /tmp}*/file_name-b.conf* 307
copy running-config */conf/file_name.conf* 307
copy running-config startup-config 307
crypto map dial *map_name* 148
crypto map *map_name* 149
crypto map *map_name* 151
crypto map rename *map_name map_name* 149
crypto *map_name* 152
daily-report 329
deactivate 147
deactivate 149
debug (*) 37
debug [cmdexec|corefile|ip |kernel|mac-id-rewrite|observer|switch |system|zyinetpkt|zysh-ipt-op] (*) 40
debug alg 39
debug anti-spam 39
debug app 39
debug app show l7protocol (*) 39
debug ca (*) 39
debug content-filter 39
debug device-ha (*) 39
debug eps 39
debug force-auth (*) 39
debug gui (*) 39
debug gui (*) 39
debug hardware (*) 39
debug idp 39
debug idp-av 39
debug interface 39
debug interface ifconfig [interface] 39
debug interface-group 39
debug ip dns 39
debug ip virtual-server 39
debug ipsec 39
debug logging 39
debug manufacture 39
debug myzyxel server (*) 39
debug network arpignore (*) 39
debug no myzyxel server (*) 39
debug policy-route (*) 39
debug reset content-filter profiling 39
debug service-register 39
debug service-register erase service as 51
debug show content-filter server 39
debug show ipset 39
debug show myzyxel server status 39
debug show myzyxel server status 39
debug sslvpn 39

debug system ipv6 40
debug update server (*) 40
delete 37
delete {/cert | /conf | /idp | /packet_trace | /script | /tmp}/*file_name* 307
details 37
device-ha ap-mode backup sync now 228
device-ha ap-mode cluster-id <1..32> 227
device-ha ap-mode priority <1..254> 227
device-ha ap-mode role {master|backup} 227
device-ha link-monitoring activate 231
device-ha mode {active-passive | legacy} 226
device-ha stop-stub-interface activate 231
device-register checkuser *user_name* 50
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*] 50
dhcp6 65
dhcp6 { server | client | relay upper { *config_interface* | *ipv6_addr* } } 64
dhcp6 address-request 64
dhcp6 address-request 65
dhcp6 duid { *duid* | mac } 64
dhcp6 rapid-commit 64
dhcp6 rapid-commit 65
dhcp6 refresh-time { <600..4294967294> | infinity } 64
dhcp6-lease-object *dhcp6_profile* 64
dhcp6-lease-object *dhcp6_profile* 65
dhcp6-lease-object *dhcp6_profile* { sip-server | ntp-server | dns-server } { *ipv6_addr* | *dhcp6_profile* } 281
dhcp6-lease-object *dhcp6_profile* address *ipv6_addr* duid *duid* 280
dhcp6-lease-object *dhcp6_profile* address-pool *ipv6_addr ipv6_addr* 280
dhcp6-lease-object *dhcp6_profile* prefix-delegation *ipv6_addr_prefix* duid *duid* 280
dhcp6-lease-object rename *dhcp6_profile dhcp6_profile* 281
dhcp6-request-object *dhcp6_profile* 64
dhcp6-request-object *dhcp6_profile* 65
dhcp6-request-object *dhcp6_profile* { dns-server | ntp-server | prefix-delegation | sip-server } 281
dhcp6-request-object rename *dhcp6_profile dhcp6_profile* 281
dhcp-option <1..254> *option_name* {boolean <0..1>| uint8 <0..255> | uint16 <0..65535> 68
diag 37
diag-info 37
diag-info collect 335
dial-in 299
dir 37
dir {/cert | /conf | /idp | /packet_trace | /script | /tmp} 307
disable 37
draw-usage-graphics 329
dscp-marking <0..63> 105
dscp-marking <0..63> 106
dscp-marking class {default | *dscp_class*} 105
dscp-marking class {default | *dscp_class*} 106
duration <0..300> 345
enable 37
enable 63
enable 64
encapsulation {tunnel | transport} 149
eps insert <1..8> *eps_object_name* 238
eps insert <1..8> *eps_profile_name* 156
eps move <1..8> to <1..8> 156
eps move <1..8> to <1..8> 238

eps warning-message {windows-auto-update | windows-security-patch | anti-virus | personal-firewall | windows-registry | process | file-path} 277
exit 105
exit 106
exit 143
exit 144
exit 152
exit 206
exit 206
exit 207
exit 207
exit 208
exit 208
exit 210
exit 277
exit 330
exit 342
exit 38
exit 62
exit 76
exit 85
exit 89
exit 98
fall-back-check-interval <60..86400> 147
files-size <1..10000> 346
file-suffix <*profile_name*> 346
firewall append 139
firewall default-rule action {allow | deny | reject} { no log | log [alert] } 139
firewall delete *rule_number* 139
firewall flush 139
firewall insert *rule_number* 139
firewall move *rule_number* to *rule_number* 139
firewall *rule_number* 138
firewall *zone_object* {*zone_object*|ZyWALL} append 138
firewall *zone_object* {*zone_object*|ZyWALL} delete <1..5000> 139
firewall *zone_object* {*zone_object*|ZyWALL} flush 139
firewall *zone_object* {*zone_object*|ZyWALL} insert *rule_number* 139
firewall *zone_object* {*zone_object*|ZyWALL} move *rule_number* to *rule_number* 139
firewall *zone_object* {*zone_object*|ZyWALL} *rule_number* 138
firewall6 append 140
firewall6 default-rule action {allow | deny | reject} { no log | log [alert] } 140
firewall6 delete *rule_number* 140
firewall6 flush 140
firewall6 insert *rule_number* 140
firewall6 move *rule_number* to *rule_number* 140
firewall6 *rule_number* 139
firewall6 *zone_object* {*zone_object*|ZyWALL} append 140
firewall6 *zone_object* {*zone_object*|ZyWALL} delete <1..5000> 140
firewall6 *zone_object* {*zone_object*|ZyWALL} flush 140
firewall6 *zone_object* {*zone_object*|ZyWALL} insert *rule_number* 140
firewall6 *zone_object* {*zone_object*|ZyWALL} move *rule_number* to *rule_number* 140
firewall6 *zone_object* {*zone_object*|ZyWALL} *rule_number* 139
flood-detection block-period <1..3600> 189
flush 98
force-auth [no] exceptional-service *service_name* 237
force-auth default-rule authentication {required | unnecessary} {no log | log [alert]} .237
force-auth policy <1..1024> 237
force-auth policy append 237
force-auth policy delete <1..1024> 237

