ZyXEL

ZyWALL / USG (ZLD) Series

Security Firewalls

Version: 4.10 / 4.11 / 4.13 / 4.15 / 4.16 / 4.20

Edition 1, 8/2016

CLI Reference Guide

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

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

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

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

Do not use commands not documented in this guide.

How To Use This Guide

- Read Chapter 1 on page 23 for how to access and use the CLI (Command Line Interface).
- Read Chapter 2 on page 37 to learn about the CLI user and privilege modes.

Related Documentation

- Quick Start Guide

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

  The User’s Guide introduces the ZyWALL / USG series, describes the hardware and explains how to use the Web Configurator to configure the ZyWALL / USG.
- Web Configurator Online Help

  Click the help icon in any screen for help in configuring that screen and supplementary information.

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

- More Information

  Go to **support.zyxel.com** to find other information on the ZyWALL / USG.

Table of Contents

Chapter 42

Chapter 43

Chapter 44

Chapter 45

Chapter 46

PART I

Introduction

Command Line Interface

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

1.1 Overview

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

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

1.1.1 The Configuration File

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

You can perform the following with a configuration file:

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

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

1.2 Accessing the CLI

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

Note: The ZyWALL / USG might force you to log out of your session if reauthentication time, lease time, or idle timeout is reached. See Chapter 42 on page 315 for more information about these settings.

1.2.1 Console Port

The default settings for the console port are as follows.

Table 1 Managing the ZyWALL / USG: Console Port

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

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

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

Figure 1 Console Port Power-on Display

```
U-Boot 2011.03 (Development build, svnversion: u-boot:424M, exec:exported) (Build
time: Aug 28 2013 - 14:19:07)

BootModule Version: V1.01 | Aug 28 2013 14:19:07
DRAM: Size = 1024 Mbytes

Press any key to enter debug mode within 3 seconds.
```

After the initialization, the login screen displays.

Figure 2 Login Screen

```
Welcome to USG60W

Username:
```

Enter the user name and password at the prompts.

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

1.2.2 Web Configurator Console

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

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

1 Log into the web configurator.

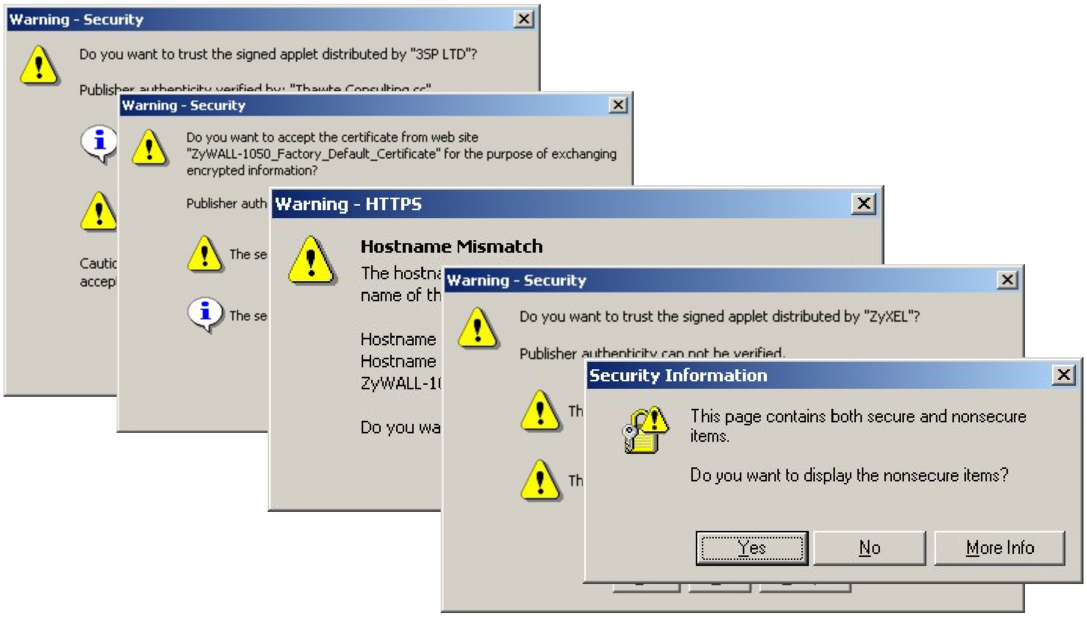
2 Click the **Console** icon in the top-right corner of the web configurator screen.

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

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

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

Figure 3 Web Console: Security Warnings



Warning - Security

Do you want to trust the signed applet distributed by "3SP LTD"?

Publisher authenticity verified by: "Thawte Consulting cc"

Cautic accep

Warning - Security

Do you want to accept the certificate from web site "ZyWALL-1050_Factory_Default_Certificate" for the purpose of exchanging encrypted information?

Publisher auth

The se

The se

Warning - HTTPS

Hostname Mismatch

The hostn name of th

Hostname Hostname ZyWALL-1

Do you wa

Warning - Security

Do you want to trust the signed applet distributed by "ZyXEL"?

Publisher authenticity can not be verified.

Th

Th

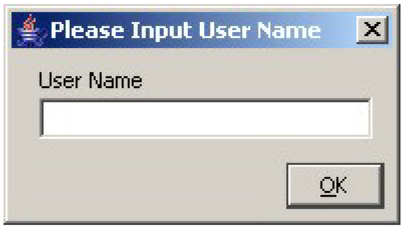
Security Information

This page contains both secure and nonsecure items.

Do you want to display the nonsecure items?

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

Figure 4 Web Console: User Name



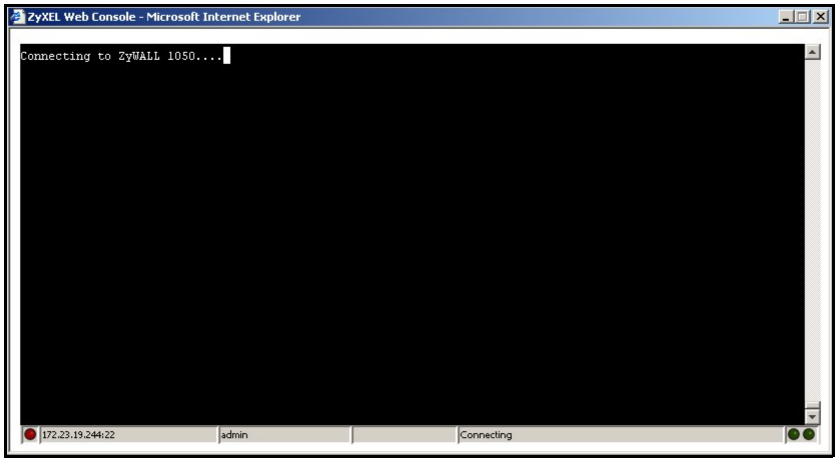
Please Input User Name

User Name

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

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

Figure 5 Web Console: Connecting

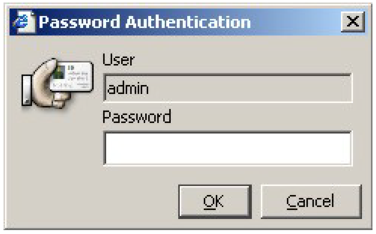


```
Connecting to ZyWALL 1050....
```

172.23.19.244:22 | admin | Connecting

Then, the **Password** screen appears.

Figure 6 Web Console: Password



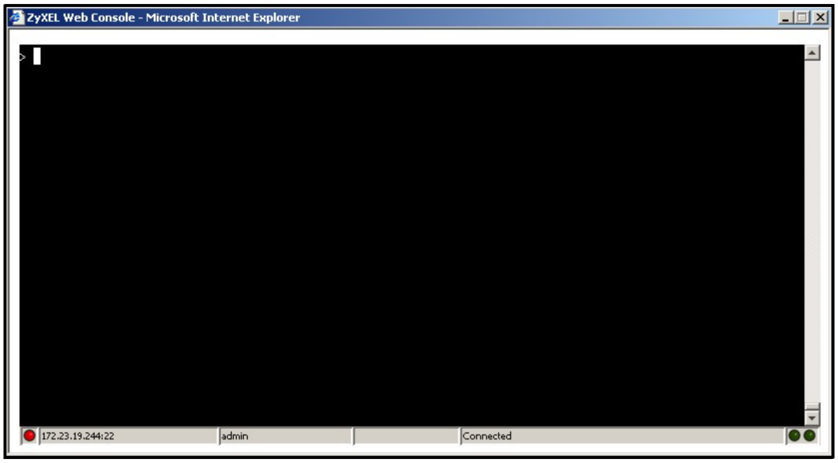
User

admin

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



```
>
```

172.23.19.244:22 | admin | Connected

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

1.2.3 Telnet

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

1. If your computer is connected to the ZyWALL / USG over the Internet, skip to the next step. Make sure your computer IP address and the ZyWALL / USG IP address are on the same subnet.
2. In Windows, click **Start** (usually in the bottom left corner) and **Run**. Then type `telnet` and the ZyWALL / USG's IP address. For example, enter `telnet 192.168.1.1` (the default management IP address).
3. Click **OK**. A login screen displays. Enter the user name and password at the prompts.

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

1.2.4 SSH (Secure SHell)

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

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

Figure 8 SSH Login Example

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

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

1.3 How to Find Commands in this Guide

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

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

1.4 How Commands Are Explained

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

1.4.1 Background Information (Optional)

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

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

1.4.2 Command Input Values (Optional)

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

1.4.3 Command Summary

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

1.4.4 Command Examples (Optional)

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

1.4.5 Command Syntax

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

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

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

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

1 Enter `service-object` exactly as it appears.

2 Enter the name of the object where you see *`object-name.`*

3 Enter `tcp` or `udp`, depending on the service object you want to create.

4 Finally, do one of the following.

- Enter `eq` exactly as it appears, followed by a number between 1 and 65535.

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

1.4.6 Changing the Password

It is highly recommended that you change the password for accessing the ZyWALL / USG. See Section 42.2 on page 316 for the appropriate commands.

1.4.7 Idle Timeout

See Section 42.2.1 on page 316 for commands on changing the default logout time when no activity is recorded.

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 / USG
How you enter it	Log in to the ZyWALL / USG	Type **enable** in **User** mode	Type **configure terminal** in **User** or **Privilege** mode	Type the command used to create the specific part in **Configuration** mode

What the prompt looks like	`Router>`	`Router#`	`Router(config)#`	(varies by part)
				`Router(zone)#`
				`Router(config-if-ge)#`
				`...`

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

See Chapter 42 on page 315 for more information about the user types. **User** users can only log in, look at (but not run) the available commands in **User** mode, and log out. **Limited-Admin** users can look at the configuration in the web configurator and CLI, and they can run basic diagnostics in the CLI. **Admin** users can configure the ZyWALL / USG in the web configurator or CLI.

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

1.6 Shortcuts and Help

1.6.1 List of Available Commands

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

Figure 9 Help: Available Commands Example 1

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

Figure 10 Help: Available Command Example 2

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

1.6.2 List of Sub-commands or Required User Input

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

Figure 11 Help: Sub-command Information Example

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

Figure 12 Help: Required User Input Example

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

1.6.3 Entering Partial Commands

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

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

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

Figure 13 Non-Unique Partial Command Example

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

1.6.4 Entering a ? in a Command

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

1.6.5 Command History

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

1.6.6 Navigation

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

1.6.7 Erase Current Command

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

1.6.8 The no Commands

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

1.7 Input Values

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

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

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

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

Table 3 Input-Value Formats for Strings in CLI Commands

<table>
<tr><th>TAG</th><th># VALUES</th><th>LEGAL VALUES</th></tr>
<tr><td>*</td><td>1</td><td>*</td></tr>
<tr><td>all</td><td>--</td><td>ALL</td></tr>
<tr><td rowspan="6">authentication key</td><td colspan="2">Used in IPSec SA</td></tr>
<tr><td>32-40
16-20</td><td>“0x” or “0X” + 32-40 hexadecimal values
alphanumeric or ;|`~!@#$%^&*()_+\\{}':,./<>=-</td></tr>
<tr><td colspan="2">Used in MD5 authentication keys for RIP/OSPF and text authentication key for RIP</td></tr>
<tr><td>0-16</td><td>alphanumeric or _-</td></tr>
<tr><td colspan="2">Used in text authentication keys for OSPF</td></tr>
<tr><td>0-8</td><td>alphanumeric or _-</td></tr>
<tr><td>certificate name</td><td>1-31</td><td>alphanumeric or ;`~!@#$%^&()_+[\]{}',.=-</td></tr>
<tr><td>community string</td><td>0-63</td><td>alphanumeric or .-
first character: alphanumeric or -</td></tr>
</table>

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

TAG	# VALUES	LEGAL VALUES
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 '()+,/:=?;!*#@$_%-
distinguished name	1-511	alphanumeric, spaces, or .@=,_-
domain name	Used in content filtering	
	0+	lower-case letters, numbers, or .-
	Used in ip dns server	
	0-247	alphanumeric or .- first character: alphanumeric or -
	Used in domainname, ip dhcp pool, and ip domain	
	0-254	alphanumeric or ._- first character: alphanumeric or -
email	1-63	alphanumeric or .@_-
e-mail	1-64	alphanumeric or .@_-
encryption key	16-64 8-32	“0x” or “0X” + 16-64 hexadecimal values alphanumeric or ;\\|`~!@#$%^&*()_+\\{}':,./<>=-
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 `~!@#$%^&*()_\-+={}|\;:'<,>./
isp account username	0-30	alphanumeric or -_@$./

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

<table>
<tr><th>TAG</th><th># VALUES</th><th>LEGAL VALUES</th></tr>
<tr><td>ipv6_addr</td><td></td><td>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.</td></tr>
<tr><td><i>key length</i></td><td>--</td><td>512, 768, 1024, 1536, 2048, 4096</td></tr>
<tr><td><i>license key</i></td><td>25</td><td>“S-” + 6 upper-case letters or numbers + “-” + 16 upper-case letters or numbers</td></tr>
<tr><td><i>mac address</i></td><td>--</td><td>aa:bb:cc:dd:ee:ff (hexadecimal)</td></tr>
<tr><td><i>mail server fqdn</i></td><td></td><td>lower-case letters, numbers, or -.</td></tr>
<tr><td><i>name</i></td><td>1-31</td><td>alphanumeric or _-</td></tr>
<tr><td><i>notification message</i></td><td>1-81</td><td>alphanumeric, spaces, or '()+,/:=?;!*#@$_%-</td></tr>
<tr><td><i>password: less than 15 chars</i></td><td>1-15</td><td>alphanumeric or `~!@#$%^&*()_\-+={}|\;:'<,>./</td></tr>
<tr><td><i>password: less than 8 chars</i></td><td>1-8</td><td>alphanumeric or ;/?:@&=+$\.-_!~*'()%,#$</td></tr>
<tr><td rowspan="8"><i>password</i></td><td colspan="2">Used in user and ip ddns</td></tr>
<tr><td>1-63</td><td>alphanumeric or `~!@#$%^&*()_-+={}|\;:'<,>./</td></tr>
<tr><td colspan="2">Used in e-mail log profile SMTP authentication</td></tr>
<tr><td>1-63</td><td>alphanumeric or `~!@#$%^&*()_-+={}|\;:'<>./</td></tr>
<tr><td colspan="2">Used in device HA synchronization</td></tr>
<tr><td>1-63</td><td>alphanumeric or ~#%^*_-={}:,.</td></tr>
<tr><td colspan="2">Used in registration</td></tr>
<tr><td>6-20</td><td>alphanumeric or .@_-</td></tr>
<tr><td><i>phone number</i></td><td>1-20</td><td>numbers or ,+</td></tr>
<tr><td><i>preshared key</i></td><td>16-64</td><td>“0x” or “0X” + 16-64 hexadecimal values
alphanumeric or ;|`~!@#$%^&*()_+\{}':,./<>=-</td></tr>
<tr><td><i>profile name</i></td><td>0-30</td><td>alphanumeric or _-
first character: letters or _-</td></tr>
<tr><td><i>proto name</i></td><td>1-16</td><td>lower-case letters, numbers, or -</td></tr>
<tr><td><i>protocol name</i></td><td>0-30</td><td>alphanumeric or _-
first character: letters or _-</td></tr>
<tr><td><i>quoted string less than 127 chars</i></td><td>1-255</td><td>alphanumeric, spaces, or ;/?:@&=+$\.-_!~*'()%,</td></tr>
<tr><td><i>quoted string less than 63 chars</i></td><td>1-63</td><td>alphanumeric, spaces, or ;/?:@&=+$\.-_!~*'()%</td></tr>
<tr><td><i>quoted string</i></td><td>0+</td><td>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</td></tr>
</table>

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

<table>
<tr><th>TAG</th><th># VALUES</th><th>LEGAL VALUES</th></tr>
<tr><td>service name</td><td>0-63</td><td>alphanumeric or -_@$./</td></tr>
<tr><td>spi</td><td>2-8</td><td>hexadecimal</td></tr>
<tr><td>string less than 15 chars</td><td>1-15</td><td>alphanumeric or -_</td></tr>
<tr><td>string: less than 63 chars</td><td>1-63</td><td>alphanumeric or `~!@#$%^&*()_-+={}|\;:'<,>./</td></tr>
<tr><td>string</td><td>1+</td><td>alphanumeric or -_@</td></tr>
<tr><td>subject</td><td>1-61</td><td>alphanumeric, spaces, or '()+,./:=?;!*#@$_%-</td></tr>
<tr><td>system type</td><td>0-2</td><td>hexadecimal</td></tr>
<tr><td>timezone [-+]hh</td><td>--</td><td>-12 through +12 (with or without “+”)</td></tr>
<tr><td>url</td><td>1-511</td><td>alphanumeric or '()+,/:.=?;!*#@$_%-</td></tr>
<tr><td rowspan="4">url</td><td colspan="2">Used in content filtering redirect</td></tr>
<tr><td>“http://”+
“https://”+</td><td>alphanumeric or ;/?:@&=+$\.-_!~*'()%,
starts with “http://” or “https://”
may contain one pound sign (#)</td></tr>
<tr><td colspan="2">Used in other content filtering commands</td></tr>
<tr><td>“http://”+</td><td>alphanumeric or ;/?:@&=+$\.-_!~*'()%,
starts with “http://”
may contain one pound sign (#)</td></tr>
<tr><td rowspan="4">user name</td><td colspan="2">Used in VPN extended authentication</td></tr>
<tr><td>1-31</td><td>alphanumeric or _-</td></tr>
<tr><td colspan="2">Used in other commands</td></tr>
<tr><td>0-30</td><td>alphanumeric or _-
first character: letters or _-</td></tr>
<tr><td>username</td><td>6-20</td><td>alphanumeric or .@_-
registration</td></tr>
<tr><td>user name</td><td>1+</td><td>alphanumeric or -_.
logging commands</td></tr>
<tr><td>user@domainname</td><td>1-80</td><td>alphanumeric or .@_-</td></tr>
<tr><td>vrrp group name: less than 15 chars</td><td>1-15</td><td>alphanumeric or _-</td></tr>
<tr><td>week-day sequence, i.e. 1=first,2=second</td><td>1</td><td>1-4</td></tr>
<tr><td>xauth method</td><td>1-31</td><td>alphanumeric or _-</td></tr>
<tr><td>xauth password</td><td>1-31</td><td>alphanumeric or ;|`~!@#$%^&*()_+\{}':,./<>=-</td></tr>
<tr><td>mac address</td><td>0-12 (even number)</td><td>hexadecimal
for example: aa aabbcc aabbccddeeff</td></tr>
</table>

1.8 Ethernet Interfaces

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

- For some ZyWALL / USG models, use ge*x*, *x* = 1~N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model.
- For other ZyWALL / USG models use a name such as wan1, wan2, opt, lan1, or dmz.

1.9 Saving Configuration Changes

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

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

1.10 Logging Out

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

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

User and Privilege Modes

This chapter describes how to use these two modes.