force-auth policy flush 237
force-auth policy insert <1..1024> 237
force-auth policy move <1..1024> to <1..1024> 237
gateway 64
gateway *ipv6_addr* metric <0..15> 62
group1 148
group2 148
group5 148
group-key <30..30000> 89
groupname rename *groupname groupname* 235
guard-interval [short | long] 89
guard-interval <short | long> 88
host-ip {*ip-address* | *profile_name* | any> 346
host-port <0..65535> 346
htm 38
http-inspection {http-xxx} log [alert] 190
icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} action {drop | reject-sender | reject-receiver | reject-both}} 190
icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} log [alert] 190
idle <30..30000> 89
idp {signature | system-protect} update daily <0..23> 199
idp {signature | system-protect} update hourly 199
idp {signature | system-protect} update signatures 199
idp {signature | system-protect} update weekly {sun | mon | tue | wed | thu | fri | sat} <0..23> 199
idp {signature| anomaly } rule { append | <1..32> | insert <1..32> } 187
idp {signature| anomaly } rule { delete <1..32> | move <1..32> to <1..32> } 187
idp anomaly *newpro* [base {all | none}] 189
idp customize signature edit *quoted_string* 195
idp customize signature *quoted_string* 195
idp reload 186
idp rename {signature | anomaly} *profile1 profile2* 186
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* 193
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* 193
idp signature *newpro* [base {all | lan | wan | dmz | none}] 188
idp statistics flush 200
idp system-protect 192
idp system-protect deactivate 186
iface {add | del} {*interface_name* | *virtual_interface_name*} 346
in-dnat <1..10> protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535> *mapped-ip address_name* <0..65535> <0..65535> 150
in-dnat append protocol {all | tcp | udp} original-ip *address_name* <0..65535> <0..65535> mapped-ip *address_name* <0..65535> <0..65535> 150
in-dnat delete <1..10> 150
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> 150
in-dnat move <1..10> to <1..10> 150
in-snat source *address_name* destination *address_name* snat *address_name* 150
interface 38
interface {*num*|append|insert *num*} *interface-name* [weight <1..10>|limit <1..2097152>|passive] 98
interface aux 94
interface cellular budget-auto-save <5..1440> 82
interface dial aux 94

interface dial *interface_name* 78
interface disconnect aux 94
interface disconnect *interface_name* 78
interface *interface_name* 69
interface *interface_name* 72
interface *interface_name* 73
interface *interface_name* 74
interface *interface_name* 75
interface *interface_name* 78
interface *interface_name* 92
interface *interface_name* 93
interface *interface_name* ipv6 62
interface *interface_name* no ipv6 64
interface reset {*interface_name*|*virtual_interface_name*|all} 65
interface send statistics interval <15..3600> 65
interface-name {*ppp_interface* | *ethernet_interface*} *user_defined_name* 65
interface-rename *old_user_defined_name new_user_defined_name* 65
ip address *ipv4 ipv4* 85
ip dhcp pool rename *profile_name profile_name* 67
ip dns server -flush 287
ip dns server rule {<1..32>|append|insert <1..32>} access-group {ALL|*address_object*} zone {ALL|*address_object*} action {accept|deny} 288
ip dns server rule move <1..32> to <1..32> 288
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}] 288
ip dns server zone-forwarder move <1..32> to <1..32> 288
ip ftp server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} 295
ip ftp server rule move *rule_number* to *rule_number* 295
ip gateway *ip* metric <0..15> 62
ip http secure-server cipher-suite {*cipher_algorithm*} [*cipher_algorithm*] [*cipher_algorithm*] [*cipher_algorithm*] 291
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} 291
ip http secure-server table {admin|user} rule move *rule_number* to *rule_number* 291
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} 291
ip http server table {admin|user} rule move *rule_number* to *rule_number* 291
ip http-redirect activate *description* 128
ip http-redirect deactivate *description* 128
ip http-redirect *description* interface *interface_name* redirect-to *w.x.y.z* <1..65535> ...128
ip http-redirect *description* interface *interface_name* redirect-to *w.x.y.z* <1..65535> deactivate 128
ip http-redirect flush 128
ip ospf authentication 73
ip ospf authentication message-digest 73
ip ospf authentication same-as-area 73
ip ospf message-digest-key <1..255> md5 *password* 73
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> 109
ip ssh server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} 293
ip ssh server rule move *rule_number* to *rule_number* 293
ip telnet server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} 294
ip telnet server rule move *rule_number* to *rule_number* 294
ip virtual-server {activate | deactivate} *profile_name* 125
ip virtual-server delete *profile_name* 125
ip virtual-server flush 125