2.1 User And Privilege Modes

This is the mode you are in when you first log into the CLI. (Do not confuse 'user mode' with types of user accounts the ZyWALL / USG uses. See Chapter 42 on page 315 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 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 psm commands are for ZyXEL's internal manufacturing process.

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

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

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

COMMAND	MODE	DESCRIPTION
`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 / USG. All unsaved changes are lost after the ZyWALL / USG restarts.

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

2.1.1 Debug Commands

Debug commands marked with an asterisk (*) are not available when the debug flag is on and are for ZyXEL service personnel use only. The debug commands follow a Linux-based syntax, so if there is a Linux equivalent, it is displayed in this chapter for your reference. You must know a command listed here well before you use it. Otherwise, it may cause undesired results.

Table 5 Debug Commands

COMMAND SYNTAX	DESCRIPTION	LINUX COMMAND EQUIVALENT
`debug alg`	FTP/SIP ALG debug commands	
`debug anti-spam`	Anti-Spam debug commands	
`debug app`	Application patrol debug command	
`debug app show l7protocol (*)`	Shows app patrol protocol list	`> cat /etc/l7_protocols/protocol.list`

Table 5 Debug Commands (continued)

COMMAND SYNTAX	DESCRIPTION	LINUX COMMAND EQUIVALENT
`debug ca (*)`	Certificate debug commands	
`debug content-filter`	Content Filtering debug commands	
`debug show content-filter https-domain-filter cache`	Displays content filtering HTTPs Domain Filter cache entries.	
`debug content-filter https-domain-filter cache flush`	Removes content filtering HTTPs Domain Filter cache entries.	
`debug device-ha (*)`	Device HA 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 server register`	Set the myzyxel.com registration server	
`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 status debug commands	
`debug show ipset`	Lists the ZyWALL / USG‘s received cards	
`debug sslvpn`	SSL VPN debug commands	
`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	

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 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.
`show reference object zone [`*`object_name`*`]`	Displays which configuration settings reference the specified zone object.

Table 6 show reference Commands (continued)

COMMAND	DESCRIPTION
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
===========================================================================
Security Policy Control
3                    N/A
LAN1-to-USG-2000
Router(config)#
```

4

Status

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

Table 7 Status Show Commands

COMMAND	DESCRIPTION
`show boot status`	Displays details about the ZyWALL / USG's startup state.
`show comport status`	Displays whether the console is on or off.
`show cpu status`	Displays the CPU utilization.
`show cpu all`	Displays the CPU utilization of each CPU.
`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 led status`	Displays the status of each LED on the ZyWALL / USG.
`show mac`	Displays the ZyWALL / USG's MAC address.
`show mem status`	Displays what percentage of the ZyWALL / USG's memory is currently being used.
`show ram-size`	Displays the size of the ZyWALL / USG's on-board RAM.
`show serial-number`	Displays the serial number of this ZyWALL / USG.
`show socket listen`	Displays the ZyWALL / USG's listening ports
`show socket open`	Displays the ports that are open on the ZyWALL / USG.
`show system uptime`	Displays how long the ZyWALL / USG has been running since it last restarted or was turned on.
`show version`	Displays the ZyWALL / USG's model, firmware and build information.

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

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

Router(config)# show cpu all
CPU core 0 utilization: 0 %
CPU core 0 utilization for 1 min: 0 %
CPU core 0 utilization for 5 min: 0 %
CPU core 1 utilization: 0 %
CPU core 1 utilization for 1 min: 0 %
CPU core 1 utilization for 5 min: 2 %
CPU core 2 utilization: 0 %
CPU core 2 utilization for 1 min: 0 %
CPU core 2 utilization for 5 min: 0 %
CPU core 3 utilization: 0 %
CPU core 3 utilization for 1 min: 0 %
CPU core 3 utilization for 5 min: 0 %
```

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

```
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 110
firmware version: 2.20(AQQ.0)b3
BM version      : 1.08
build date      : 2014-01-21 01:18:06
```

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

```
Router> show led status
sys: green
usbled: off
Router>
```

5

Registration

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

5.1 myZyXEL.com Overview

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

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

First, go to *http://www.myZyXEL.com* with the ZyWALL / USG's serial number and LAN MAC address to register the ZyWALL / USG. Refer to the web site's on-line help for details. You can also go to the portal and see license status using the **Licensing > Registration** screens.

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

5.1.1 Subscription Services Available on the ZyWALL / USG

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

ZyWALL models need a license for UTM (Unified Threat Management) functionality. See the Introduction chapter in the ZyWALL / USG User's Guide or the product datasheet for details.

You can purchase an EiCard and enter the license key from it, at *http://www.myzyxel.com* to have the ZyWALL use UTM services or have the ZyWALL / USG use more SSL VPN tunnels. See the respective chapters in the User's Guide for more information about UTM features.

- The ZyWALL / USG's anti-virus packet scanner uses the signature files on the ZyWALL / USG to detect virus files. Your ZyWALL / USG scans files transmitting through the enabled interfaces into the network. Subscribe to signature files for ZyXEL's anti-virus engine. After the service is activated, the ZyWALL / USG can download the up-to-date signature files from the update server.

  After the trial expires, you need to purchase an EiCard and enter the PIN number (license key) at *http://www.myzyxel.com*.
- The IDP and application patrol features use the IDP/AppPatrol signature files on the ZyWALL / USG. IDP detects malicious or suspicious packets and responds immediately. Application patrol conveniently manages the use of various applications on the network. After the service is activated, the ZyWALL / USG can download the up-to-date signature files from the update server.
- SSL VPN tunnels provide secure network access to remote users. You can purchase and enter a license key to have the ZyWALL / USG use more SSL VPN tunnels.

- The content filter allows or blocks access to web sites. Subscribe to category-based content filtering to block access to categories of web sites based on content. Your ZyWALL / USG accesses an external database that has millions of web sites categorized based on content. You can have the ZyWALL / USG block, block and/or log access to web sites based on these categories.
- You will get automatic e-mail notification of new signature releases from mySecurityZone after you activate the IDP/AppPatrol service. You can also check for new signatures at *http://mysecurity.zyxel.com*.

See the respective chapters for more information about these features.

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

5.2 Registration Commands

The following table 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 8 Command Summary: Registration

COMMAND	DESCRIPTION
`service-register checkexpire`	Gets information of all service subscriptions from myZyXEL.com and updates the status table.
`show device-register status`	Displays whether the device is registered and account information.
`show service-register status {all|idp|av|sslvpn-status|as|content-filter|external-ap-control|pkg}`	Displays service license information.
`show service-register status content-filter {commtouch}`	Displays Commtouch content filter service license information.
`show service-register content-filter-engine`	Displays which external web filtering service the ZyWALL / USG is set to use for content filtering.
`show service-register status as`	Displays whether the Anti-Spam service is registered and account information.
`debug myzyxel2 show [as|av|idp|content-filter|sslvpn|extmaps|pkg] shm`	Shows debug information for services at myZyXEL.com
`debug show myzyxel-server status`	Shows debug information for the myZyXEL.com server.

5.2.1 Command Examples

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
```

6

AP Management

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

6.1 AP Management Overview

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

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

6.2 AP Management Commands

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

Table 9 Input Values for General AP Management Commands

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

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

Table 10 Command Summary: AP Management

COMMAND	DESCRIPTION
`capwap ap add` *`ap_mac`* `[`*`ap_model`*`]`	Adds the specified AP to the ZyWALL / USG for management. If manual add is disabled, this command can still be used; if you add an AP before it connects to the network, then this command simply preconfigures the management list with that AP's information.
`capwap ap kick {all |` *`ap_mac`*`}`	Removes the specified AP (*ap_mac*) or all connected APs (*all*) from the management list. Doing this removes the AP(s) from the management list. If the ZyWALL / USG is set to automatically add new APs to the AP management list, then any kicked APs are added back to the management list as soon as they reconnect.
`capwap ap reboot` *`ap_mac`*	Forces the specified AP (*ap_mac*) to restart. Doing this severs the connections of all associated stations.
`capwap ap local-ap`	Enters sub-command mode for the built-in AP (in ZyWALL / USG models with a W in the name).
`[no]` *`cw_slot_name_ac`* `ssid-profile <1..8>`	Sets the radio (*slot_name*) to AP mode and assigns a created profile to the radio. Use the no command to remove the AP mode profile assignment for the specified radio (*slot_name*).
`[no] override` *`cw_slot_name_ac`* `{radio-setting | ssid-setting | output-power}`	Sets the ZyWALL / USG to overwrite the AP's output power, radio or SSID profile settings for the specified radio. Use the no command to not overwrite the specified settings.
`[no] override lan-provision`	Sets the ZyWALL / USG to overwrite the AP's LAN port settings. Use the no command to not overwrite the specified settings.
`[no] override vlan-setting`	Sets the ZyWALL / USG to overwrite the AP's LAN port settings. Use the no command to not overwrite the specified settings.
`ap-group-profile` *`wlan_profile`*	Sets the AP group to which the AP belongs.
`cw_slot_name_ac` `output-power` *`wlan_power`*	Sets the output power (between 0 to 30 dBm) for the radio on the built-in AP that belongs to this group.
`capwap ap` *`ap_mac`*	Enters sub-command mode for the specified external AP.
`cw_slot_name_ac` `output-power` *`wlan_power`*	Sets the output power (between 0 to 30 dBm) for the radio on the the specified AP (*ap_mac*) that belongs to this group.
`[no]` *`slot_name`* `ap-profile` *`profile_name`*	Sets the radio (*slot_name*) to AP mode and assigns a created profile to the radio. Use the no command to remove the AP mode profile assignment for the specified radio (*slot_name*).
`[no]` *`slot_name`* `monitor-profile` *`profile_name`*	Sets the specified radio (*slot_name*) to monitor mode and assigns a created profile to the radio. Monitor mode APs act as wireless monitors, which can detect rogue APs and help you in building a list of friendly ones. See also Section 8.2 on page 67. Use the no command to remove the monitor mode profile assignment for the specified radio (*slot_name*).
`ap-group-profile` *`ap-group-profile_name`*	Sets the AP group to which the AP belongs.
`description` *`ap_description`*	Sets the description for the specified AP.

Table 10 Command Summary: AP Management (continued)

COMMAND	DESCRIPTION
[no] force vlan	Sets whether or not the ZyWALL / USG changes the AP's management VLAN to match the one you configure using the vlan sub-command. The management VLAN on the ZyWALL / USG and AP must match for the ZyWALL / USG to manage the AP.
lan-provision *lan_port* {activate | inactivate} pvid <1..4094>	Sets the ZyWALL / USG to enable or disable the specified LAN port on the AP and configures a PVID (Port VLAN ID) for this port. *lan_port*: the name of the AP's LAN port (lan1 for example).
lan-provision *vlan_interface* {activate | inactivate} vid <1..4094> join *lan_port* {tag | untag} [*lan_port* {tag | untag}] [*lan_port* {tag | untag}]	Sets the ZyWALL / USG to create a new VLAN or configure an existing VLAN. You can disable or enable the VLAN, set the VLAN ID, assign up to three ports to this VLAN as members and set whether the port is to tag outgoing traffic with the VLAN ID. *vlan_interface*: the name of the VLAN (vlan1 for example).
[no] override *slot_name* {output-power | radio-setting | ssid-setting}	Sets the ZyWALL / USG to overwrite the AP's output power, radio or SSID profile settings for the specified radio. Use the no command to not overwrite the specified settings.
[no] override lan-provision	Sets the ZyWALL / USG to overwrite the AP's LAN port settings. Use the no command to not overwrite the specified settings.
[no] override vlan-setting	Sets the ZyWALL / USG to overwrite the AP's LAN port settings. Use the no command to not overwrite the specified settings.
vlan <1..4094> {tag | untag}	Sets the VLAN ID for the specified AP as well as whether packets sent to and from that ID are tagged or untagged.
exit	Exits the sub-command mode for the specified AP.
capwap ap ac-ip *{primary_ac_ip} {secondary_ac_ip}*	Specifies the primary and secondary IP address or domain name of the AP controller (the ZyWALL / USG) to which the AP connects.
capwap ap ac-ip auto	Sets the AP to use DHCP to get the address of the AP controller (the ZyWALL / USG).
capwap ap fallback disable	Sets the managed AP(s) to not change back to associate with the primary AP controller when the primary AP controller is available.
capwap ap fallback enable	Sets the managed AP(s) to change back to associate with the primary AP controller as soon as the primary AP controller is available.
capwap ap fallback interval <30..86400>	Sets how often (in seconds) the managed AP(s) check whether the primary AP controller is available.
capwap ap led-off *ap_mac*	Sets the LEDs of the specified AP to turn off after it's ready.
capwap ap led-on *ap_mac*	Sets the LEDs of the specified AP to stay lit after the ZyWALL / USG is ready.
country-code *country_code*	Sets the country where the ZyWALL / USG is located/installed. This is the default country code the ZyWALL / USG uses in a new radio profile or monitor profile if you do not change it. The available channels vary depending on the country you selected. *country_code*: 2-letter country-codes, such as TW, DE, or FR.
lan-provision ap *ap_mac*	Enters the sub-command mode for the specified AP
lan_port {activate | inactivate} pvid <1..4094>	Enables or disables the specified LAN port on the AP and configures a PVID (Port VLAN ID) for this port. *lan_port*: the name of the AP's LAN port (lan1 for example).

Table 10 Command Summary: AP Management (continued)

COMMAND	DESCRIPTION
`*vlan_interface* {activate | inactivate} vid <1..4094> join *lan_port* {tag | untag} [*lan_port* {tag | untag}] [*lan_port* {tag | untag}]`	Creates a new VLAN or configures an existing VLAN. You can disable or enable the VLAN, set the VLAN ID, assign up to three ports to this VLAN as members and set whether the port is to tag outgoing traffic with the VLAN ID. *vlan_interface*: the name of the VLAN (vlan1 for example).
[no] *vlan_interface*	Removes the specified VLAN.
capwap manual-add {enable | disable}	Allows the ZyWALL / USG to either automatically add new APs to the network (*disable*) or wait until you manually confirm them (*enable*).
capwap show statistic	Displays statistics about the wireless radio transmitters in each of the APs connected to the ZyWALL / USG.
capwap station kick *sta_mac*	Forcibly disconnects the specified station from the network.
capwap firmware-update check	Displays the latest AP firmware version available on the firmware server.
capwap firmware-update apply	Downloads newer firmware from the firmware server.
capwap fw-updating method {capwap | ftp}	Specifies how you want the ZyWALL / USG to upgrade AP firmware: CAPWAP or FTP.
default country-code *two_alphabet_country_code*	Sets the default country code that represents countries for use in newly created radio/monitor profiles. Use show country-code list to see the codes that represent countries.
show capwap ap firmware	Displays the current AP firmware version on the ZyWALL / USG. The ZyWALL / USG must have the latest AP firmware to manage all supported APs.
show capwap firmware-update info	Displays if there is a later AP firmware version available on the firmware server.
show capwap firmware-update releasenote-url	Displays the release notes for a later AP firmware version available on the firmware server.
show capwap ap wait-list	Displays a list of connected but as-of-yet unmanaged APs. This is known as the 'wait list'.
show capwap ap *ap_mac slot_name* detail	Displays details for the specified radio (*slot_name*) on the specified AP (*ap_mac*).
show capwap ap {all | *ap_mac*}	Displays the management list (*all*) or whether the specified AP is on the management list (*ap_mac*).
show capwap ap {all | *ap_mac*} config status	Displays whether or not any AP's configuration or the specified AP's configuration is in conflict with the ZyWALL / USG's settings for the AP and displays the settings in conflict if there are any.
show capwap ap ac-ip	Displays the address of the ZyWALL / USG or auto if the AP finds the ZyWALL / USG through broadcast packets.
show capwap ap all statistics	Displays radio statistics for all APs on the management list.
show capwap ap fallback	Displays whether the managed AP(s) will change back to associate with the primary AP controller when the primary AP controller is available.
show capwap ap fallback interval	Displays the interval for how often the managed AP(s) check whether the primary AP controller is available.
show country-code list	Displays a reference list of two-letter country codes.
show default country-code	Displays the default country code configured on the ZyWALL / USG.

Table 10 Command Summary: AP Management (continued)

COMMAND	DESCRIPTION
show lan-provision ap *ap_mac* interface {*lan_port* | *vlan_interface* | all| ethernet | uplink | vlan}	Displays the port and/or VLAN settings for the specified AP. You can also set to display settings for a specified port, a sepcified VLAN, all physical Ethernet ports, the uplink port or all VLANs on the AP.
show capwap manual-add	Displays the current manual add option.
show capwap station all	Displays information for all stations connected to the APs on the management list.

6.2.1 AP Management Commands Example

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

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

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

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

7

AP Group

This chapter shows you how to configure AP groups, which define the radio, port, VLAN and load balancing settings and apply the settings to all APs in the group. An AP can belong to one AP group at a time.

7.1 Wireless Load Balancing Overview

Wireless load balancing is the process whereby you limit the number of connections allowed on an wireless access point (AP) or you limit the amount of wireless traffic transmitted and received on it. Because there is a hard upper limit on the AP's wireless bandwidth, this can be a crucial function in areas crowded with wireless users. Rather than let every user connect and subsequently dilute the available bandwidth to the point where each connecting device receives a meager trickle, the load balanced AP instead limits the incoming connections as a means to maintain bandwidth integrity.

7.2 AP Group Commands

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

Table 11 Input Values for General AP Management Commands

LABEL	DESCRIPTION
`ap_group_profile_name`	The wireless LAN radio profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`slot_name`	The slot name for the AP's on-board wireless LAN card. Use either `slot1` or `slot2`. (The NWA5560-N supports up to 2 radio slots.)

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

Table 12 Command Summary: AP Group

COMMAND	DESCRIPTION
`ap-group first-priority ap_group_profile_name`	Sets an AP group file that is used as the default group file. Any AP that is not configured to associate with a specific AP group belongs to the default group automatically.
`ap-group flush wtp-setting ap_group_profile_name`	Sets the ZyWALL / USG to overwrite the settings of all managed APs in the specified group with the group profile settings.

Table 12 Command Summary: AP Group (continued)

COMMAND	DESCRIPTION
ap-group-member *ap_group_wlan_name*[no] member local-ap	Specifies the SSID of the built-in AP that you want to apply the specified AP group profile and add to the group. Use the no command to remove the built-in AP from this group.
ap-group-member *ap_group_profile_name* [no] member *mac_address*	Specifies the MAC address of the AP that you want to apply the specified AP group profile and add to the group. Use the no command to remove the specified AP from this group.
[no] ap-group-profile *ap_group_profile_name*	Enters configuration mode for the specified AP group profile. Use the no command to remove the specified profile.
[no] *slot_name* ap-profile *radio_profile_name*	Sets the specified radio to work as an AP and specifies the radio profile the radio is to use. Use the no command to remove the specified profile.
[no] *slot_name* monitor-profile *monitor_profile_name*	Sets the specified radio to work in monitor mode and specifies the monitor profile the radio is to use. Use the no command to remove the specified profile.
[no] *slot_name* output-power *wlan_power*	Sets the output power (between 0 to 30 dBm) for the radio on the AP that belongs to this group. Use the no command to remove the output power setting.
[no] *slot_name* ssid-profile <1..8> *ssid_profile_name*	Sets the SSID profile that is associated with this profile. You can associate up to eight SSID profiles with an AP radio. Use the no command to remove the specified profile.
description *description*	Sets a description for this group. You can use up to 31 characters, spaces and underscores allowed. Use the no command to remove the specified description.
exit	Exits configuration mode for this profile.
[no] force vlan	Sets the ZyWALL / USG to change the AP's management VLAN to match the configuration in this profile. Use the no command to not change the AP's management VLAN setting.
[no] lan-provision model {nwa5301-nj | wac6502d-e | wac6502d-s | wac6503d-s | wac6553d-e} *ap_lan_port* activate pvid <1..4094>	Sets the model of the managed AP and enable the model-specific LAN port and configure the port VLAN ID. Use the no command to remove the specified port and VLAN settings. *ap_lan_port*: the Ethenet LAN port on the managed AP, such as lan1 or lan2.
[no] lan-provision model {nwa5301-nj | wac6502d-e | wac6502d-s | wac6503d-s | wac6553d-e} *ap_lan_port* inactivate pvid <1..4094>	Sets the model of the managed AP and disable the model-specific LAN port and configure the port VLAN ID. Use the no command to remove the specified port and VLAN settings. *ap_lan_port*: the Ethenet LAN port on the managed AP, such as lan1 or lan2.

Table 12 Command Summary: AP Group (continued)

COMMAND	DESCRIPTION
`[no] lan-provision model {nwa5301-nj | wac6502d-e | wac6502d-s | wac6503d-s | wac6553d-e} vlan_interface activate vid <1..4094> join ap_lan_port {tag | untag} [ap_lan_port {tag | untag}] [ap_lan_port {tag | untag}]`	Sets the model of the managed AP, enable a VLAN and configure the VLAN ID. It also sets the Ethernet port(s) on the managed AP to be a member of the VLAN, and sets the port(s) to send packets with or without a VLAN tag. Use the no command to remove the specified port and VLAN settings. *vlan_interface*: the name of the VLAN, such as vlan0. *ap_lan_port*: the Ethenet LAN port on the managed AP, such as lan1 or lan2.
`[no] lan-provision model {nwa5301-nj | wac6502d-e | wac6502d-s | wac6503d-s | wac6553d-e} vlan_interface inactivate vid <1..4094> join ap_lan_port {tag | untag} [ap_lan_port {tag | untag}] [ap_lan_port {tag | untag}]`	Sets the model of the managed AP, disable a VLAN and configure the VLAN ID. It also sets the Ethernet port(s) on the managed AP to be a member of the VLAN, and sets the port(s) to send packets with or without a VLAN tag. Use the no command to remove the specified port and VLAN settings. *vlan_interface*: the name of the VLAN, such as vlan0. *ap_lan_port*: the Ethenet LAN port on the managed AP, such as lan1 or lan2.
`[no] load-balancing activate`	Enables load balancing. Use the no parameter to disable it.
`load-balancing alpha <1..255>`	Sets the load balancing alpha value. When the AP is balanced, then this setting delays a client's association with it by this number of seconds. Note: This parameter has been optimized for the ZyWALL / USG and should not be changed unless you have been specifically directed to do so by ZyXEL support.
`load-balancing beta <1..255>`	Sets the load balancing beta value. When the AP is overloaded, then this setting delays a client's association with it by this number of seconds. Note: This parameter has been optimized for the ZyWALL / USG and should not be changed unless you have been specifically directed to do so by ZyXEL support.
`load-balancing kickInterval <1..255>`	Enables the kickout feature for load balancing and also sets the kickout interval in seconds. While load balancing is enabled, the AP periodically disconnects stations at intervals equal to this setting. This occurs until the load balancing threshold is no longer exceeded.
`[no] load-balancing kickout`	Enables an overloaded AP to disconnect ("kick") idle clients or clients with noticeably weak connections.

Table 12 Command Summary: AP Group (continued)

COMMAND	DESCRIPTION
`load-balancing liInterval <1..255>`	Sets the interval in seconds that each AP communicates with the other APs in its range for calculating the load balancing algorithm. Note: This parameter has been optimized for the ZyWALL / USG and should not be changed unless you have been specifically directed to do so by ZyXEL support.
`load-balancing max sta <1..127>`	If load balancing by the number of stations/wireless clients, this sets the maximum number of devices allowed to connect to a load-balanced AP.
`load-balancing mode {station | traffic | smart-classroom}`	Enables load balancing based on either number of stations (also known as wireless clients) or wireless traffic on an AP. station or traffic: once the threshold is crossed (either the maximum station numbers or with network traffic), the AP delays association request and authentication request packets from any new station that attempts to make a connection. smart-classroom: the AP ignores association request and authentication request packets from any new station when the maximum number of stations is reached.
`load-balancing sigma <51..100>`	Sets the load balancing sigma value. This value is algorithm parameter used to calculate whether an AP is considered overloaded, balanced, or underloaded. It only applies to ‘by traffic mode’. Note: This parameter has been optimized for the ZyWALL / USG and should not be changed unless you have been specifically directed to do so by ZyXEL support.
`load-balancing timeout <1..255>`	Sets the length of time that an AP retains load balancing information it receives from other APs within its range.
`load-balancing traffic level {high | low | medium}`	If load balancing by traffic threshold, this sets the traffic threshold level.
`vlan <1..4094> {tag | untag}`	Sets the management VLAN ID for the AP(s) in this group as well as whether packets sent to and from that VLAN ID are tagged or untagged.
`show ap-group first-priority`	Displays the name of the default AP group profile.
`show ap-group-profile {all |` *`ap_group_profile_name`*`}`	Displays the settings of the AP group profile(s). `all`: Displays all profiles. *`ap_group_profile_name`*: Displays the specified profile.
`show ap-group-profile rule_count`	Displays how many AP group profiles have been configured on the ZyWALL / USG.
`show ap-group-profile` *`ap_group_profile_name`* `load-balancing config`	Displays the load balancing configuration of the specified AP group profile.

Table 12 Command Summary: AP Group (continued)

COMMAND	DESCRIPTION
show ap-group-profile *ap_group_profile_name* lan-provision model {nwa5301-nj | wac6502d-e | wac6502d-s | wac6503d-s | wac6553d-e} interface {all | vlan | ethernet | *ap_lan_port* | *vlan_interface*}	Displays the LAN port and/or VLAN settings on the managed AP which is in the specified AP group and of the specified model. *vlan_interface*: the name of the VLAN, such as vlan0. *ap_ lan_port*: the Ethenet LAN port on the managed AP, such as lan1 or lan2.
show ap-group-profile *ap_group_profile_name* load-balancing config	Displays the load balancing configuration of the specified AP group profile.
show ap-group-profile ap_group_profile_name lan-provision model	Shows the model name of the managed AP which belongs to the specified AP group.
show ap-group-profile *ap_group_profile_name* model	Shows the model name of the managed AP which belongs to the specified AP group.
show ap-group-profile rule_count	Displays how many AP group profiles have been configured on the ZyWALL / USG.
ap-group-profile rename *ap_group_profile_name1* *ap_group_profile_name2*	Gives an existing AP group profile (*ap_group_profile_name1*) a new name (*ap_group_profile_name2*).

7.2.1 AP Group Examples

The following example shows you how to create an AP group profile (named “TEST”) and configure the AP’s first radio to work in repeater mode using the “default” radio profile and the “ZyMesh_TEST” ZyMesh profile. It also adds the AP with the MAC address 00:a0:c5:01:23:45 to this AP group.

```
Router(config)# ap-group-profile TEST
Router(config-ap-group TEST)# slot1 repeater-ap default
Router(config-ap-group TEST)# exit
Router(config)# ap-group-member TEST member 00:a0:c5:01:23:45
Router(config)#
```

The following example shows you how to create an AP group profile (named GP1) and configure AP load balancing in "by station" mode. The maximum number of stations is set to 1.

```
Router(config)# ap-group-profile GP1
Router(config-ap-group GP1)# load-balancing mode station
Router(config-ap-group GP1)# load-balancing max sta 1
Router(config-ap-group GP1)# exit
Router(config)# show ap-group-profile GP1 load-balancing config
AP Group Profile:GP1
load balancing config:
Activate: yes
Kickout: no
Mode: station
Max-sta: 1
Traffic-level: high
Alpha: 5
Beta: 10
Sigma: 60
Timeout: 20
LIInterval: 10
KickoutInterval: 20
Router(config)#
```

The following example shows you how to create an AP group profile (named GP2) and configure AP load balancing in "by traffic" mode. The traffic level is set to low, and "disassociate station" is enabled.

```
Router(config)# ap-group-profile GP2
Router(config-ap-group GP2)# load-balancing mode traffic
Router(config-ap-group GP2)# load-balancing traffic level low
Router(config-ap-group GP2)# load-balancing kickout
Router(config-ap-group GP2)# exit
Router(config)# show ap-group-profile GP2 load-balancing config
AP Group Profile:GP2
load balancing config:
Activate: yes
Kickout: yes
Mode: traffic
Max-sta: 1
Traffic-level: low
Alpha: 5
Beta: 10
Sigma: 60
Timeout: 20
LIInterval: 10
KickoutInterval: 20
Router(config)#
```

The following example shows the settings and status of the VLAN(s) configured for the managed APs (NWA5301-NJ) in the default AP group.

```
Router(config)# show ap-group-profile default lan-provision model nwa5301-nj
interface vlan
No. Name            Active VID   Member
============================================================================
1   vlan0           yes    1     lan1,lan2,lan3
Router(config)# show ap-group-profile default lan-provision model nwa5301-nj
interface vlan0
active: yes
interface name: vlan0
VID: 1
member: lan1&lan2&lan3
lan1_tag: untag
lan2_tag: untag
lan3_tag: untag
Router(config)#
```

The following example shows the status of Ethernet ports for the managed APs (NWA5301-NJ) in the default AP group. It also shows whether the lan1 port is enabled and what the port’s VLAN ID is.

```
Router(config)# show ap-group-profile default lan-provision model nwa5301-nj
interface ethernet
No. Name            Active PVID
============================================================================
1   uplink          yes    n/a
2   lan1            yes    1
3   lan2            yes    1
4   lan3            yes    1
Router(config)# show ap-group-profile default lan-provision model nwa5301-nj
interface lan1
Name            Active PVID
============================================================================
lan1            yes    1
Router(config)#
```

Wireless LAN Profiles

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

8.1 Wireless LAN Profiles Overview

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

8.2 AP Radio Profile Commands

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

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

Table 13 Input Values for General Radio and Monitor Profile Commands

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

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

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

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

Table 14 Command Summary: Radio Profile

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

Table 14 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
`country-code` *`country_code`*	Sets the country where the ZyWALL / USG is located/installed. The available channels vary depending on the country you selected. Be sure to select the correct/same country for both radios on an AP and all connected APs, in order to prevent roaming failure and interference to other systems. *`country_code`*: 2-letter country-codes, such as TW, DE, or FR.
`[no] dcs activate`	Starts dynamic channel selection. Use the no parameter to turn it off.
`dcs 2g-selected-channel` *`2.4g_channels`*	Sets the channels that are available in the 2.4 GHz band when you manually configure the channels an AP can use.
`dcs dcs-2g-method {auto|manual}`	Sets the AP to automatically search for available channels or manually configures the channels the AP uses in the 2.4 GHz band.
`dcs dcs-5g-method {auto}`	Sets the AP to automatically search for available channels.
`dcs client-aware {enable|disable}`	When enabled, this ensures that an AP will not change channels as long as a client is connected to it. If disabled, the AP may change channels regardless of whether it has clients connected to it or not.
`dcs channel-deployment {3-channel|4-channel}`	Sets either a 3-channel deployment or a 4-channel deployment. In a 3-channel deployment, the AP running the scan alternates between the following channels: 1, 6, and 11. In a 4-channel deployment, the AP running the scan alternates between the following channels: 1, 4, 7, and 11 (FCC) or 1, 5, 9, and 13 (ETSI). Sets the option that is applicable to your region. (Channel deployment may be regulated differently between countries and locales.)
`dcs dfs-aware {enable|disable}`	Enables this to allow an AP to avoid phase DFS channels below the 5 GHz spectrum.
`dcs sensitivity-level {high| medium |low}`	Sets how sensitive DCS is to radio channel changes in the vicinity of the AP running the scan.
`dcs time-interval` *`interval`*	Sets the interval that specifies how often DCS should run.
`[no] disable-dfs-switch`	Makes the DFS switch active or inactive. By default this is inactive.
`[no] dot11n-disable-coexistence`	Fixes the channel bandwidth as 40 MHz. The no command has the AP automatically choose 40 MHz if all the clients support it or 20 MHz if some clients only support 20 MHz.
`[no] ctsrts <0..2347>`	Sets or removes the RTS/CTS value for this profile. Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions). A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off. The default is 2347.

Table 14 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
`[no] frag <256..2346>`	Sets or removes the fragmentation value for this profile. The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. The default is 2346.
`dtim-period <1..255>`	Sets the DTIM period for this profile. Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255. The default is 1.
`beacon-interval <40..1000>`	Sets the beacon interval for this profile. When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. This value can be set from 40ms to 1000ms. A high value helps save current consumption of the access point. The default is 100.
`[no] ampdu`	Activates MPDU frame aggregation for this profile. Use the *no* parameter to disable it. Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates. By default this is enabled.
`limit-ampdu <100..65535>`	Sets the maximum frame size to be aggregated. By default this is 50000.
`subframe-ampdu <2..64>`	Sets the maximum number of frames to be aggregated each time. By default this is 32.
`[no] amsdu`	Activates MPDU frame aggregation for this profile. Use the *no* parameter to disable it. Mac Service Data Unit (MSDU) aggregation collects Ethernet frames without any of their 802.11n headers and wraps the header-less payload in a single 802.11n MAC header. This method is useful for increasing bandwidth throughput. It is also more efficient than A-MPDU except in environments that are prone to high error rates. By default this is enabled.
`limit-amsdu <2290..4096>`	Sets the maximum frame size to be aggregated. The default is 4096.

Table 14 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
`[no] multicast-to-unicast`	"Multicast to unicast" broadcasts wireless multicast traffic to all wireless clients as unicast traffic to provide more reliable transmission. The data rate changes dynamically based on the application's bandwidth requirements. Although unicast provides more reliable transmission of the multicast traffic, it also produces duplicate packets. The no command turns multicast to unicast off to send wireless multicast traffic at the rate you specify with the `2g-multicast-speed` or `5g-multicast-speed` command.
`[no] block-ack`	Makes `block-ack` active or inactive. Use the *no* parameter to disable it.
`ch-width` *`wlan_htcw`*	Sets the channel width for this profile.
`guard-interval` *`wlan_htgi`*	Sets the guard interval for this profile. The default for this is *`short`*.
`2g-basic-speed` *`wlan_2g_basic_speed`*	Sets the 2.4 GHz basic band rates. The default is 1.0 2.0 5.5 11.0.
`2g-channel` *`wireless_channel_2g`*	Sets the broadcast band for this profile in the 2.4 GHz frequency range. The default is 6.
`2g-mcs-speed {disable |` *`wlan_mcs_speed`*`}`	Disables or sets the 2.4 GHz HT MCS rate. The default is 0~15.
`2g-multicast-speed` *`wlan_2g_support_speed`*	When you disable multicast to unicast, use this command to set the data rate `{ 1.0 | 2.0 | … }` in Mbps for 2.4 GHz multicast traffic.
`2g-support-speed {disable |` *`wlan_2g_support_speed`*`}`	Disables or sets the 2.4 GHz support rate. The default is 1.0~54.0.
`5g-basic-speed` *`wlan_5g_basic_speed`*	Sets the 5 GHz basic band rate. The default is 6.0 12.0 24.0.
`5g-channel` *`wireless_channel_5g`*	Sets the broadcast band for this profile in the 5 GHz frequency range. The default is 36.
`5g-mcs-speed {disable |` *`wlan_mcs_speed`*`}`	Disables or sets the 5 GHz HT MCS rate. The default is 0~15.
`5g-multicast-speed {`*`wlan_5g_basic_speed`*`}`	When you disable multicast to unicast, use this command to set the data rate `{ 6.0 | 9.0 | … }` in Mbps for 5 GHz multicast traffic.
`5g-support-speed {disable |` *`wlan_5g_support_speed`*`}`	Disables or sets the 5 GHz support rate. The default is 6.0~54.0.
`tx-mask` *`chain_mask`*	Sets the outgoing chain mask rate.
`rx-mask` *`chain_mask`*	Sets the incoming chain mask rate.
`[no] htprotection`	Activates HT protection for this profile. Use the *no* parameter to disable it. By default, this is disabled.
`output-power` *`wlan_power`*	Sets the output power for the radio in this profile. The default is 100%.

Table 14 Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
`[no] ssid-profile` *`wlan_interface_index ssid_profile`*	Assigns an SSID profile to this radio profile. Requires an existing SSID profile. Use the no parameter to disable it.
`exit`	Exits configuration mode for this profile.

8.2.1 AP Profile Commands Example

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

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

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

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

8.3 AP Monitor Profile Commands

The monitor profile commands allow you to set up monitor mode configurations that allow your APs to scan for other APs in the vicinity.

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 Monitor Profile Commands

LABEL	DESCRIPTION
monitor_profile_name	The monitor 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.
wireless_channel_2g	Sets the 2 GHz channel used by the profile. The channel range is `1 - 14`. Note: Your choice of channel may be restricted by regional regulations.
wireless_channel_5g	Sets the 5 GHz channel used by the profile. The channel range is `36 - 165`. Note: Your choice of channel may be restricted by regional regulations.

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

Table 16 Command Summary: Monitor Profile

COMMAND	DESCRIPTION
`show wlan-monitor-profile {all | monitor_profile_name}`	Displays all monitor profiles or just the specified one.
`wlan-monitor-profile rename monitor_profile_name1 monitor_profile_name2`	Gives an existing monitor profile (*monitor_profile_name1*) a new name (*monitor_profile_name2*).
`[no] wlan-monitor-profile monitor_profile_name`	Enters configuration mode for the specified monitor profile. Use the *no* parameter to remove the specified profile.
`[no] activate`	Makes this profile active or inactive. By default, this is enabled.
`country-code country_code`	Sets the country where the ZyWALL / USG is located/installed. The available channels vary depending on the country you selected. Be sure to select the correct/same country for both radios on an AP and all connected APs, in order to prevent roaming failure and interference to other systems. *country_code*: 2-letter country-codes, such as TW, DE, or FR.
`description description`	Sets the description for the profile. You may use up to 60 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive
`[no] 2g-scan-channel wireless_channel_2g`	Sets the broadcast band for this profile in the 2.4 Ghz frequency range. Use the *no* parameter to disable it.
`[no] 5g-scan-channel wireless_channel_5g`	Sets the broadcast band for this profile in the 5 GHz frequency range. Use the *no* parameter to disable it.
`scan-method scan_method`	Sets the channel scanning method for this profile.

Table 16 Command Summary: Monitor Profile (continued)

COMMAND	DESCRIPTION
`scan-dwell <100..1000>`	Sets the duration in milliseconds that the device using this profile scans each channel.
`exit`	Exits configuration mode for this profile.

8.4 SSID Profile Commands

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

Table 17 Input Values for General SSID Profile Commands

LABEL	DESCRIPTION
ssid_profile_name	The SSID profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
ssid	The SSID broadcast name. You may use 1-32 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive.
wlan_qos	Sets the type of QoS the SSID should use. *disable*: Turns off QoS for this SSID. *wmm*: Turns on QoS for this SSID. It automatically assigns Access Categories to packets as the device inspects them in transit. *wmm_be*: Assigns the “best effort” Access Category to all traffic moving through the SSID regardless of origin. *wmm_bk*: Assigns the “background” Access Category to all traffic moving through the SSID regardless of origin. *wmm_vi*: Assigns the “video” Access Category to all traffic moving through the SSID regardless of origin. *wmm_vo*: Assigns the “voice” Access Category to all traffic moving through the SSID regardless of origin.
vlan_iface	The VLAN interface name of the controller (in this case, it is NXC5200). The maximum VLAN interface number is product-specific; for the ZyWALL / USG, the number is 512.
securityprofile	Assigns an existing security profile to the SSID profile. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
macfilterprofile	Assigns an existing MAC filter profile to the SSID profile. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
description2	Sets the description of the profile. You may use up to 60 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive.

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

Table 18 Command Summary: SSID Profile

COMMAND	DESCRIPTION
`show wlan-ssid-profile {all | ssid_profile_name}`	Displays the SSID profile(s). `all`: Displays all profiles for the selected operating mode. *`ssid_profile_name`*: Displays the specified profile for the selected operating mode.
`wlan-ssid-profile rename ssid_profile_name1 ssid_profile_name2`	Gives an existing SSID profile (*`ssid_profile_name1`*) a new name (*`ssid_profile_name2`*).
`[no] wlan-ssid-profile ssid_profile_name`	Enters configuration mode for the specified SSID profile. Use the *no* parameter to remove the specified profile.
`bandselect check-sta-interval <1..60000>`	Sets how often (in seconds) the AP checks and deletes old wireless client data.
`bandselect drop-authentication <1..16>`	Sets how many authentication request from a client to a 2.4GHz Wi-Fi network is ignored during the specified timeout period.
`bandselect drop-probe-request <1..32>`	Sets how many prob request from a client to a 2.4GHz Wi-Fi network is ignored during the specified timeout period.
`bandselect min-sort-interval <1..60000>`	Sets the minimum interval (in seconds) at which the AP sorts the wireless client data when the client queue is full.
`bandselect mode {disable | force | standard}`	To improve network performance and avoid interference in the 2.4 GHz frequency band, you can enable this feature to use the 5 GHz band first. You should set 2.4GHz and 5 GHz radio profiles to use the same SSID and security settings. Note: The managed APs must be dual-band capable. `disable`: to turn off this feature. `force`: to have the wireless clients always connect to an SSID using the 5 GHZ band. Connections to an SSID using the 2.4GHz band are not allowed. It is recommanded you select this option when the AP and wireless clients can function in either frequency band. `standard`: to have the AP try to connect the wireless clients to the same SSID using the 5 GHZ band. Connections to an SSID using the 2.4GHz band are still allowed.
`bandselect time-out-period <1..256>`	Sets the timeout period (in seconds) within which the AP drops the specified number of prob or authentication requests to a 2.4GHz Wi-Fi network.
`bandselect time-out-standard <1..255>`	Sets the timeout period (in seconds) within which the AP accepts probe or authentication requests to a 2.4GHz Wi-Fi network when the band select mode is set to `standard`.
`[no] block-intra`	Enables intra-BSSID traffic blocking. Use the no parameter to disable it in this profile. By default this is disabled.
`downlink-rate-limit data_rate`	Sets the maximum incoming transmission data rate (either in mbps or kbps) on a per-station basis.

Table 18 Command Summary: SSID Profile (continued)

COMMAND	DESCRIPTION
[no] hide	Prevents the SSID from being publicly broadcast. Use the no parameter to re-enable public broadcast of the SSID in this profile. By default this is disabled.
[no] macfilter *macfilterprofile*	Assigns the specified MAC filtering profile to this SSID profile. Use the no parameter to remove it. By default, no MAC filter is assigned.
qos *wlan_qos*	Sets the type of QoS used by this SSID.
security *securityprofile*	Assigns the specified security profile to this SSID profile.
ssid	Sets the SSID. This is the name visible on the network to wireless clients. Enter up to 32 characters, spaces and underscores are allowed. The default SSID is 'ZyXEL'.
uplink-rate-limit *data_rate*	Sets the maximum outgoing transmission data rate (either in mbps or kbps) on a per-station basis.
vlan-id <1..4094>	Applies to each SSID profile that uses localbridge. If the VLAN ID is equal to the AP's native VLAN ID then traffic originating from the SSID is not tagged. The default VLAN ID is 1.
[no] vlan-support	Sets the ZyWALL / USG to tag traffic from the local Virtual AP (VAP) with the VLAN ID specified in this SSID profile. The no command sets the ZyWALL / USG to not tag traffic from the local Virtual AP (VAP) with the VLAN ID.
exit	Exits configuration mode for this profile.

8.4.1 SSID Profile Example

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

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

8.5 Security Profile Commands

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

Table 19 Input Values for General Security Profile Commands

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

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

Table 20 Command Summary: Security Profile

COMMAND	DESCRIPTION
show wlan-security-profile {all | *security_profile_name*}	Displays the security profile(s). *all*: Displays all profiles for the selected operating mode. *security_profile_name*: Displays the specified profile for the selected operating mode.
wlan-security-profile rename *security_profile_name1 security_profile_name2*	Gives existing security profile (*security_profile_name1*) a new name, (*security_profile_name2*).
[no] wlan-security-profile *security_profile_name*	Enters configuration mode for the specified security profile. Use the *no* parameter to remove the specified profile.
[no] dot11w	Data frames in 802.11 WLANs can be encrypted and authenticated with WEP, WPA or WPA2. But 802.11 management frames, such as beacon/probe response, association request, association response, de-authentication and disassociation are always unauthenticated and unencrypted. IEEE 802.11w Protected Management Frames allows APs to use the existing security mechanisms (encryption and authentication methods defined in IEEE 802.11i WPA/WPA2) to protect management frames. This helps prevent wireless DoS attacks. Enables management frame protection (MFP) to add security to 802.11 management frames. Use the no parameter to disable it.
dot11w-op <1..2>	Sets whether wireless clients have to support management frame protection in order to access the wireless network. 1: if you do not require the wireless clients to support MFP. Management frames will be encrypted if the clients support MFP. 2: wireless clients must support MFP in order to join the AP's wireless network.
mode {none | wep | wpa | wpa2 | wpa2-mix}	Sets the security mode for this profile.

Table 20 Command Summary: Security Profile (continued)

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

8.5.1 Security Profile Example

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

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

8.6 MAC Filter Profile Commands

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

Table 21 Input Values for General MAC Filter Profile Commands

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

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

Table 22 Command Summary: MAC Filter Profile

COMMAND	DESCRIPTION
`show wlan-macfilter-profile {all | macfilter_profile_name}`	Displays the security profile(s). `all`: Displays all profiles for the selected operating mode. *macfilter_profile_name*: Displays the specified profile for the selected operating mode.
`wlan-macfilter-profile rename` *macfilter_profile_name1 macfilter_profile_name2*	Gives an existing security profile (*macfilter_profile_name1*) a new name (*macfilter_profile_name2*).
`[no] wlan-macfilter-profile` *macfilter_profile_name*	Enters configuration mode for the specified MAC filter profile. Use the *no* parameter to remove the specified profile.
`filter-action {allow | deny}`	Permits the wireless client with the MAC addresses in this profile to connect to the network through the associated SSID; select deny to block the wireless clients with the specified MAC addresses. The default is set to *deny*.
`[no] MAC description` *description2*	Sets the MAC address (with optional description) to which this profile applies.
`exit`	Exits configuration mode for this profile.

8.6.1 MAC Filter Profile Example

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

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

Rogue AP

This chapter shows you how to set up Rogue Access Point (AP) detection and containment.

9.1 Rogue AP Detection Overview

Rogue APs are wireless access points operating in a network's coverage area that are not under the control of the network's administrators, and can potentially open holes in the network security. Attackers can take advantage of a rogue AP's weaker (or non-existent) security to gain illicit access to the network, or set up their own rogue APs in order to capture information from wireless clients.

Conversely, a friendly AP is one that the ZyWALL / USG network administrator regards as non-threatening. This does not necessarily mean the friendly AP must belong to the network managed by the ZyWALL / USG; rather, it is any unmanaged AP within range of the ZyWALL / USG's own wireless network that is allowed to operate without being contained. This can include APs from neighboring companies, for example, or even APs maintained by your company's employees that operate outside of the established network.

9.2 Rogue AP Detection Commands

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

Table 23 Input Values for Rogue AP Detection Commands

LABEL	DESCRIPTION
ap_mac	Specifies the MAC address (in XX:XX:XX:XX:XX:XX format) of the AP to be added to either the rogue AP or friendly AP list. The no command removes the entry.
description2	Sets the description of the AP. You may use 1-60 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive.

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

Table 24 Command Summary: Rogue AP Detection

COMMAND	DESCRIPTION
`rogue-ap detection`	Enters sub-command mode for rogue AP detection.
`    [no] activate`	Activates rogue AP detection. Use the no parameter to deactivate rogue AP detection.

Table 24 Command Summary: Rogue AP Detection (continued)

COMMAND	DESCRIPTION
rogue-ap *ap_mac description2*	Sets the device that owns the specified MAC address as a rogue AP. You can also assign a description to this entry on the rogue AP list.
no rogue-ap *ap_mac*	Removes the device that owns the specified MAC address from the rogue AP list.
friendly-ap *ap_mac description2*	Sets the device that owns the specified MAC address as a friendly AP. You can also assign a description to this entry on the friendly AP list.
no friendly-ap *ap_mac*	Removes the device that owns the specified MAC address from the friendly AP list.
monitoring flush	Removes all detected APs from the rogue AP list.
exit	Exits configuration mode for rogue AP detection.
show rogue-ap detection monitoring	Displays a table of detected APs and information about them, such as their MAC addresses, when they were last seen, and their SSIDs, to name a few.
show rogue-ap detection list {rogue | friendly| all}	Displays the specified rogue/friendly/all AP list.
show rogue-ap detection status	Displays whether rogue AP detection is on or off.
show rogue-ap detection info	Displays a summary of the number of detected devices from the following categories: rogue, friendly, ad-hoc, unclassified, and total.

9.2.1 Rogue AP Detection Examples

This example sets the device associated with MAC address 00:13:49:11:11:11 as a rogue AP, and the device associated with MAC address 00:13:49:11:11:22 as a friendly AP. It then removes MAC address from the rogue AP list with the assumption that it was misidentified.