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] 124
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] 125
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] 124
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] 124
ip virtual-server rename *profile_name profile_name* 125
ip6 route *destv6/prefix* { *ipv6_global_address* | *ipv6_link_local* | *interface*} [<0..127>] 109
ip6 route *destv6/prefix* { *ipv6_link_local interface*} [<0..127>] 109
ip6 route replace *destv6/prefix* { *gatewayv6* | *interface*} [<0..127>] with *destv6/prefix* { *gatewayv6* | *interface*} [<0..127>] 109
ipsec-isakmp *policy_name* 149
ipv6 6to4 [prefix *ipv6_addr_prefix* | destination-prefix *ipv4_cidr* | relay *ipv4*] 85
ipv6 address *dhcp6_profile dhcp6_suffix_128* 63
ipv6 address *dhcp6_profile dhcp6_suffix_128* 65
ipv6 address *ipv6_addr_prefix* 85
ipv6 dhcp6 [client] 79
ipv6 dhcp6 duid { *duid* | mac } 79
ipv6 neighbor flush {*ipv6* | all} 347
ip-version {ip|ip6|any} 346
isakmp keepalive <2..60> 147
isakmp policy rename *policy_name policy_name* 148
keystring *pre_shared_key* 148
l2tp-over-ipsec authentication *aaa authentication profile_name* 163
l2tp-over-ipsec crypto *map_name* 163
l2tp-over-ipsec pool *address-object* 163
l2tp-over-ipsec recover default-ipsec-policy 163
language <English | Simplified_Chinese | Traditional_Chinese> 301
ldap {activate|deactivate} 265
ldap ip {*ip*|*fqdn*} port <1..65535> [id *name* password *password*] [deactivate] 265
lifetime <180..3000000> 147
list signature {anti-virus | personal-firewall | status} 276
loadbalancing-index <inbound|outbound|total> 99
local-id type {ip *ip* | fqdn *domain_name* | mail *e_mail* | dn *distinguished_name*} 148
local-ip {ip {*ip* | *domain_name*} | interface *interface_name*} 148
local-ip *ip* 151
local-policy *address_name* 149
logging console category *module_name* level {alert | crit | debug | emerg | error | info | notice | warn} 326
logging mail <1..2> schedule daily hour <0..23> minute <0..59> 325
logging mail <1..2> schedule weekly day *day* hour <0..23> minute <0..59> 325
logging mail <1..2> sending_now 325
logging system-log category *module_name* {disable | level normal | level all} 322
logging usb-storage category *category* disable 86
logging usb-storage category *category* level <all|normal> 86
logging usb-storage flushThreshold <1..100> 86
login-page background-color {*color-rgb* | *color-name* | *color-number*} 284
login-page message-color {*color-rgb* | *color-name* | *color-number*} 284
login-page title *title* 284
login-page title-color {*color-rgb* | *color-name* | *color-number*} 284

login-page window-color {*color-rgb* | *color-name* | *color-number*} 285
logo background-color {*color-rgb* | *color-name* | *color-number*} 285
mac *mac* 75
mail-subject set *subject* 329
matching-criteria {any | all} 276
mode {main | aggressive} 147
mode {normal|trunk} 99
move <1..8> to <1..8> 99
mtu <576..1492> 79
mtu <576..1492> 82
nd ra accept 63
nd ra accept 64
nd ra advertise 63
nd ra advertise 64
nd ra default-lifetime 65
nd ra default-lifetime <4..9000> 63
nd ra hop-limit 65
nd ra hop-limit <0..255> 63
nd ra managed-config-flag 63
nd ra managed-config-flag 64
nd ra max-rtr-interval 65
nd ra max-rtr-interval <4..1800> 63
nd ra min-rtr-interval 65
nd ra min-rtr-interval <3..1350> 63
nd ra mtu 64
nd ra mtu <1280..1500> | <0> 63
nd ra other-config-flag 63
nd ra other-config-flag 64
nd ra prefix-advertisement *dhcp6_profile dhcp6_suffix_64* 64
nd ra prefix-advertisement DHCP6_PROFILE DHCP6_SUFFIX_64 65
nd ra prefix-advertisement *ipv6_addr_prefix* [auto { on | off }] [link{ on | off }] [pre-
ferred-time { <0..4294967294> | infinity }] [valid-time{ <0..4294967294> | infinity }]
63
nd ra reachable-time 65
nd ra reachable-time <0..3600000> 63
nd ra retrans-timer 65
nd ra retrans-timer <0..4294967295> 63
nd ra router-preference { low | medium | high } 63
network *ip mask* 68
network IP/<1..32> 68
no address-object *object_name* 242
no anti-spam dnsbl domain *dnsbl_domain* 221
no anti-virus mail-infect-ext activate 178
no app other *rule_number* 171
no app *protocol_name* rule *rule_number* 169
no area IP virtual-link IP message-digest-key <1..255> 113
no arp *ip* 348
no authentication key 112
no bind 187
no budget log [recursive] 81
no budget log-percentage 82
no ca category {local|remote} *certificate_name* 265
no ca validation *name* 265
no content-filter profile *filtering_profile* commtouch-url match {log} 209
no content-filter profile *filtering_profile* commtouch-url match-unsafe {log} 209
no content-filter profile *filtering_profile* commtouch-url offline {log} 209
no content-filter profile *filtering_profile* commtouch-url unrate {log} 209
no content-filter profile *filtering_profile* url match {log} 208
no content-filter profile *filtering_profile* url match-unsafe {log} 208