```
Router(config)# rogue-ap detection
Router(config-detection)# rogue-ap 00:13:49:11:11:11 rogue
Router(config-detection)# friendly-ap 00:13:49:11:11:22 friendly
Router(config-detection)# no rogue-ap 00:13:49:11:11:11
Router(config-detection)# exit
```

This example displays the rogue AP detection list.

```
Router(config)# show rogue-ap detection list rogue
no.   mac                 description
contain
===========================================================================
1     00:13:49:18:15:5A                                                            0
```

This example shows the friendly AP detection list.

```
Router(config)# show rogue-ap detection list friendly
no.   mac                 description
===========================================================================
1     11:11:11:11:11:11   third floor
2     00:13:49:11:22:33
3     00:13:49:00:00:05
4     00:13:49:00:00:01
5     00:0D:0B:CB:39:33   dept1
```

This example shows the combined rogue and friendly AP detection list.

```
Router(config)# show rogue-ap detection list all
no.   role         mac                 description
===========================================================================
1     friendly-ap  11:11:11:11:11:11   third floor
2     friendly-ap  00:13:49:11:22:33
3     friendly-ap  00:13:49:00:00:05
4     friendly-ap  00:13:49:00:00:01
5     friendly-ap  00:0D:0B:CB:39:33   dept1
6     rogue-ap     00:13:49:18:15:5A
```

This example shows both the status of rogue AP detection and the summary of detected APs.

```
Router(config)# show rogue-ap detection status
rogue-ap detection status: on

Router(config)# show rogue-ap detection info
rogue ap: 1
friendly ap: 4
adhoc: 4
unclassified ap: 0
total devices: 0
```

9.3 Rogue AP Containment Overview

These commands enable rogue AP containment. You can use them to isolate a device that is flagged as a rogue AP. They are global in that they apply to all managed APs on the network (all APs utilize the same containment list, but only APs set to monitor mode can actively engage in containment of rogue APs). This means if we add a MAC address of a device to the containment list, then every AP on the network will respect it.

Note: Containing a rogue AP means broadcasting unviable login data at it, preventing legitimate wireless clients from connecting to it. This is a kind of Denial of Service attack.

9.4 Rogue AP Containment Commands

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 Rogue AP Containment Commands

LABEL	DESCRIPTION
ap_mac	Specifies the MAC address (in XX:XX:XX:XX:XX:XX format) of the AP to be contained. The no command removes the entry.

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

Table 26 Command Summary: Rogue AP Containment

COMMAND	DESCRIPTION
`rogue-ap containment`	Enters sub-command mode for rogue AP containment.
`[no] activate`	Activates rogue AP containment. Use the no parameter to deactivate rogue AP containment.
`[no] contain` *ap_mac*	Isolates the device associated with the specified MAC address. Use the no parameter to remove this device from the containment list.
`exit`	Exits configuration mode for rogue AP containment.
`show rogue-ap containment config`	Displays whether rogue AP containment is enabled or not.
`show rogue-ap containment list`	Displays the rogue AP containment list.

9.4.1 Rogue AP Containment Example

This example contains the device associated with MAC address 00:13:49:11:11:12 then displays the containment list for confirmation.

```
Router(config)# rogue-ap containment
Router(config-containment)# activate
Router(config-containment)# contain 00:13:49:11:11:12
Router(config-containment)# exit
Router(config)# show rogue-ap containment list
no.   mac
=====================================================================
1     00:13:49:11:11:12
```

Wireless Frame Capture

This chapter shows you how to configure and use wireless frame capture on the ZyWALL / USG.

10.1 Wireless Frame Capture Overview

Troubleshooting wireless LAN issues has always been a challenge. Wireless sniffer tools like Ethereal can help capture and decode packets of information, which can then be analyzed for debugging. It works well for local data traffic, but if your devices are spaced increasingly farther away then it often becomes correspondingly difficult to attempt remote debugging. Complicated wireless packet collection is arguably an arduous and perplexing process. The wireless frame capture feature in the ZyWALL / USG can help.

This chapter describes the wireless frame capture commands, which allows a network administrator to capture wireless traffic information and download it to an Ethereal/Tcpdump compatible format packet file for analysis.

10.2 Wireless Frame Capture Commands

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

Table 27 Input Values for Wireless Frame Capture Commands

LABEL	DESCRIPTION
ip_address	The IP address of the Access Point (AP) that you want to monitor. Enter a standard IPv4 IP address (for example, 192.168.1.2).
mon_dir_size	The total combined size (in kbytes) of all files to be captured. The maximum you can set is 50 megabtyes (52428800 bytes.)
file_name	The file name prefix for each captured file. The default prefix is monitor while the default file name is monitor.dump. You can use 1-31 alphanumeric characters, underscores or dashes but the first character cannot be a number. This string is case sensitive.

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

Table 28 Command Summary: Wireless Frame Capture

COMMAND	DESCRIPTION
frame-capture configure	Enters sub-command mode for wireless frame capture.
src-ip {add|del} {*ipv4_address* | local}	Sets or removes the IPv4 address of an AP controlled by the ZyWALL / USG that you want to capture wireless network traffic going through the AP interfaces. You can use this command multiple times to add additional IPs to the ~~monitor~~ list.
file-prefix *file_name*	Sets the file name prefix for each captured file. Enter up to 31 alphanumeric characters. Spaces and underscores are not allowed.
files-size *mon_dir_size*	Sets the total combined size (in kbytes) of all files to be captured.
exit	Exits configuration mode for wireless frame capture.
[no] frame-capture activate	Starts wireless frame capture. Use the no parameter to turn it off.
show frame-capture status	Displays whether frame capture is running or not.
show frame-capture config	Displays the frame capture configuration.

10.2.1 Wireless Frame Capture Examples

This example configures the wireless frame capture parameters for an AP located at IP address 192.168.1.2.

```
Router(config)# frame-capture configure
Router(frame-capture)# src-ip add 192.168.1.2
Router(frame-capture)# file-prefix monitor
Router(frame-capture)# files-size 1000
Router(frame-capture)# exit
Router(config)#
```

This example shows frame capture status and configuration.

```
Router(config)# show frame-capture status
capture status: off

Router(config)# show frame-capture config
capture source: 192.168.1.2
file prefix: monitor
file size: 1000
```

11

Dynamic Channel Selection

This chapter shows you how to configure and use dynamic channel selection on the ZyWALL / USG.

11.1 DCS Overview

Dynamic Channel Selection (DCS) is a feature that allows an AP to automatically select the radio channel upon which it broadcasts by passively listening to the area around it and determining what channels are currently being broadcast on by other devices.

When numerous APs broadcast within a given area, they introduce the possibility of heightened radio interference, especially if some or all of them are broadcasting on the same radio channel. This can make accessing the network potentially rather difficult for the stations connected to them. If the interference becomes too great, then the network administrator must open his AP configuration options and manually change the channel to one that no other AP is using (or at least a channel that has a lower level of interference) in order to give the connected stations a minimum degree of channel interference.

11.2 DCS Commands

See Section 8.2 on page 67 for detailed information about how to configure DCS settings in a radio profile.

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

Table 29 Command Summary: DCS

COMMAND	DESCRIPTION
`dcs now {ap_mac | profile_name}`	Sets the managed AP to scan for and select an available channel immediately.

12

Auto-Healing

This chapter shows you how to configure auto-healing settings.

12.1 Auto-Healing Overview

Auto-healing allows you to extend the wireless service coverage area of the managed APs when one of the managed APs fails.

12.2 Auto-Healing Commands

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

Table 30 Input Values for Auto-Healing Commands

LABEL	DESCRIPTION
interval	Enters the auto-healing interval time. The range is 5 ~ 30 minutes.

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

Table 31 Command Summary: Auto-Healing

COMMAND	DESCRIPTION
`[no] auto-healing activate`	Turns on the auto-healing feature. Use the no parameter to turn it off.
`auto-healing healing-interval` *`interval`*	Sets the interval that specifies how often the managed APs scan their neighborhoods and report the status of neighbor APs to the AP controller (ZyWALL / USG). An AP is considered “failed” if the AP controller obtains the same scan result that the AP is missing from the neighbor list of other APs three times.
`auto-healing healing-threshold`	Sets a minimum signal strength. A managed AP is added to the neighbor lists only when the signal strength of the AP is stronger than the specified threshold.
`auto-healing power-threshold <-50~-80>`	Sets a power threshold (in dBm). This value is used to calculate the power level (`power-threshold + margin`) to which the neighbor APs of the failed AP increase their output power in order to extend their wireless service coverage areas. When the failed AP is working again, its neighbor APs return their output power to the original level.

Table 31 Command Summary: Auto-Healing (continued)

COMMAND	DESCRIPTION
`auto-healing margin`	Enters a number from 0 to 9. This value is used to calculate the power level (`power-threshold` + `margin`) to which the neighbor APs of the failed AP increase their output power in order to extend their wireless service coverage areas.
`auto-healing update`	Sets all manged APs to immediately scan their neighborhoods three times in a row and update their neighbor lists to the AP controller (ZyWALL / USG).
`show auto-healing config`	Displays the current auto-healing configuration.

12.2.1 Auto-Healing Examples

This example enables auto-healing and sets the power level (in dBm) to which the neighbor APs of the failed AP increase their output power.

```
Router(config)# auto-healing activate
Router(config)# auto-healing power-threshold -70
Router(config)# show auto-healing config
auto-healing activate: yes
auto-healing interval: 10
auto-healing power threshold: -70 dBm
auto-healing healing threshold: -85 dBm
auto-healing margin: 0
Router(config)#
```

13

LEDs

This chapter describes two features that controls the LEDs of the managed APs connected to your ZyWALL / USG - Locator and Suppression.

13.1 LED Suppression Mode

The LED Suppression feature allows you to control how the LEDs of an AP behave after it's ready. The deafult LED suppression setting of the AP is different depending on your AP model.

✍ When the AP is booting or performing firmware upgrade, the LEDs will light regardless of the setting in LED suppression.

13.2 LED Suppression Commands

Use these commands to set how you want the LEDs to behave after the device is ready. You must use the `configure terminal` command before you can use these commands.

Table 32 LED Suppression Commands

COMMAND	DESCRIPTION
`led_suppress` *`ap_mac_address`* `enable`	Sets the LEDs of the specified AP to turn off after it's ready.
`led_suppress` *`ap_mac_address`* `disable`	Sets the LEDs of the specified AP to stay lit after the ZyWALL / USG is ready.
`show led_suppress` *`ap_mac_address`* `status`	Displays whether LED suppression mode is enabled or disabled on the specified AP.

13.2.1 LED Suppression Commands Example

The following example activates LED suppression mode on the AP with the MAC address 00:a0:c5:01:23:45 and displays the settings.