no content-filter profile *filtering_profile* url offline {log} 208
no content-filter profile *filtering_profile* url unrate {log} 208
no device-ha link-monitoring 231
no device-ha stop-stub-interface 231
no dhcp6-lease-object *dhcp6_profile* 281
no dhcp6-request-object *dhcp6_profile* 281
no dhcp-option <1..254> 68
no dscp-marking 105
no dscp-marking 106
no http-inspection {http-xxx} log 190
no icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} action 190
no icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} log 190
no idp {signature | anomaly} *profile3* 186
no idp {signature| anomaly } rule <1..32> 187
no idp customize signature *custom_sid* 195
no ip dns server rule <1..32> 288
no ip ftp server rule *rule_number* 295
no ip http secure-server cipher-suite {*cipher_algorithm*} 291
no ip http secure-server table {admin|user} rule *rule_number* 291
no ip http server table {admin|user} rule *rule_number* 291
no ip http-redirect *description* 128
no ip ospf authentication 73
no ip ospf message-digest-key 73
no ip ssh server rule *rule_number* 293
no ip telnet server rule *rule_number* 294
no ip virtual-server *profile_name* 124
no ip6 route *destv6/prefix* { *gatewayv6* | *interface*} [<0..127>] 109
no l2tp-over-ipsec session tunnel-id <0..65535> 164
no mac 75
no mail-subject set 329
no network 68
no packet-trace 38
no port <1..*x*> 76
no sa spi *spi* 153
no sa tunnel-name *map_name* 153
no scan-detection sensitivity 189
no schedule-object *object_name* 251
no security {none | wep | wpa | wpa-wpa2 | wpa2} 91
no server-type 271
no service-object *object_name* 247
no signature *sid* action 188
no signature *SID* action 192
no signature *sid* log 188
no signature *sid* log 192
no smtp-address 329
no smtp-auth username 329
no snmp-server rule *rule_number* 297
no sslvpn policy *profile_name* 157
no tcp-decoder {tcp-xxx} log 190
no udp-decoder {truncated-header | undersize-len | oversize-len} action 190
no udp-decoder {truncated-header | undersize-len | oversize-len} log 190
no use-defined-mac 76
no user 152
no username *username* 234
nslookup 38
ntp sync 286
object-group address rename *group_name group_name* 245

object-group service rename *group_name group_name* 249
ocsp {activate|deactivate} 265
ocsp url *url* [id *name* password *password*] [deactivate] 265
or 168
or 169
or 170
or 170
os-type {windows | linux | mac-osx | others} 275
output-power [100% | 50% | 25% | 12.5%] 88
out-snat source *address_name* destination *address_name* snat *address_name* 150
packet-capture configure 345
packet-flow buffer clear *pf_cpu_core_num* 342
packet-flow buffer write 342
packet-flow filter *pf_filter_num_range* 341
packet-trace 38
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*] 345
peer-id type {any | ip *ip* | fqdn *domain_name* | mail *e_mail* | dn *distinguished_name*} 148
peer-ip {*ip* | *domain_name*} [*ip* | *domain_name*] 148
peer-ip *ip* 151
ping 38
ping6 38
ping6{*ipv6* | *hostname*} [source *ipv6*] [size <0..65527>] [forever| count <1..4096>] [interface {*interface_name* | *virtual_interface_name*}][extension *filter_extension*] 346
ping-check {*domain_name* | *ip* | default-gateway} 74
ping-check {*domain_name* | *ip* | default-gateway} fail-tolerance <1..10> 74
ping-check {*domain_name* | *ip* | default-gateway} method {icmp | tcp} 74
ping-check {*domain_name* | *ip* | default-gateway} period <5..30> 74
ping-check {*domain_name* | *ip* | default-gateway} port <1..65535> 74
ping-check {*domain_name* | *ip* | default-gateway} timeout <1..10> 74
policy {*policy_number* | append | insert *policy_number*} 104
policy default-route 107
policy delete *policy_number* 107
policy flush 107
policy list table 107
policy move *policy_number* to *policy_number* 107
policy6 {*policy_number* | append | insert *policy_number*} 106
port <0..65535> 169
port <0..65535> 171
port <1..65535> ending-port <1..65535>] 271
port <1..65535> ending-port <1..65535>] [program-path *program-path*] 271
port status Port<1..*x*> 76
port-grouping *representative_interface* port <1..*x*> 76
proto-type {icmp | icmp6 | igmp | igrp | pim | ah | esp | vrrp | udp | tcp | any} 346
psm 38
qos [none | wmm} 88
qos <none | wmm> 88
reauth <30..30000> 90
reboot 38
redistribute {static | ospf} metric <0..16> 112
release 38
release dhcp *interface-name* 69
remote-policy *address_name* 149
rename 38
rename {/cert | /conf | /idp | /packet_trace | /script | /tmp}/*old-file_name* {/cert | /conf | /idp | /packet_trace | /script | /tmp}/*new-file_name* 307
rename /script/*old-file_name* /script/*new-file_name* 307
renew 38

renew dhcp *interface-name* 69
report packet size statistics clear 329
reset-counter-now 330
ring-buffer <enable|disable> 346
role ap 88
router ospf 112
router ospf 113
router ospf 113
router ospf 72
router rip 112
router rip 72
run 38
run /script/*file_name.zysh* 307
scan-detection block-period <1..3600> 189
scan-detection sensitivity {low | medium | high} 189
scenario {site-to-site-static|site-to-site-dynamic|remote-access-server|remote-access-client} 149
schedule hour <0..23> minute <00..59> 330
schedule-object *object_name date time date time* 252
schedule-object *object_name time time* [*day*] [*day*] [*day*] [*day*] [*day*] [*day*] [*day*] 252
schedule-run 1 *file_name.zysh* {daily | monthly | weekly} time {*date* | sun | mon | tue | wed | thu | fri | sat} 307
security mode {none | wep | wpa | wpa-wpa2 | wpa2} 90
security wep <64 | 128> default-key <1..4> 90
security wep mode <open | share> 90
security wpa <tkip | aes> eap external 90
security wpa <tkip | aes> eap internal *profile-name* tls-cert *certificate name* 90
security wpa <tkip | aes> psk key *psk-key* 90
security wpa2 <tkip | aes> eap external 90
security wpa2 <tkip | aes> eap internal *profile-name* tls-cert *certificate name* 90
security wpa2 <tkip | aes> psk key *psk-key* 90
security wpa-wpa2 <tkip | aes> eap external 90
security wpa-wpa2 <tkip | aes> eap internal *profile-name* tls-cert *certificate name* 90
security wpa-wpa2 <tkip | aes> psk key *psk-key* 90
send-now 330
server-type {file-sharing | owa | web-server} url URL [entry-point *entry_point*] 270
server-type file-sharing share-path *share-path* 271
server-type rdp server-address *server-address* [starting- 271
server-type vnc server-address *server-address* [starting- 271
server-type weblink url *url* 271
service-object *object_name* {tcp | udp} {eq <1..65535> | range <1..65535> <1..65535>} 247
service-object *object_name* icmp *icmp_value* 248
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} 248
service-object *object_name* protocol <1..255> 248
service-object rename *object_name object_name* 248
service-register checkexpire 50
service-register content-filter-engine { bluecoat | commtouch } 51
service-register service-type standard license-key *key_value* 51
service-register service-type trial av-engine {kav|zav} 51
service-register service-type trial service {content-filter|idp} 51
service-register service-type trial service all {kav|zav} 51
service-register service-type trial service as 51
service-register service-type trial service av {kav|zav} 51
session timeout {udp-connect <1..300> | udp-deliver <1..300> | icmp <1..300>} 333
session timeout session {tcp-established | tcp-synrecv | tcp-close | tcp-finwait | tcp-synsent | tcp-closewait | tcp-lastack | tcp-timewait} <1..300> 333
session-limit append 144