```
Router(config)# led_suppress 00:a0:c5:01:23:45 enable
Router(config)# show led_suppress 00:a0:c5:01:23:45 status
Suppress Mode Status : Enable
Router(config)#
```

13.3 LED Locator

The LED locator feature identifies the location of the WAC AP among several devices in the network. You can run this feature and set a timer.

13.4 LED Locator Commands

Use these commands to run the LED locator feature. You must use the `configure terminal` command before you can use these commands.

Table 33 LED Locator Commands

COMMAND	DESCRIPTION
`led_locator` *`ap_mac_address`* `on`	Enables the LED locator function on the specified AP. It will show the actual location of the AP among several devices in the network.
`led_locator` *`ap_mac_address`* `off`	Disables the LED locator function on the specified AP.
`led_locator` *`ap_mac_address`* `blink-timer <1..60>`	Sets a time interval between 1 and 60 minutes to stop the locator LED from blinking on the specified AP. Note: You should run this command before enabling the LED locator function.
`show led_locator` *`ap_mac_address`* `status`	Displays whether LED locator function is enabled on the specified AP and the timer setting.

13.4.1 LED Locator Commands Example

The following example turns on the LED locator feature on the AP with the MAC address 00:a0:c5:01:23:45, sets how long the locator LED stays blinking, and also displays the settings.

```
Router(config)# led_locator 00:a0:c5:01:23:45 blink-timer 5
Router(config)# led_locator 00:a0:c5:01:23:45 on
Router(config)# show led_locator 00:a0:c5:01:23:45 status
Locator LED Status : ON
Locator LED Time : 5
Router(config)#
```

14

Interfaces

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

14.1 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 interfaces 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.

14.1.1 Types of Interfaces

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

- **Port groups** create a hardware connection between physical ports at the layer-2 (data link, MAC address) level.
- **Ethernet interfaces** are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- **VLAN interfaces** receive and send tagged frames. The ZyWALL / USG automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- **Bridge interfaces** create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Unlike port groups, bridge interfaces can take advantage of some security features in the ZyWALL / USG. You can also assign an IP address and subnet mask to the bridge.
- **PPPoE/PPTP interfaces** support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE/PPTP interfaces.
- **Cellular interfaces** are for 3G WAN connections via a connected 3G device.
- **Virtual interfaces** (IP alias) provide additional routing information in the ZyWALL / USG. There are three types: **virtual Ethernet interfaces**, **virtual VLAN interfaces**, and **virtual bridge interfaces**.
- **VPN Tunnel Interface (VTI)** encrypts or decrypts IPv4 traffic from or to the interface according to the IP routing table.

- **Link Aggregation Group (LAG) interfaces** combine multiple physical Ethernet interfaces into a single logical interface, thus increasing uplink bandwidth and availability in the event a link goes down.
- **Trunks** manage load balancing between interfaces.

Port groups, and trunks 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 34 Characteristics of Ethernet, VLAN, Bridge, PPPoE/PPTP, and Virtual Interface (for some ZyWALL / USG models)

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 35 Ethernet, VLAN, Bridge, PPP, and Virtual Interface Characteristics (For other ZyWALL / USG 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
Packet size (MTU)	Yes	Yes	Yes	Yes	Yes	Yes	No

Table 35 Ethernet, VLAN, Bridge, PPP, and Virtual Interface Characteristics (For other ZyWALL / USG models) (continued)

CHARACTERISTICS	ETHERNET	ETHERNET	ETHERNET	VLAN	BRIDGE	PPP	VIRTUAL
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 36 Cellular and WLAN Interface Characteristics

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

* - 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.

14.1.2 Relationships Between Interfaces

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

Table 37 Relationships Between Different Types of Interfaces

INTERFACE	REQUIRED PORT / INTERFACE
Ethernet interface	physical port port group
VLAN interface	Ethernet interface
bridge interface	Ethernet interface* VLAN interface*
PPPoE/PPTP interface (For some ZyWALL / USG models)	Ethernet interface* VLAN interface* bridge interface
PPPoE/PPTP interface (For other ZyWALL / USG models)	WAN1, WAN2, OPT*
virtual interface	
(virtual Ethernet interface)	Ethernet interface*
(virtual VLAN interface)	VLAN interface*
(virtual bridge interface)	bridge interface
trunk	Ethernet interface Cellular interface VLAN interface bridge interface PPPoE/PPTP 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.

14.2 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 38 Input Values for General Interface Commands

LABEL	DESCRIPTION
interface_name	The name of the interface. Ethernet interface: For some ZyWALL / USG models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model. For other ZyWALL / USG 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 / USG 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 / USG model supports.
profile_name	The name of the DHCP pool. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
domain_name	Fully-qualified domain name. You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.

The following sections introduce commands that are supported by several types of interfaces. See Section 14.6 on page 117 for the unique commands for each type of interface.

14.2.1 Basic Interface Properties and IP Address Commands

This table lists basic properties and IP address commands.

Table 39 interface General Commands: Basic Properties and IP Address Assignment

COMMAND	DESCRIPTION
`show interface {ethernet | vlan | bridge | ppp} 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 | all}`	Displays information about the specified interface, specified type of interfaces, or all interfaces. See Section 14.6.1 on page 119 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 39 interface General Commands: Basic Properties and IP Address Assignment (continued)

COMMAND	DESCRIPTION
`show interface send statistics interval`	Displays the interval for how often the ZyWALL / USG refreshes the sent packet statistics for the interfaces.
`show interface summary all`	Displays basic information about the interfaces.
`show interface summary all status`	Displays the connection status of the interfaces.
`[no] interface` *`interface_name`*	Creates the specified interface if necessary and enters sub-command mode. The `no` command deletes the specified interface.
`[no] description` *`description`*	Specifies the description for the specified interface. The `no` command clears the description. *`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 / USG divides larger packets into smaller fragments. The `no` command resets the MTU to 1500.
`[no] shutdown`	Deactivates the specified interface. The `no` command activates it.
`traffic-prioritize {tcp-ack|content-filter|dns|ipsec-vpn|ssl-vpn} bandwidth <0..1048576> priority <1..7> [maximize-bandwidth-usage];`	Applies traffic priority when the interface sends TCP-ACK traffic, traffic for querying the content filter, traffic for resolving domain names, or encrypted traffic for an IPSec or SSL VPN tunnel. It also sets how much bandwidth the traffic can use and can turn on maximize bandwidth usage.
`traffic-prioritize {tcp-ack|content-filter|dns|ipsec-vpn|ssl-vpn} deactivate`	Turns off traffic priority settings for when the interface sends the specified type of traffic.
`[no] upstream <0..1048576>`	Specifies the upstream bandwidth for the specified interface. The `no` command sets the upstream bandwidth to 1048576.
`interface` *`interface_name`* `ipv6`	Creates the specified IPv6 interface if necessary and enters sub-command mode.
`address` *`ipv6_addr_prefix`*	Sets an IPv6 address with prefix for the interface.
`gateway` *`ipv6_addr`* `metric <0..15>`	Sets the specified IPv6 address's metric.

Table 39 `interface` General Commands: Basic Properties and IP Address Assignment (continued)

COMMAND	DESCRIPTION
`enable`	Turns on the IPv6 interface.
`nd ra accept`	Sets the IPv6 interface to accept IPv6 neighbor discovery router advertisement messages.
`nd ra advertise`	Sets the IPv6 interface to send IPv6 neighbor discovery router advertisement messages.
`nd ra managed-config-flag`	Turns on the flag in IPv6 router advertisements that tells hosts to use managed (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration.
`nd ra other-config-flag`	Turns on the other stateful configuration flag in IPv6 router advertisements that tells hosts to use administered (stateful) protocol to obtain autoconfiguration information other than addresses.
`nd ra mtu <1280..1500> | <0>`	Sets the Maximum Transmission Unit (MTU) size of IPv6 packets sent on the interface.
`nd ra hop-limit <0..255>`	Sets the maximum number of hops for router advertisements and all IPv6 packets originating from the interface.
`nd ra router-preference {low | medium | high }`	Sets the Default Router Preference (DRP) extension metric (low, medium, or high) in the interface's IPv6 neighbor discovery router advertisement messages.
`nd ra prefix-advertisement` *`ipv6_addr_prefix`* `[ auto { on | off} ] [ link{ on | off } ] [ preferred-time { <0..4294967294> | infinity }] [valid-time{ <0..4294967294> | infinity }]`	Sets the IPv6 prefix that the ZyWALL / USG advertises to its clients, whether or not to advertise it, and how long before the prefix's preference and lifetime expire.
`nd ra min-rtr-interval <3..1350>`	Sets the minimum IPv6 router advertisement transmission interval.
`nd ra max-rtr-interval <4..1800>`	Sets the maximum IPv6 router advertisement transmission interval.
`nd ra reachable-time <0..3600000>`	Sets the amount of time a remote IPv6 node is considered reachable after a reachability confirmation event.
`nd ra default-lifetime <4..9000>`	Sets the router lifetime value is included in all IPv6 router advertisements sent out the interface. The router lifetime value should be equal to or greater than the router advertisement interval.
`nd ra retrans-timer <0..4294967295>`	Sets the IPv6 router advertisement retransmission interval in milliseconds.
`ipv6 address` *`dhcp6_profile dhcp6_suffix_128`*	Has the ZyWALL / USG obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. *`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 / USG 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 39 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 / USG 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 39 interface General Commands: Basic Properties and IP Address Assignment (continued)

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

14.2.1.1 Basic Interface Properties Command Examples

The following commands make Ethernet interface ge1 a DHCP client.

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

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

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

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

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

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

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

14.2.2 IGMP Proxy Commands

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

Enter configuration terminal mode and select an interface

Table 40 `interface` Commands: IGMP Proxy Commands

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

14.2.2.1 IGMP Command Example

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

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

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

14.2.3 DHCP Setting Commands

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

Table 41 `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 / USG treats this DHCP pool as a static DHCP entry. • If you do not use the `host` command and use the `network` command, the ZyWALL / USG treats this DHCP pool as a pool of IP addresses. • 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.

Table 41 interface Commands: DHCP Settings (continued)

COMMAND	DESCRIPTION
	Use the following commands to create a static DHCP entry. If you do not use the host command, the commands that are not in this section have no effect, but you can still set them.
[no] host *ip*	Specifies the static IP address the ZyWALL / USG should assign. Use this command, along with hardware-address, to create a static DHCP entry. 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 / USG treats this DHCP pool like a static entry, regardless of the network setting. The no command clears this field.
[no] hardware-address *mac_address*	Reserves the DHCP pool for the specified MAC address. Use this command, along with host, to create a static DHCP entry. The no command clears this field.
[no] client-identifier *mac_address*	Specifies the MAC address that appears in the DHCP client list. The no command clears this field.
[no] client-name *host_name*	Specifies the host name that appears in the DHCP client list. The no command clears this field. *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.

Table 41 `interface` Commands: DHCP Settings (continued)

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

14.2.3.1 DHCP Setting Command Examples

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

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

14.2.3.2 DHCP Extended Option Setting Command Example

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

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

14.2.4 Interface Parameter Command Examples

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

Table 42 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		**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 vlan1 Router(config-if-vlan)# description downstream exit ip ipv6 mss mtu no ping-check port shutdown traffic-prioritize type upstream vlan-id

Table 42 Examples for Different Interface Parameters

BRIDGE		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		downstream exit ip ipv6 metric mtu no ping-check shutdown traffic-prioritize tunnel upstream

14.2.5 RIP Commands

This table lists the commands for RIP settings.

Table 43 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 17 on page 147 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.

14.2.6 OSPF Commands

This table lists the commands for OSPF settings.

Table 44 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.
[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.

Table 44 interface Commands: OSPF Settings (continued)

COMMAND	DESCRIPTION
`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 / USG is available. The `no` command sets the number of seconds to 10. See `ip ospf dead-interval` for more information.
`[no] ip ospf dead-interval <1..65535>`	Sets the number of seconds the ZyWALL / USG waits for “hello” messages from peer routers before it assumes the peer router is not available and deletes associated routing information. The `no` command sets the number of seconds to 40. See `ip ospf hello-interval` for more information.
`[no] ip ospf retransmit-interval <1..65535>`	Sets the number of seconds the ZyWALL / USG waits for an acknowledgment in response to a link state advertisement before it re-sends the advertisement. Link state advertisements (LSA) are used to share the link state and routing information between routers.

14.2.7 Connectivity Check (Ping-check) Commands

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

This table lists the `ping-check` commands

Table 45 `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 / USG log connectivity check result continuously. The `no` command disables the setting.
`show connectivity-check continuous-log status`	Displays the continuous log setting about connectivity check.
`interface `*`interface_name`*	Enters sub-command mode.
`[no] ping-check activate`	Enables ping check for the specified interface. The `no` command disables ping check for the specified interface.
`ping-check {`*`domain_name`*` | `*`ip`*` | default-gateway}`	Specifies what the ZyWALL / USG pings for the ping check; you can specify a fully-qualified domain name, IP address, or the default gateway for the interface.
`ping-check {`*`domain_name`*` | `*`ip`*` | default-gateway} period <5..30>`	Specifies what the ZyWALL / USG pings for the ping check and sets the number of seconds between each ping check.
`ping-check {`*`domain_name`*` | `*`ip`*` | default-gateway} timeout <1..10>`	Specifies what the ZyWALL / USG pings for the ping check and sets the number of seconds the ZyWALL / USG waits for a response.
`ping-check {`*`domain_name`*` | `*`ip`*` | default-gateway} fail-tolerance <1..10>`	Specifies what the ZyWALL / USG pings for the ping check and sets the number of times the ZyWALL / USG times out before it stops routing through the specified interface.
`ping-check {`*`domain_name`*` | `*`ip`*` | default-gateway} method {icmp | tcp}`	Sets how the ZyWALL / USG checks the connection to the gateway. `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.

14.2.7.1 Connectivity Check Command Example

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

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

14.3 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 46 Input Values for Ethernet Interface Commands

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

14.3.1 MAC Address Setting Commands

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

Table 47 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 47 interface Commands: MAC Setting (continued)

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

14.3.2 Port Grouping Commands

This section covers commands that are specific to port grouping.

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

Table 48 Basic Interface Setting Commands

COMMAND	DESCRIPTION
show port-grouping	Displays which physical ports are assigned to each representative interface.
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.

14.3.2.1 Port Grouping Command Examples

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

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

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

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

14.4 Virtual Interface Specific Commands

Virtual interfaces use many of the general interface commands discussed at the beginning of Section 14.2 on page 97. There are no additional commands for virtual interfaces.

14.4.1 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
```

14.5 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 14.2 on page 97.

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

Table 49 Input Values for PPPoE/PPTP Interface Commands

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

This table lists the PPPoE/PPTP interface commands.

Table 50 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 / USG get the IP address of the PPPoE/PPTP server automatically when it establishes the connection.

Table 50 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 / USG use its default MSS setting.
`mtu <576..1492>`	Sets the Maximum Transmission Unit in bytes.
`[no] ipv6 enable`	Turns on the IPv6 interface. The no command turns it off.
`[no] ipv6 nd ra accept`	Sets the IPv6 interface to accept IPv6 neighbor discovery router advertisement messages. The no command sets the IPv6 interface to discard IPv6 neighbor discovery router advertisement messages.
`[no] ipv6 metric <0..15>`	Sets the interface’s metric for IPv6 traffic. The no command clears it.
`[no] ipv6 address` *`dhcp6_profile dhcp6_suffix_128`*	Has the ZyWALL / USG obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. The no command removes the specified setting for using a delegated prefix as the beginning part of the network prefix. *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 / USG 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 / USG not get this interface’s IPv6 address from the DHCPv6 server.
`ipv6 dhcp6 duid {` *`duid`* `| mac }`	Specify the DHCP Unique IDentifier (DUID) of the interface or have it generated from the interface’s default MAC address.
`[no] ipv6 dhcp6-request-object` *`dhcp6_profile`*	For a DHCPv6 client interface, specify the profile of DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. The no command removes the DHCPv6 request settings profile.
`show interface ppp system-default`	Displays system default PPP interfaces (non-deletable) that come with the ZyWALL / USG.
`show interface ppp user-define`	Displays all PPP interfaces that were manually configured on the ZyWALL / USG.

14.5.1 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
```

14.6 Cellular Interface Specific Commands

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

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

Table 51 Interface Cellular 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.
`account` *`profile_name`*	Specifies the ISP account for the specified cellular interface.
`[no] band {auto|wcdma|gsm|lte}`	Sets (or clears) the cellular band that the cellular interface uses. `auto` has the ZyWALL / USG 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 / USG 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. `lte` has this interface only use a 4G LTE network. This option only appears when a USG dongle for 4G technology is inserted.

Table 51 Interface Cellular 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 / USG'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 / USG takes the actions you specified when a limit is exceeded during the month. Use the no command to disable budget control.
`[no] budget time active <1..672>`	Sets the amount of time (in hours) that the 3G connection can be used within one month. If you change the value, the ZyWALL / USG resets the statistics. Use the no command to disable time budget control.
`[no] budget data active {download-upload|download|upload} <1..100000>`	Sets how much downstream and/or upstream data (in Mega bytes) can be transmitted via the 3G connection within one month. download: set a limit on the downstream traffic (from the ISP to the ZyWALL / USG). upload: set a limit on the upstream traffic (from the ZyWALL / USG to the ISP). download-upload: set a limit on the total traffic in both directions. If you change the value, the ZyWALL / USG resets the statistics. Use the no command to disable data budget control.
`budget reset-day <0..31>`	Sets the date on which the ZyWALL / USG resets the budget every month. If the date you selected is not available in a month, such as 30th or 31st, the ZyWALL / USG resets the budget on the last day of the month.
`budget reset-counters`	Resets the time and data budgets immediately. The count starts over with the 3G connection’s full configured monthly time and data budgets. This does not affect the normal monthly budget restart.
`budget {log|log-alert}[recursive <1..65535>]`	Sets the ZyWALL / USG to create a log (log) or an alert log (log-alert) when the time or data limit is exceeded. You can also specify how often (from 1 to 65535 minutes) to generate a log or an alert.
`no budget log`	Sets the ZyWALL / USG to not create a log 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 / USG allows you to transmit data using the current connection, but you cannot build a new connection if the existing connection is disconnected.

Table 51 Interface Cellular Commands (continued)

COMMAND	DESCRIPTION
`budget percentage {ptime|pdata} <0..99>`	Sets a percentage (0~99) of time budget (ptime) or data (pdata) limit. When the specified limit is exceeded, the ZyWALL / USG takes the action configured using the budget {log-percentage|log-percentage-alert} command.
`budget {log-percentage|log-percentage-alert} [recursive <1..65535>]`	Sets to have the ZyWALL / USG create a log (log-percentage) or an alert log (log-percentage-alert) when the set percentage of time budget or data limit is exceeded. You can configure the percentage using the budget percentage command. You can also set how often (from 1 to 65535 minutes) to send the log or alert.
`no budget log-percentage`	Sets the ZyWALL / USG to not create a log when the set percentage of time budget or data limit is exceeded. You can configure the percentage using the budget percentage command.
`connectivity {nail-up | dial-on-demand}`	Sets the connection to be always on or only when there is traffic.
`[no] local-address <ip>`	Sets (or clears) the cellular interface’s local (own) IP address.
`mtu <576..1492>`	Sets the Maximum Transmission Unit in bytes.
`[no] pin <pin code>`	Sets (or clears) the PIN code for the cellular device’s 3G card. Use 1-4 alphanumeric characters, underscores(_), or dashes (-).
`[no] remote-address <ip>`	Sets (or clears) the IP address of the cellular interface’s peer (like a gateway or PPPoE server).
`interface cellular budget-auto-save <5..1440>`	Sets how often (in minutes) the ZyWALL / USG saves time and data usage records for a connection using the 3G card.
`show interface cellular [corresponding-slot|device-status|support-device]`	Shows the status of the specified cellular interface.
`show interface cellular corresponding-slot`	Shows which cellular interface is on which slot and whether which cellular interface has been configured.
`show interface cellular device-status`	Displays the installed SIM card and 3G card status.
`show interface cellular support-device`	Displays all 3G card models the ZyWALL / USG can support.
`show interface cellular budget-auto-save`	Displays how often (in minutes) the ZyWALL / USG records time and data usage of your 3G budgets.
`show interface cellular status`	Displays the traffic statistics and connection status for your cellular interfaces. See Section 14.6.1 on page 119 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.

14.6.1 Cellular Status

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

Table 52 Cellular Status

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

Table 52 Cellular Status

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

14.6.2 Cellular Interface Command Examples

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

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

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

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

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

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

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

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

14.7 Tunnel Interface Specific Commands

The ZyWALL / USG uses tunnel interfaces in Generic Routing Encapsulation (GRE), IPv6 in IPv4, and 6to4 tunnels. This section covers commands specific to tunnel interfaces. Tunnel interfaces also use many of the general interface commands discussed at the beginning of Section 14.2 on page 97.

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 14.2.7 on page 111 for more on ping check.

Table 53 interface Tunnel 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 / USG divides larger packets into smaller fragments. The `no` command resets the MTU to 1480.
`[no] downstream <0..1048576>`	Specifies the downstream bandwidth for the specified interface. The `no` command sets the downstream bandwidth to 1048576.
`tunnel mode [ ipv6ip [ manual | 6to4 ] ] ]`	Sets the interface to be an IPv6 over IPv4 tunnel. `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} priority-code <0..7> 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.

14.7.1 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
```

14.8 USB Storage Specific Commands

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

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

Table 54 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 / USG send a warning message when the remaining USB storage space is less than the set value.
`usb-storage mount`	Mounts the connected USB storage device.
`usb-storage umount`	Unmounts the connected USB storage device.
`[no] logging usb-storage`	Sets to have the ZyWALL / USG log or not log any information about the connected USB storage device(s) for the system log.
`show logging status usb-storage`	Displays the logging settings for the connected USB storage device.
logging usb-storage category *category* level <all|normal>	Configures the logging settings for the specified category for the connected USB storage device.
logging usb-storage category *category* disable	Stops logging for the specified category to the connected USB storage device.
`logging usb-storage flushThreshold <1..100>`	Configures the maximum storage space (in percentage) for storing system logs on the connected USB storage device.