session-limit delete *rule_number* 144
session-limit flush 144
session-limit insert *rule_number* 144
session-limit limit <0..8192> 143
session-limit move *rule_number* to *rule_number* 144
session-limit *rule_number* 143
session-limit6 append 144
session-limit6 delete *rule_number* 144
session-limit6 flush 144
session-limit6 insert *rule_number* 144
session-limit6 limit <0..8192> 144
session-limit6 move *rule_number* to *rule_number* 144
session-limit6 *rule_number* 144
set pfs {group1 | group2 | group5 | none} 149
set security-association lifetime seconds <180..3000000> 149
set session-key {ah <256..4095> *auth_key* | esp <256..4095> [cipher *enc_key*] authenticator *auth_key*} 151
setenv 38
setenv-startup stop-on-error off 308
show 169
show 171
show 172
show 216
show 235
show 238
show 38
show 67
show [all] 179
show {address-object | address6-object | service-object | schedule-object} [*object_name*] 242
show aaa authentication {*group-name*|default} 259
show aaa group server ad *group-name* 255
show aaa group server ldap *group-name* 256
show aaa group server radius *group-name* 257
show access-page settings 285
show account [pppoe *profile_name* | pptp *profile_name*] 268
show account cellular *profile_name* 269
show ad-server 253
show anti-spam {smtp | pop3} defaultport 217
show anti-spam activation 215
show anti-spam black-list [status] 219
show anti-spam dnsbl domain 221
show anti-spam dnsbl ip-check-order 221
show anti-spam dnsbl max-query-ip 221
show anti-spam dnsbl query-timeout {smtp | pop3} 221
show anti-spam dnsbl query-timeout time 221
show anti-spam dnsbl statistics 221
show anti-spam dnsbl status 221
show anti-spam ip-reputation private-check 217
show anti-spam ip-reputation query-timeout time 217
show anti-spam ip-reputation statistics 223
show anti-spam mail-scan query-timeout pop3 217
show anti-spam mail-scan query-timeout smtp 217
show anti-spam mail-scan query-timeout time 217
show anti-spam mail-scan statistics 223
show anti-spam mail-scan status 217
show anti-spam rule [*rule_number*] 216
show anti-spam statistics collect 223
show anti-spam statistics ranking {source | mail-address} 223
show anti-spam statistics summary 223

show anti-spam tag {dnsbl | dnsbl-timeout} 221
show anti-spam tag {mail-content | virus-outbreak} 217
show anti-spam tag black-list 219
show anti-spam tag query-timeout 217
show anti-spam white-list [status] 219
show anti-spam xheader {mail-content | virus-outbreak} 217
show anti-spam xheader {white-list | black-list} 219
show anti-spam xheader dnsbl 222
show anti-spam xheader query-timeout 217
show anti-virus activation 178
show anti-virus eicar activation 178
show anti-virus signatures status 182
show anti-virus skip-unknown-file-type activation 178
show anti-virus statistics collect 183
show anti-virus statistics ranking {destination | source | virus-name} 183
show anti-virus statistics summary 183
show anti-virus update 182
show anti-virus update status 182
show app {general|im|p2p|stream} 173
show app all 173
show app all defaultport 173
show app all statistics 173
show app config 173
show app highest sip bandwidth priority 174
show app im support action 173
show app other config 173
show app other rule all 173
show app other rule all statistics 173
show app other rule default 173
show app other rule default statistics 173
show app other rule *rule_number* 173
show app other rule *rule_number* statistics 173
show app other statistics 173
show app *protocol_name* config 173
show app *protocol_name* defaultport 173
show app *protocol_name* rule all 173
show app *protocol_name* rule all statistics 173
show app *protocol_name* rule default 173
show app *protocol_name* rule default statistics 173
show app *protocol_name* rule *rule_number* 173
show app *protocol_name* rule *rule_number* statistics 173
show app *protocol_name* statistics 173
show app-watch-dog config 352
show app-watch-dog monitor-list 352
show app-watch-dog reboot-log 352
show arp-table 348
show boot status 45
show bridge available member 94
show bwm activation 107
show bwm activation 174
show bwm-usage < [policy-route *policy_number*] | [interface *interface_name*] 107
show ca category {local|remote} [name *certificate_name* format {text|pem}] 266
show ca category {local|remote} name *certificate_name* certpath 266
show ca spaceusage 266
show ca validation name *name* 266
show clock date 286
show clock status 286
show clock time 286
show cnm-agent configuration 300