Table 54 USB Storage General Commands (continued)

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

14.8.1 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
```

14.9 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 14.2 on page 97.

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

Table 55 Input Values for VLAN Interface Commands

LABEL	DESCRIPTION
`interface_name`	VLAN interface: vlan*x*, *x* = 0 - 4094 Ethernet interface: For some ZyWALL / USG models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model. For other ZyWALL / USGmodels use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz.

This table lists the VLAN interface commands.

Table 56 `interface` Commands: VLAN Interfaces

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

14.9.1 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
```

14.10 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 14.2 on page 97.

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

Table 57 Input Values for Bridge Interface Commands

LABEL	DESCRIPTION
`interface_name`	The name of the interface. Ethernet interface: For some ZyWALL / USG models use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model. For other ZyWALL / USG 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 / USG model supports.

This table lists the bridge interface commands.

Table 58 `interface` Commands: Bridge Interfaces

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

14.10.1 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
```

14.11 LAG Commands

This section covers commands that are specific to Link Aggregation Group (LAG) interfaces. LAG is a way to combine multiple physical Ethernet interfaces into a single logical interface. This increases uplink bandwidth. It also increases availability as even if a member link goes down, LAG can continue to transmit and receive traffic over the remaining links.

To configure LAG, configure a link number and specify the member ports in the link. All ports must have the same speed and be in full-duplex mode. You must configure the LAG on both sides of the link and you must set the interfaces on either side of the link to be the same speed.

Note: At the time of writing, up to 4 ports can be grouped into a LAG and up to 4 LAGs can be configured on a ZyWALL / USG.

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

Table 59 Input Values for LAG Interface Commands

LABEL	DESCRIPTION
interface_name	LAG interface: lag*x*, *x* = 0 - 4 (at the time of writing). Ethernet interface: For some ZyWALL / USG models use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model. For other ZyWALL / USG models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. VLAN interface: vlan*x*, *x* = 0 - 4094

This table lists the LAG-specific interface commands. See Table 39 on page 97 for common interface commands.

Table 60 interface Commands: LAG Interfaces

COMMAND	DESCRIPTION
`interface` *interface_name*	Creates the specified LAG interface (`lag0` for example) and enters sub-command mode.
`traffic-prioritize {tcp-ack|content-filter|dns} bandwidth <0..1048576>];`	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.
`traffic-prioritize {tcp-ack|content-filter|dns} priority-code <0..7> deactivate`	Turns off traffic priority settings for when the interface sends the specified type of traffic.
`mode {802_3ad | active-backup | balance-alb | mode 802_3ad}`	Sets the LAG mode. Mode refers to whether the LAG is acting as follows: • **`active-backup`** where only one slave in the LAG interface is active and another slave becomes active only if the active slave fails. • **`802.3ad`** (IEEE 802.3ad Dynamic link aggregation) where Link Aggregation Control Protocol (LACP) negotiates automatic combining of links and balances the traffic load across the LAG link by sending LACP packets to the directly connected device that also implements LACP. The slaves must have the same speed and duplex settings. • **`balance-alb`** (adaptive load balancing) where traffic is distributed according to the current load on each slave by ARP negotiation. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.
`[no] slave` *interface_name*	Specifies the member ports in the link. A slave is a physical Ethernet interface that is a member of a LAG. Slaves do not have an IP Address and in some cases share the same MAC address. The no command removed the member ports from the link.
`link-monitoring {arp | mii | none}`	Sets link monitoring to be arp, `mii` or none. • arp monitoring sends ARP queries and uses the reply to know if the link is up and that traffic is flowing over the link • `mii` monitoring monitors the state of the local interface; it can't tell if the link can transmit or receive packets. • none means no link monitoring is done.
`arp {arp-interval <1..1000> | arp-ip-target <W.X.Y.Z>}`	Configure for arp Link Monitoring. `arp-interval:` Specifies the frequency of ARP requests sent to confirm a that slave interface is up. `arp-ip-target <W.X.Y.Z>:` Specifies the IP address of the link to send ARP queries.

Table 60 interface Commands: LAG Interfaces (continued)

COMMAND	DESCRIPTION
`miimon <1..1000>`	Configure for `mii` Link Monitoring. Specifies the link check interval in milliseconds that the system polls the Media Independent Interface (MII) to get status.
`xmit-hash-policy {layer2 | layer2_3}`	Configure for `802.3ad` Mode. Specifies the algorithm for slave selection according to the selected TCP/IP layer.
`lacp-rate {fast | slow}`	Configure for `802.3ad` Mode. Specifies the preferred LACPDU packet transmission rate (`fast | slow`) to request from 802.3ad partner.
`updelay <0..1000>`	Configure for `mii` Link Monitoring. Specifies the waiting time in milliseconds to confirm the slave interface status is up.
`downdelay <0..1000>`	Configure for `mii` Link Monitoring. Specifies the waiting time in milliseconds to confirm the slave interface status is down.
`igmp {activate | direction {downstream | upstream} | version <1..3>}`	See Table 40 on page 103 for these command descriptions.
`ping-check`	See Table 45 on page 111 for these command descriptions.
`type {external | general | internal}`	Specifies one of the following option depending on the type of network to which the ZyWALL / USG is connected or if you want to additionally manually configure some related settings. **`internal`** is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The ZyWALL / USG automatically adds default SNAT settings for traffic flowing from this interface to an external interface. **`external`** is for connecting to an external network (like the Internet). The ZyWALL / USG automatically adds this interface to the default WAN trunk. For **`general`**, the rest of the screen’s options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.
`show lag available slaves`	Displays the available slaves that could be added to a LAG.
`show interface lag`	Displays interface details for all LAG interfaces.
`show interface lagx`	Displays interface details for LAG x.

14.11.1 LAG Interface Command Example

The following commands set up a LAG with slaves ge3, ge5 and ge6.

```
Router# configure terminal
Router(config)# interface lag1
Router(config-if-lag)# mode 802_3ad
Router(config-if-lag)# slave ge3
Router(config-if-lag)# slave ge5
Router(config-if-lag)# slave ge6
Router(config-if-lag)# link-monitoring mii
Router(config-if-lag)# miimon 1000
Router(config-if-lag)# xmit-hash-policy layer2
Router(config-if-lag)# lacp-rate fast
Router(config-if-lag)# updelay 500
Router(config-if-lag)# downdelay 500
Router(config-if-lag)# igmp activate
Router(config-if-lag)# type external
Router(config-if-lag)# exit
Router(config)# show lag available slaves
available slave count: 5
available slave: ge1,ge2,ge4,ge7,ge8
Router(config)# show interface lag1
active: yes
interface name: lag1
modifiable: yes
mode: 802.3ad
primary: none
slaves count: 3
slaves: ge3,ge5,ge6
description:
type: external
link monitoring: mii
miimon: 1000
updelay: 500
downdelay: 500
ARP interval: 20
ARP IP target: 0.0.0.0
LACP rate: fast
xmit hash policy: layer2
IP type: static
IP address: 0.0.0.0
netmask: 0.0.0.0
gateway:
metric: 0
igmp active: yes
igmp direction: upstream
igmp version: IGMPv3
upstream: 1048576
downstream: 1048576
MTU: 1500
MSS: 0
tcp-ack traffic prioritize:
    active                      : yes
    bandwidth                   : 1048576
    priority                    : 1
    maximize-bandwidth-usage    : yes
Router(config)# show interface lag
No. Name            Address type IP address      Mode           Active Slaves
===============================================================================
1   lag0            static       0.0.0.0         active-backup  yes
2   lag1            static       0.0.0.0         802.3ad        yes    ge3, ge5, ge6
```

14.12 VTI Commands

IPsec VPN Tunnel Interface (VTI) encrypts or decrypts IPv4 traffic from or to the interface according to the IP routing table.

VTI allows static routes to send traffic over the VPN. The IPsec tunnel endpoint is associated with an actual (virtual) interface. Therefore many interface capabilities such as Policy Route, Static Route, Trunk, and BWM can be applied to the IPsec tunnel as soon as the tunnel is active

Create a trunk using VPN tunnel interfaces for load balancing.

14.12.1 Restrictions for IPsec Virtual Tunnel Interface

- IPv4 traffic only
- IPSec tunnel mode only. A shared keyword must not be configured when using tunnel mode.
- With a VTI VPN you do not add local or remote LANs to your VPN configuration.
- For a VTI VPN you should only have one local and one remote WAN.
- A dynamic peer is not supported
- The IPsec VTI is limited to IP unicast and multicast traffic only.

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 VTI Interface Commands

LABEL	DESCRIPTION
interface_name	VTO interface: lag*x*, where x is a number from 0 to the maximum number of VPN connections allowed for your ZyWALL / USG model. Ethernet interface: For some ZyWALL / USG models use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model. For other ZyWALL / USG models use a name such as wan1, wan2, opt, lan1, ext-wlan, or dmz. VLAN interface: vlan*x*, *x* = 0 - 4094

This table lists the LAG-specific interface commands. See Table 39 on page 97 for common `interface` commands.

Table 62 `interface` Commands: VTI Interfaces

COMMAND	DESCRIPTION
`interface` *`interface_name`*	Creates the specified VTI interface (`vti1` for example) and enters sub-command mode. Note: You should have created a VPN tunnel for a Vpn Tunnel Interface scenario first.
`[no] downstream <0..1048576>`	Specifies the downstream bandwidth for the specified interface. The `no` command sets the downstream bandwidth to 1048576.
`[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] metric <0..15>`	Sets the VTI interface’s priority relative to other interfaces. The lower the number, the higher the priority.
`[no] ping-check activate`	Enables ping check for the specified interface. The `no` command disables ping check for the specified interface.

Table 62 interface Commands: VTI Interfaces (continued)

COMMAND	DESCRIPTION
ping-check {*domain_name* | *ip*}	Specifies what the ZyWALL / USG pings for the ping check; you can specify a fully-qualified domain name or IP address for the interface.
ping-check {*domain_name* | *ip*} period <5..30>	Specifies what the ZyWALL / USG pings for the ping check and sets the number of seconds between each ping check.
ping-check {*domain_name* | *ip*} timeout <1..10>	Specifies what the ZyWALL / USG pings for the ping check and sets the number of seconds the ZyWALL / USG waits for a response.
ping-check {*domain_name* | *ip*} fail-tolerance <1..10>	Specifies what the ZyWALL / USG pings for the ping check and sets the number of times the ZyWALL / USG times out before it stops routing through the specified interface.
ping-check {*domain_name* | *ip*} method {icmp | tcp}	Sets how the ZyWALL / USG checks the connection to the gateway. icmp: ping the domain name or IP address you specify to make sure it is still available. tcp: perform a TCP handshake with the domain name or IP address you specify to make sure it is still available.
ping-check {*domain_name* | *ip*} port <1..65535>	Specifies the port number to use for a TCP connectivity check.
[no] shutdown	Deactivates the specified interface. The no command activates it.
[no] upstream <0..1048576>	Specifies the upstream bandwidth for the specified interface. The no command sets the upstream bandwidth to 1048576.
binding interface *interface_name* crypto-map *map_name*	Binds the VTI interface to an IPSec SA that uses the VPN Tunnel Interface scenario (scenario vpn-tunnel-interface)
show interface vti	Displays interface details for all VTI interfaces.
show interface vtix	Displays interface details for VTI x.

14.12.2 VTI Interface Command Example

The following commands set up a VTI interface with the shown parameters and binds it to an IPSec SA using a VPN Tunnel Interface scenario.