show comport status 45
show conn [user {*username*|any|unknown}] [service {*service-name*|any|unknown}] [source {*ip*|any}] [destination {*ip*|any}] [begin <1..128000>] [end <1..128000>] 328
show conn ip-traffic destination 328
show conn ip-traffic source 328
show conn status 328
show connectivity-check continuous-log status 322
show connectivity-check continuous-log status 74
show connlimit max-per-host 139
show connlimit6 max-per-host 140
show console 286
show content-filter common-list {trust|forbid} 207
show content-filter passed warning 207
show content-filter policy 207
show content-filter profile [*filtering_profile*] 209
show content-filter settings 207
show content-filter statistics collect 210
show content-filter statistics summary 210
show content-filter statistics summary 210
show content-filter url-cache 210
show content-filter url-cache [all-category] [begin *url_cache_range* end *url_cache_range*] [_count] 210
show corefile copy usb-storage 87
show cpu status 45
show crypto map [*map_name*] 148
show daily-report status 329
show ddns [*profile_name*] 120
show device-ha ap-mode backup sync 228
show device-ha ap-mode backup sync status 228
show device-ha ap-mode backup sync summary 228
show device-ha ap-mode forwarding-port *interface_name* 228
show device-ha ap-mode interfaces 228
show device-ha ap-mode master sync 228
show device-ha ap-mode next-sync-time 228
show device-ha ap-mode status 228
show device-ha link-monitoring 231
show device-ha status 226
show device-ha stop-stub-interface 231
show device-ha sync 230
show device-ha sync backup next-sync-time 230
show device-ha sync status 230
show device-ha vrrp-group 230
show device-register status 51
show dhcp6 interface 280
show dhcp6 object-binding *interface_name* 280
show dhcp6-lease-object [*dhcp6_profile*] 280
show dhcp6-request-object [*dhcp6_profile*] 280
show diag-info 335
show diag-info copy usb-storage 87
show dial-in 299
show disk 45
show eps failure-messages 274
show eps profile [*profile_name*] 276
show eps profile *profile_name* signature {anti-virus | personal-firewall} 276
show eps signature {anti-virus | personal-firewall | status} 276
show eps warning-message {windows-auto-update | windows-security-patch | anti-virus | personal-firewall | windows-registry | process | file-path} 276
show extension-slot 45
show fan-speed 45

show firewall 139
show firewall any ZyWALL 139
show firewall block_rules 139
show firewall *rule_number* 139
show firewall status 139
show firewall *zone_object* {*zone_object*|ZyWALL} 139
show firewall *zone_object* {*zone_object*|ZyWALL} *rule_number* 139
show firewall6 140
show firewall6 any ZyWALL 140
show firewall6 block_rules 140
show firewall6 *rule_number* 140
show firewall6 status 140
show firewall6 *zone_object* {*zone_object*|ZyWALL} 140
show firewall6 *zone_object* {*zone_object*|ZyWALL} *rule_number* 140
show force-auth activation 237
show force-auth exceptional-service 237
show force-auth policy {<1..1024> | all} 237
show fqdn 285
show groupname [*groupname*] 235
show hardware-watchdog-timer status 351
show idp 186
show idp {signature | anomaly} base profile 186
show idp {signature | system-protect} signatures {version | date | number} 199
show idp {signature | system-protect} update 199
show idp {signature | system-protect} update status 199
show idp {signature| anomaly } rules 187
show idp anomaly *profile* flood-detection [all details] 191
show idp anomaly *profile* flood-detection {tcp-flood | udp-flood | ip-flood | icmp-flood} details 191
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 ...191
show idp anomaly *profile* http-inspection all details 191
show idp anomaly *profile* icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} details 191
show idp anomaly *profile* icmp-decoder all details 191
show idp anomaly *profile* scan-detection [all details] 190
show idp anomaly *profile* scan-detection {icmp-sweep | icmp-filtered-sweep | open-port} details 191
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 191
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 191
show idp anomaly *profile* scan-detection {udp-portscan | udp-decoy-portscan | udp-portsweep | udp-distributed-portscan | udp-filtered-portscan | udp-filtered-decoy-portscan | .191
show idp anomaly *profile* tcp-decoder {undersize-len | undersize-offset | oversize-offset | bad-length-options | truncated-options | ttcp-detected | obsolete-options | experimental-options} details 191
show idp anomaly *profile* tcp-decoder all details 191
show idp anomaly *profile* udp-decoder {truncated-header | undersize-len | oversize-len} details 191
show idp anomaly *profile* udp-decoder all details 191
show idp *profile* signature {all | custom-signature} details 188
show idp *profile* signature *sid* details 188

show idp profiles 186
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* 193
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* 193
show idp signature all details 186
show idp signature base profile {all|none|wan|lan|dmz} settings 186
show idp signature *profile* signature all details 186
show idp signatures custom-signature all details 195
show idp signatures custom-signature *custom_sid* {details | contents | non-contents} 195
show idp signatures custom-signature number 195
show idp statistics collect 200
show idp statistics ranking {signature-name | source | destination} 200
show idp statistics summary 200
show idp system-protect all details 192
show interface {ethernet | vlan | bridge | ppp | auxiliary} status 61
show interface {*interface_name* | ethernet | vlan | bridge | ppp | virtual ethernet | virtual vlan | virtual bridge | auxiliary | all} 61
show interface cellular [corresponding-slot|device-status|support-device] 82
show interface cellular budget-auto-save 82
show interface cellular corresponding-slot 82
show interface cellular device-status 82
show interface cellular status 82
show interface cellular support-device 82
show interface *interface_name* [budget] 82
show interface *interface_name* device profile 82
show interface *interface_name* device status 82
show interface ppp system-default 79
show interface ppp user-define 79
show interface send statistics interval 62
show interface summary all 62
show interface summary all status 62
show interface tunnel status 85
show interface *tunnel_iface* 85
show interface-group {system-default|user-define|*group-name*} 98
show interface-name 65
show ip dhcp binding [*ip*] 69
show ip dhcp dhcp-options 67
show ip dhcp pool [*profile_name*] 67
show ip dhcp pool *profile_name* dhcp-options 67
show ip dns server 288
show ip dns server database 288
show ip dns server status 288
show ip ftp server status 295
show ip http server secure status 291
show ip http server status 291
show ip http-redirect [*description*] 128
show ip load-balancing link-sticking status 101
show ip route [kernel | connected | static | ospf | rip | bgp] 114
show ip route control-virtual-server-rules 110
show ip route static-dynamic 337
show ip route-settings 109
show ip ssh server status 293
show ip telnet server status 294
show ip virtual-server [*profile_name*] 124
show ipv6 dhcp6 binding 280
show ipv6 interface {*interface_name* | all} 61

show ipv6 nd ra status *config_interface* 61
show ipv6 neighbor-list 347
show ipv6 static address *interface* 61
show ipv6 status 302
show isakmp keepalive 147
show isakmp policy [*policy_name*] 147
show isakmp sa 153
show l2tp-over-ipsec 164
show l2tp-over-ipsec session 164
show language {setting | all} 301
show ldap-server 254
show led status 45
show lockout-users 239
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*] . 323
show logging debug entries field *field* [begin <1..1024> end <1..1024>] 323
show logging debug status 323
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*] 322
show logging entries field *field* [begin <1..512> end <1..512>] 322
show logging status console 326
show logging status mail 324
show logging status syslog 324
show logging status system-log 322
show logging status usb-storage 86
show login-page default-title 285
show login-page settings 285
show logo settings 285
show mac 45
show mem status 45
show ntp server 286
show object-group {address | address6} [*group_name*] 244
show object-group service *group_name* 248
show ospf area IP virtual-link 113
show packet-capture config 347
show packet-capture status 346
show packet-flow buffer [*pf_cpu_core_num*] 342
show packet-flow filter *pf_filter_num_range* 342
show packet-flow status 342
show page-customization 285
show ping-check [*interface_name* | status] 74
show policy-route [*policy_number*] 107
show policy-route begin <1..200> end <1..200> 107
show policy-route controll-ipsec-dynamic-rules 107
show policy-route controll-virtual-server-rules 107
show policy-route override-direct-route 107
show policy-route rule_count 107
show policy-route underlayer-rules 107
show policy-route6 override-direct-route 107
show port setting 76
show port status 76
show port vlan-id 93
show port-grouping 76
show radius-server 255
show ram-size 45
show redundant-power status 45

show reference object aaa authentication [default | *auth_method*] 43
show reference object account pppoe [*object_name*] 43
show reference object account pptp [*object_name*] 43
show reference object address [*object_name*] 43
show reference object address6 [*object_name*] 43
show reference object ca category {local|remote} [*cert_name*] 43
show reference object crypto map [*crypto_name*] 43
show reference object dhcp6-lease-object [*object_name*] 44
show reference object dhcp6-request-object [*object_name*] 44
show reference object eps [*object_name*] 43
show reference object interface [*interface_name* | *virtual_interface_name*] 43
show reference object isakmp policy [*isakmp_name*] 43
show reference object schedule [*object_name*] 43
show reference object service [*object_name*] 43
show reference object sslvpn application [*object_name*] 43
show reference object sslvpn policy [*object_name*] 43
show reference object username [*username*] 43
show reference object zone [*object_name*] 44
show reference object-group aaa ad [*group_name*] 44
show reference object-group aaa ldap [*group_name*] 44
show reference object-group aaa radius [*group_name*] 44
show reference object-group address [*object_name*] 44
show reference object-group address6 [*object_name*] 44
show reference object-group interface [*object_name*] 44
show reference object-group service [*object_name*] 44
show reference object-group username [*username*] 44
show report [*interface_name* {ip | service | url}] 327
show report packet size statistics {*interface_name*} [interval *interval*] 329
show report packet size statistics status 328
show report status 327
show rip {global | interface {all | *interface_name*}} 72
show route order 337
show running-config 308
show sa monitor [{begin <1..1000>} | {end <1..1000>} | {crypto-map *regexp*} | {policy *regexp*}
|{rsort *sort_order*} | {sort *sort_order*}] 153
show schedule-object 251
show serial-number 45
show service-object [*object_name*] 247
show service-register content-filter-engine 51
show service-register reseller-info 51
show service-register server-type 51
show service-register status {all|idp|av|sslvpn|sslvpn-status} 51
show service-register status as 51
show service-register status content-filter { bluecoat | commtouch } 51
show session timeout {icmp | tcp-timewait | udp} 333
show session-limit 144
show session-limit begin *rule_number* end *rule_number* 144
show session-limit *rule_number* 144
show session-limit status 144
show session-limit6 144
show session-limit6 begin *rule_number* end *rule_number* 144
show session-limit6 *rule_number* 144
show session-limit6 status 144
show setenv-startup 308
show snmp status 297
show socket listen 45
show socket open 45
show software-watchdog-timer log 351
show software-watchdog-timer status 351