```
Router# configure terminal
Router(config)# interface vti0
Router(config-if-vti)# downstream 10000
Router(config-if-vti)# upstream 10000
Router(config-if-vti)# ip address 1.1.1.1 255.255.255.0
Router(config-if-vti)# metric 5
Router(config-if-vti)# traffic-prioritize content-filter deactivate
Router(config-if-vti)# exit
Router(config)# show interface vti0
interface name: vti0
active: no
vpn rule:
connection: no
IP address: 1.1.1.1
netmask: 255.255.255.0
upstream: 10000
downstream: 10000
metric: 5
Router(config)#
Router(config)# crypto map test
Router(config-crypto test)# scenario vpn-tunnel-interface
Router(config-crypto test)# exit
Router(config)# binding interface vti0 crypto-map test
Router(config)#
```

15

Trunks

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

15.1 Trunks Overview

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

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

15.2 Trunk Scenario Examples

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

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

15.3 Trunk Commands Input Values

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

Table 63 interface-group Command Input Values

LABEL	DESCRIPTION
group-name	A descriptive name for the trunk. ZyWALL / USG uses up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.
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 some ZyWALL / USG models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model. Other ZyWALL / USG models use a name such as wan1, wan2, opt, lan1, or dmz. PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL / USG 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 / USG model supports.
num	The interface's position in the trunk's list of members <1..8>.
<CR>	Carriage Return (the "enter" key).

15.4 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 63 on page 134 for details about the values you can input with these commands.

Table 64 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 64 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 / USG will apply the specified algorithm. Outbound traffic means the traffic travelling from an internal interface (ex. LAN) to an external interface (ex. WAN). Inbound traffic means the opposite.
mode {normal|trunk}	Sets the mode for a trunk. Do this first in the trunk's sub-command mode.
move <1..8> to <1..8>	Changes the interface order in a trunk.
[no] interface {*num*|*interface-name*}	Removes an interface from the trunk.
system default-interface-group *group-name*	Sets the ZyWALL / USG to first attempt to use the the specified WAN trunk.
[no] system default-snat	Enables or disables Source NAT (SNAT). When SNAT is enabled, the ZyWALL / USG uses the IP address of the outgoing interface as the source IP address of the packets it sends out through the WAN interfaces.
show system default-snat	Displays whether the ZyWALL / USG enable SNAT or not. The ZyWALL / USG performs SNAT by default for traffic going to or from the WAN interfaces.
show system default-interface-group	Displays the WAN trunk the ZyWALL / USG first attempts to use.

15.5 Trunk Command Examples

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

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

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

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

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

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

16

Route

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

16.1 Policy Route

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

16.2 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 65 Input Values for General Policy Route Commands

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

Table 65 Input Values for General Policy Route Commands (continued)

LABEL	DESCRIPTION
interface_name	The name of the interface. Ethernet interface: Some ZyWALL / USG models use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model. Other ZyWALL / USG 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 / USG 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 / USG model supports.
policy_number	The number of a policy route. 1 - *X* where *X* is the highest number of policy routes the ZyWALL / USG model supports. See the ZyWALL / USG's User's Guide for details.
schedule_object	The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
service_name	The name of the service (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
user_name	The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
destv6	The IPv6 route prefix (subnet address) for the destination.
prefix	The IPv6 prefix length, 0 - 128.
gatewayv6	The IPv6 address of the specified gateway.
ipv6_addr	An IPv6 address.
ipv6_global_address	An IPv6 address excluding the link-local address (fe80::).
ipv6_link_local	An fe80:: IPv6 address.

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

Table 66 Command Summary: Policy Route

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

Table 66 Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
`[no] auto-destination`	When you set `tunnel` as the next-hop type (using the `next-hop tunnel` command) for this route, you can use this command to have the ZyWALL / USG use the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy instead of what you configure by using the `destination` command. The no command disables the setting.
`[no] auto-disable`	When you set `interface` or `trunk` as the next-hop type (using the `next-hop interface` or `next-hop trunk` command) for this route, you can use this command to have the ZyWALL / USG automatically disable this policy route when the next-hop's connection is down. The no command disables the setting.
`conn-check {FQDN | addr | activate}`	Turns on the connection check to the gateway identified by its FQDN or IP address.
`[no] deactivate`	Disables the specified policy. The no command enables the specified policy.
`[no] description` *`description`*	Sets a descriptive name for the policy. The no command removes the name for the policy.
`[no] destination {`*`address_object`*`|any}`	Sets the destination IP address the matched packets must have. The no command resets the destination IP address to the default (any). any means all IP addresses.
`[no] dscp {any | <0..63>}`	Sets a custom DSCP code point (0~63). This is the DSCP value of incoming packets to which this policy route applies. any means all DSCP value or no DSCP marker.
`[no] dscp class {default |` *`dscp_class`*`}`	Sets a DSCP class. Use `default` to apply this policy route to incoming packets that are marked with DSCP value 0. Use one of the pre-defined AF classes (including af11~af13, af21~af23, af31~af33, and af41~af43) to apply this policy route to incoming packets that are marked with the DSCP AF class. 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 142 for more details. *`dscp_class`* can set cs0~cs7 too.
`dscp-marking <0..63>`	Sets a DSCP value to have the ZyWALL / USG apply that DSCP value to the route's outgoing packets.
`dscp-marking class {default |` *`dscp_class`*`}`	Sets how the ZyWALL / USG handles the DSCP value of the outgoing packets that match this route. Set this to `default` to have the ZyWALL / USG set the DSCP value of the packets to 0. Set this to an "af" class (including af11~af13, af21~af23, af31~af33, and af41~af43) which stands for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 142 for more details. *`dscp_class`* can set cs0~cs7 too.
`no dscp-marking`	Use this command to have the ZyWALL / USG not modify the DSCP value of the route's outgoing packets.
`exit`	Leaves the sub-command mode.
`[no] interface` *`interface_name`*	Sets the interface on which the incoming packets are received. The no command resets the incoming interface to the default (`any`). `any` means all interfaces.
`[no] next-hop {auto|gateway` *`address object`* `|interface` *`interface_name`* `|trunk` *`trunk_name`*`|tunnel` *`tunnel_name`*`}`	Sets the next-hop to which the matched packets are routed. The no command resets next-hop settings to the default (`auto`).

Table 66 Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
`[no] schedule` *schedule_object*	Sets the schedule. The `no` command removes the schedule setting to the default (`none`). `none` means any time.
`[no] service {`*service_name*`|any}`	Sets the IP protocol. The `no` command resets service settings to the default (`any`). `any` means all services.
`[no] snat {outgoing-interface|pool {`*address_object*`}}`	Sets the source IP address of the matched packets that use SNAT. The `no` command removes source NAT settings from the rule.
`[no] source {`*address_object*`|any}`	Sets the source IP address that the matched packets must have. The `no` command resets the source IP address to the default (`any`). `any` means all IP addresses.
`[no] srcport {`*profile_name*`|any}`	Sets the source port that the matched packets must have. The `no` command resets the source port to the default (`any`). `any` means all ports.
`[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] 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] 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 142 for more details. *dscp_class* can set cs0~cs7 too.
`dscp-marking <0..63>`	Sets a DSCP value to have the ZyWALL / USG apply that DSCP value to the route’s outgoing packets.

Table 66 Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
dscp-marking class {default | *dscp_class*}	Sets how the ZyWALL / USG handles the DSCP value of the outgoing packets that match this route. Set this to default to have the ZyWALL / USG set the DSCP value of the packets to 0. Set this to an “af” class (including af11~af13, af21~af23, af31~af33, and af41~af43) which stands for Assured Forwarding. The number following the “af” identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ on page 142 for more details. *dscp_class* can set cs0~cs7 too.
no dscp-marking	Use this command to have the ZyWALL / USG not modify the DSCP value of the route’s outgoing packets.
exit	Leaves the sub-command mode.
[no] interface *interface_name*	Sets the interface on which the matched packets are received. The no command resets the incoming interface to the default (any). any means all interfaces.
[no] next-hop {auto|gateway *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] 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] srcport {*profile_name*|any}	Sets the source port that the matched packets must have. The no command resets the source port to the default (any). any means all ports.
[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.
[no] policy controll-ipsec-dynamic-rules activate	Enables the ZyWALL / USG to use policy routes to manually specify the destination addresses of dynamic IPSec rules. You must manually create these policy routes. The ZyWALL / USG automatically obtains source and destination addresses for dynamic IPSec rules that do not match any of the policy routes. The no command has the ZyWALL / USG automatically obtain source and destination addresses for all dynamic IPSec rules.
policy default-route	Enters the policy-route sub-command mode to set a route with the name “default-route”.
policy delete *policy_number*	Removes a routing policy.
policy flush	Clears the policy routing table.
policy list table	Displays all policy route settings.
policy move *policy_number* to *policy_number*	Moves a routing policy to the number that you specified.
[no] policy override-direct-route activate	Has the ZyWALL / USG forward packets that match a policy route according to the policy route instead of sending the packets to a directly connected network. Use the no command to disable it.

Table 66 Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
`[no] policy controll-virtual-server-rules activate`	Gives policy routes priority over NAT virtual server rules (1-1 SNAT). Use the no command to give NAT virtual server rules priority over policy routes.
`[no] policy6 override-direct-route activate`	Has the ZyWALL / USG forward IPv6 packets that match a policy route according to the policy route instead of sending the packets to a directly connected network. Use the no command to disable it.
`show bwm activation`	Displays whether or not the global setting for bandwidth management on the ZyWALL / USG is enabled.
`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 conn-check`	Displays the policy route for the connection check.
`show policy-route conn-check [`*`policy_number`*`]`	Displays the specified policy route for the connection check.
`show policy-route conn-check status [`*`policy_number`*`]`	Displays the connection check status for the specified policy route.
`show policy-route controll-ipsec-dynamic-rules`	Displays whether the ZyWALL / USG checks policy routes first before IPSec dynamic rules.
`show policy-route override-direct-route`	Displays whether or not the ZyWALL / USG forwards packets that match a policy route according to the policy route instead of sending the packets to a directly connected network.
`show policy-route controll-virtual-server-rules`	Displays whether or not policy routes have priority over NAT virtual server rules (1-1 SNAT).
`show policy-route6 override-direct-route`	Displays whether or not the ZyWALL / USG forwards IPv6 packets that match a policy route according to the policy route instead of sending the packets to a directly connected network.
`show policy-route rule_count`	Displays the number of policy routes that have been configured on the ZyWALL / USG.
`show policy-route underlayer-rules`	Displays all policy route rule details for advanced debugging.
`show policy-route6 [`*`policy_number`*`]`	Displays all or specified IPv6 policy route settings.
`show policy-route6 begin <1..200> end <1..200>`	Displays the specified range of IPv6 policy route settings.
`show policy-route6 controll-ipsec-dynamic-rules`	Displays whether the ZyWALL / USG checks IPv6 policy routes first before IPSec dynamic rules.
`show policy-route6 rule_count`	Displays the number of IPv6 policy routes that have been configured on the ZyWALL / USG.

16.2.1 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 67 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)

16.2.2 Policy Route Command Example

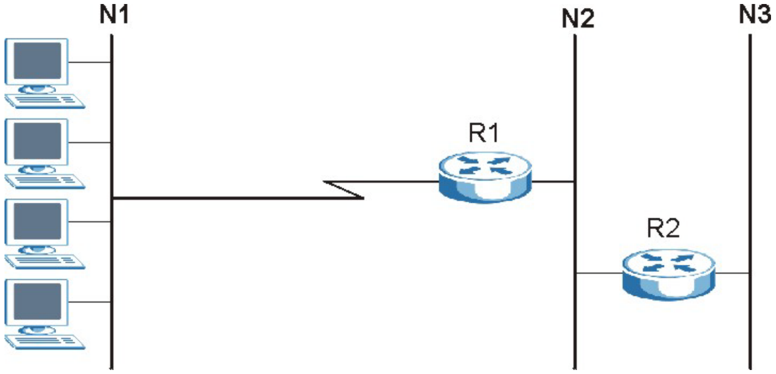
The following commands create two address objects (TW_SUBNET and GW_1) and insert a policy that routes the packets (with the source IP address TW_SUBNET and any destination IP address) through the interface ge1 to the next-hop router GW_1. This route uses the IP address of the outgoing interface as the 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
  auto-disable: no
  description: example
  user: any
  schedule: none
  interface: ge1
  tunnel: none
  sslvpn: none
  source: TW_SUBNET
  destination: any
  DSCP code: any
  service: any
  srcport: any
  nexthop type: Gateway
  nexthop: GW_1
  nexthop state: Not support
  auto destination: no
  SNAT: outgoing-interface
  DSCP marking: preserve
  connectivity-check: no
Router(config)#
```

16.3 IP Static Route

The ZyWALL / USG has no knowledge of the networks beyond the network that is directly connected to the ZyWALL / USG. For instance, the ZyWALL / USG knows about network **N2** in the following figure through gateway **R1**. However, the ZyWALL / USG is unable to route a packet to network **N3** because it doesn't know that there is a route through the same gateway **R1** (via gateway **R2**). The static routes are for you to tell the ZyWALL / USG about the networks beyond the network connected to the ZyWALL / USG directly.

Figure 14 Example of Static Routing Topology



16.4 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 65 on page 137 for information on input values.

Table 68 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 17.2.5 on page 150.
`ip6 route destv6/prefix { ipv6_global_address	ipv6_link_local	interface} [<0..127>]`	Sets an IPv6 static route.
`ip6 route destv6/prefix { ipv6_link_local interface} [<0..127>]`	Sets an IPv6 link local static route.
`no ip6 route destv6/prefix { gatewayv6	interface} [<0..127>]`	Deletes the specified IPv6 static route.
`ip6 route replace destv6/prefix { gatewayv6	interface} [<0..127>] with destv6/prefix { gatewayv6	interface} [<0..127>]`	Changes an existing IPv6 route's settings.
`[no] ip route control-virtual-server-rules activate`	Gives static routes priority over NAT virtual server rules (1-1 SNAT). It also automatically gives policy routes priority over NAT virtual server rules. Use the no command to give NAT virtual server rules priority over static routes.
`show ip route control-virtual-server-rules`	Displays whether or not static routes have priority over NAT virtual server rules (1-1 SNAT).

16.4.1 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
     2002:22:22:34::                                 64
     ge2                                             1
2    2002:22:22:34::                                 64
     2001:12::12                                     2
3    2002:22:22:34::                                 64
     Fe80::1:2                                       2
```

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
```

17

Routing Protocol

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

17.1 Routing Protocol Overview

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

The ZyWALL / USG supports two standards, RIP and OSPF, for routing protocols. RIP and OSPF are compared in Table 69 on page 147, and they are discussed further in the next two sections.

Table 69 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

17.2 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 70 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.

17.2.1 RIP Commands

This table lists the commands for RIP.

Table 71 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".
`encrypted-string ciphertext`	Sets the cipher to encrypt the string.

17.2.2 General OSPF Commands

This table lists the commands for general OSPF configuration.

Table 72 router Commands: General OSPF Configuration

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

17.2.3 OSPF Area Commands

This table lists the commands for OSPF areas.

Table 73 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.

17.2.4 Virtual Link Commands

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

Table 74 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.
`[no] area IP virtual-link IP encrypted-authentication-key <`*`ciphertext`*`>`	Sets the ciphertext for text encryption in the specified virtual link. The no command clears the ciphertext.
`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.

Table 74 router Commands: Virtual Links in OSPF Areas (continued)

COMMAND	DESCRIPTION
`area IP virtual-link IP message-digest-key <1..255> encrypted-authentication-key`	Sets the MD5 ID 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.

17.2.5 Learned Routing Information Commands

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

Table 75 ip route Commands: Learned Routing Information

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

17.2.6 show ip route Command Example

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

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

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

18

Zones

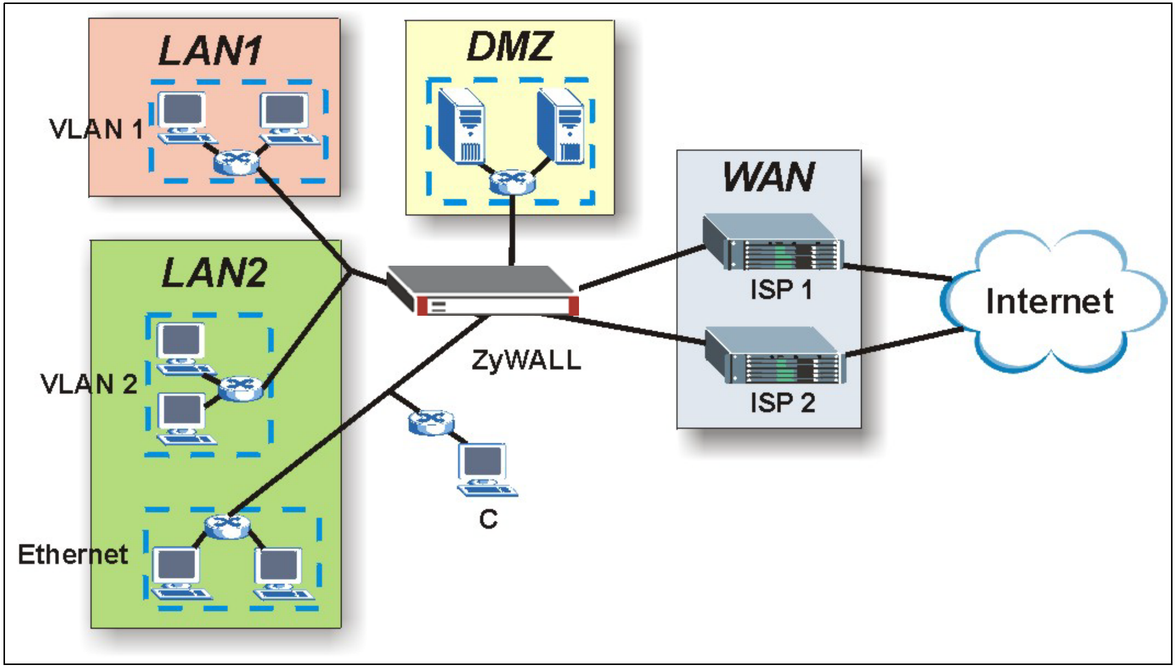
Set up zones to configure network security and network policies in the ZyWALL / USG.

18.1 Zones Overview

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

Zones cannot overlap. Each Ethernet interface, VLAN interface, bridge interface, PPPoE/PPTP interface, 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 15 Example: Zones



18.2 Zone Commands Summary

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

Table 76 Input Values for Zone Commands

LABEL	DESCRIPTION
profile_name	The name of a zone, or the name of a VPN tunnel. For some ZyWALL / USG modelsuse up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other ZyWALL / USGmodels: • 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 77 zone Commands

COMMAND	DESCRIPTION
show zone [*profile_name*]	Displays information about the specified zone or about all zones.
show zone binding-iface	Displays each interface and zone mappings.
show zone default-binding	Displays the pre-configured interface and zone mappings that come with the ZyWALL / USG.
show zone none-binding	Displays the interfaces, tunnels and SSL VPNs that are not associated with a zone yet.
show zone system-default	Displays the pre-configured default zones that you cannot delete from the ZyWALL / USG.
show zone user-define	Displays all customized zones.
[no] zone *profile_name*	Creates the zone if necessary and enters sub-command mode. The no command deletes the zone.
zone *profile_name*	Enter the sub-command mode.
[no] interface *interface_name*	Adds the specified interface to the specified zone. The no command removes the specified interface from the specified zone. See Section 14.2 on page 97 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.

18.2.1 Zone Command Examples

The following commands add Ethernet interfaces ge1 and ge2 to zone A.

```
Router# configure terminal
Router(config)# zone A
Router(zone)# interface ge1
Router(zone)# interface ge2
Router(zone)# exit
Router(config)# show zone
No. Name                             Member
===========================================================================
1   A                                ge1,ge2
Router(config)# show zone A
No. Type                             Member
===========================================================================
1   interface                        ge1
2   interface                        ge2
```

19

DDNS

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

19.1 DDNS Overview

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

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

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

Table 78 Network > DDNS

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

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

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

19.2 DDNS Commands Summary

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

Table 79 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 80 ip ddns Commands

COMMAND	DESCRIPTION
`show ddns [`*profile_name*`]`	Displays information about the specified DDNS profile or about all DDNS profiles.
`show ddns-status`	Shows which DDNS profiles are active, inactive or have failed.
`[no] ip ddns profile` *profile_name*	Creates or edits the specified DDNS profile and enters sub-command mode if necessary. The no command deletes this profile.
`[no]https activate`	Encrypts traffic using SSL (port 443) to the DDNS server. Not all DDNS providers support this option. The no command disables HTTPS.
`[no] service-type {dyndns | dyndns_static | dyndns_custom | dynu-basic | dynu-premium | no-ip | peanut-hull | 3322-dyn | 3322-static | Selfhost | User custom}`	Sets the service type in the specified DDNS profile. The no command clears it.
`[no] username` *username* `password` *password*	Sets the username and password in the specified DDNS profile. The no command clears these fields. *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.

Table 80 ip ddns Commands (continued)

COMMAND	DESCRIPTION
`[no] mx {ip | domain_name}`	Enables the mail exchanger and sets the fully-qualified domain name of the mail server to which mail from this domain name is forwarded. The `no` command disables the mail exchanger. *domain_name*: You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character must be alphanumeric.
`[no] wan-iface interface_name`	Sets the WAN interface in the specified DDNS profile. The `no` command clears it.
`[no] backup-iface interface_name`	Sets the backup WAN interface in the specified DDNS profile. The `no` command clears it.
`[no] ha-iface interface_name`	Sets the HA interface in the specified DDNS profile. The `no` command clears it.
`[no] backmx`	Enables the backup mail exchanger. The `no` command disables it.
`[no] wildcard`	Enables the wildcard feature. The `no` command disables it.
`[no] url {URL TEXT}`	Type the URL that can be used to access the server that will host the DDSN service. For example, `# url /api/dynamic/update.php?hostname=home.example.com& ip=10.1.1.1` The `no` command disables it.
`[no] ddns-server {FQDN DNS}`	Type the IP address of the server that will host the DDSN service. For example, `# ddns-server www.dnspark.net` The `no` command disables it.
`[no] additional-ddns-options`	Avaialable for `User custom`. Enter one ofg the following. • `--ip_server_name` which should be the URL to get the server's public IP address - for example, http://myip.easylife.tw/ • `--dyndns_system` to specify the DYNDNS Server type - for example, dyndns@dyndns.org

19.3 DDNS Commands Example

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

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

20

Virtual Servers

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

20.1 Virtual Server Overview

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

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

20.1.1 1:1 NAT and Many 1:1 NAT

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

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

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

20.2 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 81 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 82 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 20.1.1 on page 159 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 / USG available to a public network outside the ZyWALL / USG (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 20.1.1 on page 159 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 / USG available to a public network outside the ZyWALL / USG (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 20.1.1 on page 159 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 / USG available to a public network outside the ZyWALL / USG (like the Internet). The deactivate command disables the virtual server rule.

Table 82 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 20.1.1 on page 159 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 / USG available to a public network outside the ZyWALL / USG (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`*.

20.2.1 Virtual Server Command Examples

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

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

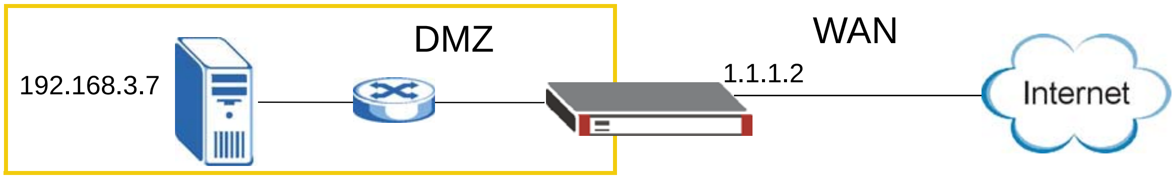
The following command shows information about all the virtual servers in the ZyWALL / USG.

```
Router(config)# show ip virtual-server
virtual server: WAN-LAN_H323
  Index: 1
  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)#
```

20.2.2 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 some models) interface and map it to the HTTP server's private IP address of 192.168.3.7.

Figure 16 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 secure policy rule

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

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

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

21

HTTP Redirect

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

21.1 HTTP Redirect Overview

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

21.1.1 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.

21.2 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 83 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 some ZyWALL / USG models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model. For other ZyWALL / USG models use a name such as wan1, wan2, opt, lan1, 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 / USG 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 / USG model supports.

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

Table 84 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.