show sslvpn application [*application_object*] 270
show sslvpn monitor 156
show ssl-vpn network-extension local-ip 156
show sslvpn policy [*profile_name*] 156
show system default-interface-group 99
show system default-snat 99
show system route default-wan-trunk 337
show system route dynamic-vpn 337
show system route nat-1-1 337
show system route policy-route 337
show system route site-to-site-vpn 337
show system snat default-snat 337
show system snat nat-1-1 337
show system snat nat-loopback 337
show system snat order 337
show system snat policy-route 337
show system uptime 45
show usb-storage 86
show username [*username*] 234
show users {*username* | all | current} 239
show users default-setting {all | user-type {admin|user|guest|limited-admin|ext-user| ext-group-user}} 235
show users idle-detection-settings 236
show users retry-settings 236
show users simultaneous-logon-settings 236
show users update-lease-settings 236
show version 45
show vpn-concentrator [*profile_name*] 151
show vpn-configuration-provision activation 152
show vpn-configuration-provision authentication 152
show vpn-configuration-provision rules 152
show vpn-counters 153
show vrpt send device information interval 324
show vrpt send interface statistics interval 324
show vrpt send system status interval 324
show wlan mac-filter 92
show wlan mac-filter status 92
show workspace application 157
show workspace cifs 157
show zone [*profile_name*] 116
show zone binding-iface 116
show zone default-binding 116
show zone none-binding 116
show zone system-default 116
show zone user-define 116
shutdown 38
signature *sid* action {drop | reject-sender | reject-receiver | reject-both} 188
signature *sid* action {drop | reject-sender | reject-receiver | reject-both} 192
signature *sid* log [alert] 188
signature *sid* log [alert] 192
smtp-address {*ip* | *hostname*} 329
smtp-auth username *username* password *password* 329
snaplen <68..1512> 346
snmp-server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny} 297
snmp-server rule move *rule_number* to *rule_number* 297
split-size <1..2048> 346
ssid *ssid* 91
sslvpn network-extension local-ip *ip* 156

sslvpn no connection username *user_name* 157
sslvpn policy {*profile_name* | *profile_name* append | *profile_name* insert <1..16>} 156
sslvpn policy move <1..16> to <1..16> 157
sslvpn policy rename *profile_name profile_name* 157
station-limit <1..255> 91
storage <internal|usbstorage> 346
system default-interface-group *group-name* 99
tcp-decoder {tcp-xxx} log [alert] 190
telnet 38
test aaa 38
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* 260
tracepath6 {*ipv6* | *hostname*} 346
traceroute 38
traceroute {*ip* | *hostname*} 345
traceroute6 38
traceroute6 {*ipv6* | *hostname*} 345
traffic-prioritize {tcp-ack|content-filter|dns} bandwidth <0..1048576> priority <1..7> [maximize-bandwidth-usage]; 85
traffic-prioritize {tcp-ack|content-filter|dns} deactivate 85
traffic-prioritize {tcp-ack|content-filter|dns|ipsec-vpn|ssl-vpn} bandwidth <0..1048576> priority <1..7> [maximize-bandwidth-usage]; 62
traffic-prioritize {tcp-ack|content-filter|dns|ipsec-vpn|ssl-vpn} deactivate 62
transform-set *crypto_algo_ah* [*crypto_algo_ah* [*crypto_algo_ah*]] 149
transform-set *crypto_algo_esp* [*crypto_algo_esp* [*crypto_algo_esp*]] 149
transform-set isakmp-algo [isakmp_algo [*isakmp_algo*]] 147
trigger append incoming *service_name* trigger *service_name* 105
trigger delete <1..8> 105
trigger insert <1..8> incoming *service_name* trigger *service_name* 105
trigger move <1..8> to <1..8> 105
tunnel destination *ipv4* 85
tunnel mode [ipv6ip [manual | 6to4]]] 85
tunnel mode ip gre 85
tunnel source [*ipv4*|*tunnel_bind_interface*|_any] 85
type {internal | external | general} 76
udp-decoder {truncated-header | undersize-len | oversize-len} action {drop | reject-sender | reject-receiver | reject-both} 190
udp-decoder {truncated-header | undersize-len | oversize-len} log [alert] 190
udp-filtered-distributed-portscan | udp-filtered-portsweep} details 191
unlock lockout-users {*ip* | console| *ipv6_addr*} 239
url 210
url [server *rating_server*] [timeout *query_timeout*] 206
url timeout *query_timeout* 206
usb-storage mount 86
usb-storage umount 86
usb-storage warn *number* <*percentage*|megabyte> 86
use-defined-mac 76
user *username* 152
username rename *username username* 234
username *username* [no] description *description* 234
username *username* [no] logon-lease-time <0..1440> 235
username *username* [no] logon-re-auth-time <0..1440> 235
username *username* [no] logon-time-setting <default | manual> 234
username *username* nopassword user-type {admin | guest | limited-admin | user} 234
username *username* password *password* user-type {admin | guest | limited-admin | user} ...234
username *username* user-type ext-group-user associated-aaa-server *server_profile* group-id *id* 234

username *username* user-type ext-user 234
users default-setting [no] logon-lease-time <0..1440> 235
users default-setting [no] logon-re-auth-time <0..1440> 235
users default-setting [no] user-type <admin |ext-user|guest|limited-admin|user|ext-group-user> 235
users default-setting [no] user-type <admin |ext-user|guest|limited-admin|user|ext-group-user> logon-lease-time <0..1440> 235
users default-setting [no] user-type <admin |ext-user|guest|limited-admin|user|ext-group-user> logon-re-auth-time <0..1440> 236
users force-logout *username* | *ip* | *ipv6_addr* 239
vpn-concentrator rename *profile_name profile_name* 152
vpn-configuration-provision authentication *auth_method* 152
vpn-configuration-provision rule { append | *conf_index* | insert *conf_index* } 152
vpn-configuration-provision rule { delete *conf_index* | move *conf_index* to *conf_index* } .152
vrpt send device information interval <15..3600> 324
vrpt send interface statistics interval <15..3600> 324
vrpt send system status interval <15..3600> 324
wep-key <1..4> *key* 91
windows-version {windows-2000 | windows-xp | windows-2003 | windows-2008 | windows-vista | windows-7 | windows-2008r2} 276
wlan mac-filter associate <allow | deny> 92
wlan *slot_name* 88
write 308
write 38
zone *profile_name* 116