21.2.1 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
```

22

Redirect Service

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

22.1 HTTP Redirect

HTTP redirect forwards the client's HTTP request (except HTTP traffic destined for the ZyWALL / USG) to a web proxy server. A proxy server helps client devices make indirect requests to access the Internet or outside network resources/services. The web proxy provides caching service to allow quick access and reduce network usage. The proxy checks its local cache for the requested web resource first. If it is not found, the proxy gets it from the specified server and forwards the response to the client.

22.2 SMTP Redirect

SMTP redirect forwards the authenticated client's SMTP message to a SMTP server, that handles all outgoing e-mail messages. The ZyWALL / USG forwards SMTP traffic using TCP port 25.

22.3 Redirect Commands

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

Table 85 Input Values for HTTP Redirect Commands

LABEL	DESCRIPTION
profile_name	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 some ZyWALL / USG models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model. For other ZyWALL / USG models use a name such as wan1, wan2, opt, lan1, 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 / USG 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 / USG model supports.
user_name	This is the user account or user group name to which this rule is applied.

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 86 Command Summary: Redirect

COMMAND	DESCRIPTION
`redirect-service append <1..20>`	Adds a new Redirect rule and enters sub-command mode.
`redirect-service <1..20>`	Edits an existing Redirect rule and enters sub-command mode.
`[no] activate`	Enables the Redirect rule. The no command disables the Redirect rule.
`exit`	Leaves sub-command mode
`[no] interface` *interface_name*	Names the interface for the Redirect rule. The *no* command restores the interface to any.
`[no] name` *profile_name*	Names the Redirect rule to identify it. The *no* command restores the name to `default`.
`[no] port <1..65535>`	Sets the service port for the Redirect rule. The *no* command restores the `http-redirect` port to `80`, and the `smtp-redirect` port to `25`.

Table 86 Command Summary: Redirect (continued)

COMMAND	DESCRIPTION
`[no] server <fqdn> <w.x.y.z>`	Sets the fully-qualified domain name or IPv4 address for the Redirect rule. The *no* command clears the server.
`[no] service {http-redirect | smtp-redirect}`	Configures HTTP-redirect or SMTP-redirect as the Redirect rule. The *no* command restores the service to `http-redirect`.
`[no] source profile_name`	Configures the address or address group object. The *no* command restores the source to any.
`[no] user user_name`	Configures the user account or user group to which this rule is applied. The *no* command restores the user to any.
`redirect-service flush`	Clears all Redirect rules.
`redirect-service insert <1..20>`	Inserts a new Redirect rule at the specified location and enters sub-command mode.
`redirect-service move <1..20> to <1..20>`	Moves a Redirect rule to the specified location.
`show redirect-service <1..20>`	Displays details of the specified Redirect rule.

22.3.1 Redirect Command Example

The following commands show how to create and display Redirect service rules on the ZyWALL / USG.

```
Router(config)# redirect-service append
Router(redirect-service)# interface ge4
Router(redirect-service)# name test
Router(redirect-service)# port 11111
Router(redirect-service)# service smtp-redirect
Router(redirect-service)# server 1.1.1.1
Router(redirect-service)# user admin
Router(redirect-service)# activate
Router(redirect-service)# exit
Router(config)# show redirect-service
redirect service rule: 1
  active: yes
  name: default
  service: http-redirect
  user: any
  incoming interface: any
  source address: any
  server:
  port: 80
  id: 1
redirect service rule: 2
  active: yes
  name: default
  service: http-redirect
  user: any
  incoming interface: any
  source address: any
  server:
  port: 80
  id: 0
redirect service rule: 3
  active: yes
  name: default
  service: append
  user: any
  incoming interface: any
  source address: any
  server:
  port: 80
  id: 2
redirect service rule: 4
  active: yes
  name: test
  service: smtp-redirect
  user: admin
  incoming interface: ge4
  source address: any
  server: 1.1.1.1
  port: 11111
  id: 3
Router(config)#
```

23

ALG

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

23.1 ALG Introduction

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

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

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

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

23.2 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 87 alg Commands

COMMAND	DESCRIPTION
`[no] alg sip [direct-media | direct-signalling | inactivity-timeout | | media-timeout <1..86400> | signal-timeout <1..86400> | transformation]`	Turns on or configures the ALG. Use `direct-media  to` to set the ZyWALL / USG to allow SIP audio session. Use `direct-signalling` to set the ZyWALL / USG to allow SIP signaling sessions. Use `inactivity-timeout` to have the ZyWALL / USG apply SIP media and signaling inactivity time out limits. 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 / USG modify IP addresses and port numbers embedded in the SIP data payload. You do not need to use this if you have a SIP device or server that will modify IP addresses and port numbers embedded in the SIP data payload. The no command turns off the SIP ALG or removes the settings that you specify.
`alg sip defaultport`	Enters ALG SIP default port sub-command
`Router(SIP Signaling Port)# [no] port <1025..65535>`	Enter the custom UDP port number for SIP traffic. The no command removes the custom UDP port number for SIP traffic.
`[no] alg <h323 | ftp> [signal-port <1025..65535> | signal-extra-port <1025..65535> | transformation]`	Turns on or configures the H.323 or FTP ALG. 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 / USG modify IP addresses and port numbers embedded in the H.323 or FTP data payload. You do not need to use this if you have an H.323 or FTP device or server that will modify IP addresses and port numbers embedded in the H.323 or FTP data payload. The no command turns off the H.323 or FTP ALG or removes the settings that you specify.
`show alg <sip | h323 | ftp>`	Displays the specified ALG's configuration.

23.3 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
```

24

UPnP

24.1 UPnP and NAT-PMP Overview

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

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

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

24.2 UPnP and NAT-PMP Commands

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

Table 88 ip upnp Commands

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

Table 88 ip upnp Commands (continued)

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

24.3 UPnP & NAT-PMP Commands Example

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

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

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

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

25

IP/MAC Binding

25.1 IP/MAC Binding Overview

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

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

25.2 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 89 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.

25.3 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)#
```

Layer 2 Isolation

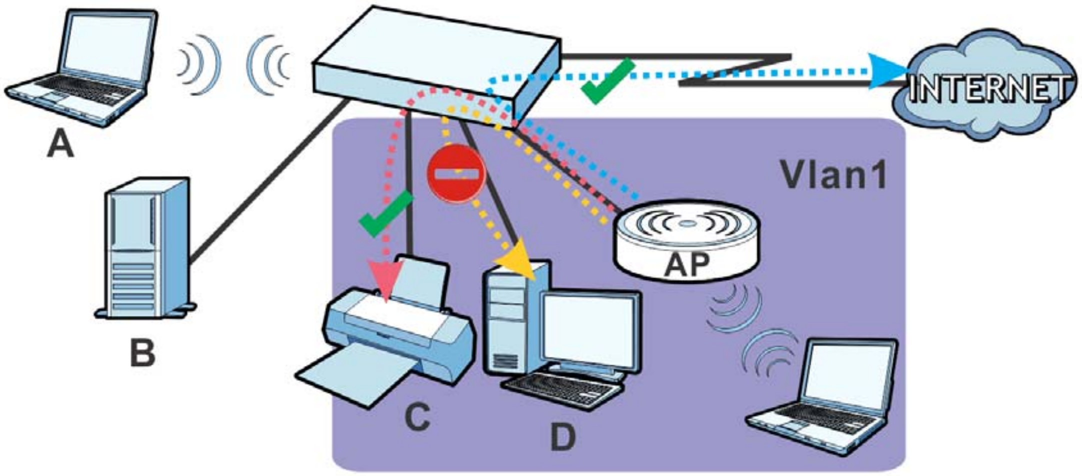
26.1 Layer 2 Isolation Overview

Layer-2 isolation is used to prevent connected devices from communicating with each other in the ZyWALL / USG's local network(s), on which layer-2 isolation is enabled, except the devices in the white list.

Note: Layer-2 isolation does not check the wireless traffic.

In the following example, layer-2 isolation is enabled on the ZyWALL / USG's interface Vlan1. A printer, PC and AP are in the Vlan1. The IP address of network printer (**C**) is added to the white list. The connected AP then cannot communicate with the PC (**D**), but can access the network printer (**C**), server (**B**), wireless client (**A**) and the Internet.

Figure 17 Layer-2 Isolation Application



26.2 Layer 2 Isolation Commands

The following table lists the l2-isolation commands. You must use the configure terminal command to enter the configuration mode before you can use these commands.

Table 90 l2-isolation Commands

COMMAND	DESCRIPTION
l2-isolation	Enters the layer 2 isolation sub-command mode to enable Layer-2 isolation on the ZyWALL / USG and specific internal interface(s).
[no] activate	Turns on Layer-2 isolation on the ZyWALL / USG. The no command disables Layer-2 isolation on the ZyWALL / USG.
[no] interface *interface_name*	Turns on Layer-2 isolation on a specific internal interface. The no command disables Layer-2 isolation for the specified interface.
white-list *rule_number*	Enters the layer 2 isolation white list sub-command mode to set a new rule in the white list. See Table 91 on page 183 for the sub-commands. *rule_number*: 1 - N, where N depends on the ZyWALL / USG model.
white-list activate	Turns on the white list on the ZyWALL / USG. IP addresses that are not listed in the white list are blocked from communicating with other devices in the layer-2-isolation-enabled internal interface(s) except for broadcast packets.
white-list append	Enters the layer 2 isolation white list sub-command mode to add a rule to the end of the white list. See Table 91 on page 183 for the sub-commands.
white-list flush	Removes all rules in the white list.
white-list no activate	Turns the white list off.
no l2-isolation activate	Disables Layer-2 isolation on the ZyWALL / USG.
no l2-isolation white-list *rule_number*	Disables the specified rule in the white list. *rule_number*: 1 - N, where N depends on the ZyWALL / USG model.
no l2-isolation white-list activate	Turns on the white list on the ZyWALL / USG.
show l2-isolation	Displays whether Layer-2 isolation is enabled on an interface.
show l2-isolation activation	Displays whether Layer-2 isolation is enabled on the ZyWALL / USG.
show l2-isolation white-list [*rule_number*]	Displays all or a specified white list rule settings. *rule_number*: 1 - N, where N depends on the ZyWALL / USG model.
show l2-isolation white-list activation	Displays whether the white list is enabled.

26.2.1 Layer 2 Isolation White List Sub-Commands

The following table describes the sub-commands for l2-isolation white-list commands.

Table 91 l2-isolation white-list Sub-commands

COMMAND	DESCRIPTION
[no] activate	Enables the rule. The no command disables the rule.

Table 91 l2-isolation white-list Sub-commands (continued)

COMMAND	DESCRIPTION
[no] description *description*	Sets a descriptive name (up to 60 printable ASCII characters) for a rule. The no command removes the descriptive name from the rule.
[no] ip-address *ip*	Sets an IPv4 address associated with this rule. The no command removes the IP address. This is the IP address of device that can be accessed by the devices connected to an internal interface on which layer-2 isolation is enabled.

26.3 Layer 2 Isolation Commands Example

The following example enables Layer-2 isolation on the ZyWALL / USG and interface lan2. It also creates a rule in the white list to allow access to the device with IP address 172.17.0.66. It then displays the Layer-2 isolation settings.

```
Router# configure terminal
Router(config)# l2-isolation
Router(l2-isolation)# activate
Router(l2-isolation)# interface lan2
Router(l2-isolation)# white-list 1
Router(white-list)# activate
Router(white-list)# description PC
Router(white-list)# ip-address 172.17.0.66
Router(white-list)# exit
Router(config)# show l2-isolation
interface
===============================================================================
lan2
Router(config)# show l2-isolation activation
Layer2 Isolation Status: yes
Router(config)# show l2-isolation white-list
layer2 isolation white list rule: 1
  active: yes
  ip address: 172.17.0.66
  description:    PC
Router(config)#
```

27

Secure Policy

This chapter introduces the ZyWALL / USG's secure policies and shows you how to configure them.

Note: In the guide Secure Policy commands may also be referred to as Firewall in general descriptions.

27.1 Secure Policy Overview

A secure policy is a template of security settings that can be applied to specific traffic at specific times. The policy can be applied:

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

The policy can be configured:

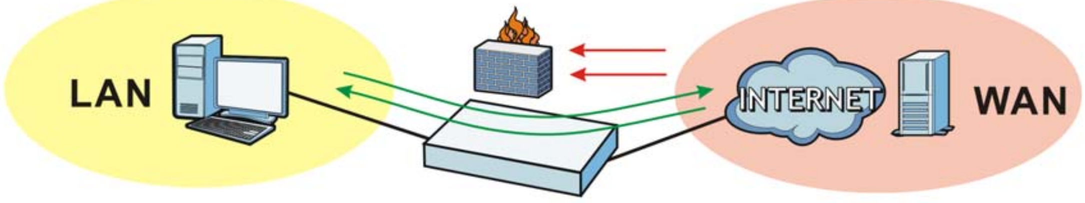
- to allow or deny traffic that matches the criteria above
- send a log or alert for traffic that matches the criteria above
- to apply the actions configured in the UTM profiles (application patrol, content filter, IDP, anti-virus, anti-spam) to traffic that matches the criteria above

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

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

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

Figure 18 Default Directional Policy Example



27.2 Secure Policy Commands

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

Table 92 Input Values for Secure Policy 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 some ZyWALL / USG models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other ZyWALL / USGmodels, use pre-defined zone names like DMZ, LAN1, SSL VPN, IPSec VPN, OPT, and WAN.
rule_number	The priority number of a secure policy. 1 - *X* where *X* is the highest number of rules the ZyWALL / USG model supports. See the ZyWALL / USG's User's Guide for details.
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 secure policy. 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 93 Command Summary: Secure Policy

COMMAND	DESCRIPTION
`secure-policy activate`	Enables Secure Policy on the ZyWALL / USG to perform access control.
show secure-policy filter from *zone_object* to *zone_object* srcip <*ip-address*> dstip <*ip*> service {any | tcp | udp | icmp | gre | esp | user-defined} *port-number* user *user_name* sch *schedule_object*	Applies IPv4 search filters to find specific IPv4 security policies based on direction, application, user, source, destination and/or schedule.
`[no] secure-policy asymmetrical-route activate`	Allows or disallows asymmetrical route topology.
secure-policy *rule_number*	Enters the secure policy sub-command mode to set a firewall rule. See Table 94 on page 189 for the sub-commands.
secure-policy *zone_object* {*zone_object*|ZyWALL} *rule_number*	Enters the secure policy sub-command mode to set a direction specific through-ZyWALL rule or to-ZyWALL rule. See Table 94 on page 189 for the sub-commands.
secure-policy *zone_object* {*zone_object*|ZyWALL} append	Enters the secure policy 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 94 on page 189 for the sub-commands.

Table 93 Command Summary: Secure Policy (continued)

COMMAND	DESCRIPTION
secure-policy *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 secure policy rule list.
secure-policy *zone_object* {*zone_object*|ZyWALL} flush	Removes all direction specific through-ZyWALL rule or to-ZyWALL rules.
secure-policy *zone_object* {*zone_object*|ZyWALL} insert *rule_number*	Enters the secure policy sub-command mode to add a direction specific through-ZyWALL rule or to-ZyWALL rule before the specified rule number. See Table 94 on page 189 for the sub-commands.
secure-policy *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] secure-policy activate	Enables the secure policy on the ZyWALL / USG. The no command disables the secure policy.
secure-policy append	Enters the secure policy sub-command mode to add a global secure policy rule to the end of the global rule list. See Table 94 on page 189 for the sub-commands.
secure-policy default-rule action {allow | deny | reject} { no log | log [alert] }	Sets how the secure policy handles packets that do not match any other secure policy rule.
secure-policy delete *rule_number*	Removes a secure policy rule.
secure-policy flush	Removes all secure policy rules.
secure-policy insert *rule_number*	Enters the secure policy sub-command mode to add a secure policy rule before the specified rule number. See Table 94 on page 189 for the sub-commands.
secure-policy move *rule_number* to *rule_number*	Moves a secure policy rule to the number that you specified.
firewall icsa {icmp-destroy-session} {enable | disable}	During ICSA certification a connection automatically terminates immediately once ICMP unreachable or ICMP TTL expired is received. Use this command to turn off this behavior.
show firewall icsa status	Displays if a ICSA certification connection is automatically terminated immediately once ICMP unreachable or ICMP TTL expired is received.
show secure-policy	Displays all Secure Policy settings.
show secure-policy *rule_number*	Displays a secure policy rule's settings.
show secure-policy *zone_object* {*zone_object*|ZyWALL}	Displays all secure policy rules settings for the specified packet direction.
show secure-policy *zone_object* {*zone_object*|ZyWALL} *rule_number*	Displays a specified secure policy rule's settings for the specified packet direction.
show secure-policy status	Displays whether or not the secure policy is active, whether or not asymmetrical route topology is allowed, and the default secure policy rule's configuration.
show secure-policy block_rules	Displays all the secure policy rules that deny access.
show secure-policy any ZyWALL	Shows all the to-ZyWALL / USG secure policy rules.
show secure-policy6 filter from *zone_object* to *zone_object* srcip6 <*ip-address*> dstip6 <*ip*> service {any | tcp | udp | icmp | gre | esp | user-defined} *port-number* user *user_name* sch *schedule_object*	Applies IPv6 search filters to find specific IPv6 (if enabled) security policies based on direction, application, user, source, destination and/or schedule.

Table 93 Command Summary: Secure Policy (continued)

COMMAND	DESCRIPTION
secure-policy6 *rule_number*	Enters the IPv6 secure policy sub-command mode to set a secure policy rule. See Table 94 on page 189 for the sub-commands.
secure-policy6 *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 94 on page 189 for the sub-commands.
secure-policy6 *zone_object* {*zone_object*|ZyWALL} append	Enters the IPv6 secure policy 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 94 on page 189 for the sub-commands.
secure-policy6 *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.
secure-policy6 *zone_object* {*zone_object*|ZyWALL} flush	Removes all direction specific IPv6 through-ZyWALL rule or to-ZyWALL rules.
secure-policy6 *zone_object* {*zone_object*|ZyWALL} insert *rule_number*	Enters the IPv6 secure policy sub-command mode to add a direction specific through-ZyWALL rule or to-ZyWALL rule before the specified rule number. See Table 94 on page 189 for the sub-commands.
secure-policy6 *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] secure-policy6 activate	Enables the IPv6 secure policy on the ZyWALL / USG. The no command disables the IPv6 firewall.
secure-policy6 append	Enters the IPv6 secure policy sub-command mode to add a global firewall rule to the end of the global rule list. See Table 94 on page 189 for the sub-commands.
secure-policy6 default-rule action {allow | deny | reject} { no log | log [alert] }	Sets how the IPv6 secure policy handles packets that do not match any other secure policy rule.
secure-policy6 delete *rule_number*	Removes a IPv6 secure policy rule.
secure-policy6 flush	Removes all IPv6 secure policy rules.
secure-policy6 insert *rule_number*	Enters the IPv6 secure policy sub-command mode to add a secure policy rule before the specified rule number. See Table 94 on page 189 for the sub-commands.
secure-policy6 move *rule_number* to *rule_number*	Moves a IPv6 secure policy rule to the number that you specified.
show secure-policy6	Displays all IPv6 secure policy settings.
show secure-policy6 *rule_number*	Displays a IPv6 secure policy rule's settings.
show secure-policy6 *zone_object* {*zone_object*|ZyWALL}	Displays all IPv6 secure policy rules settings for the specified packet direction.
show secure-policy6 *zone_object* {*zone_object*|ZyWALL} *rule_number*	Displays a specified IPv6 secure policy rule's settings for the specified packet direction.
show secure-policy6 status	Displays whether or not the IPv6 secure policy is active, whether or not IPv6 asymmetrical route topology is allowed, and the default IPv6 secure policy rule's configuration.
show secure-policy6 block_rules	Displays all the IPv6 secure policy rules that deny access.

Table 93 Command Summary: Secure Policy (continued)

COMMAND	DESCRIPTION
`show secure-policy6 any ZyWALL`	Shows all the IPv6 to-ZyWALL / USG secure policy rules.
`[no] secure-policy6 asymmetrical-route activate`	Allows or disallows asymmetrical route topology for IPv6 traffic.
`session-status-update reply-time <5..300>`	Set how many seconds the ZyWALL / USG will allow a session to remain idle (without traffic) before closing it.
`session-status-update alg {active|inactive}`	Enables or Disables ALG session updates
`show session-status-update reply-time`	Displays idle session timeout

27.2.1 Secure Policy Sub-Commands

The following table describes the sub-commands for several `secure-policy` and `secure-policy6` commands.

Table 94 firewall Sub-commands

COMMAND	DESCRIPTION
`action {allow|deny|reject}`	Sets the action the ZyWALL / USG takes when packets match this rule.
`[no] activate`	Enables a secure policy rule. The no command disables the rule.
`[no] ctmatch {dnat | snat}`	Use dnat to block packets sent from a computer on the ZyWALL / USG's WAN network from being forwarded to an internal network according to a virtual server rule. Use snat to block packets sent from a computer on the ZyWALL / USG's internal network from being forwarded to the WAN network according to a 1:1 NAT or Many 1:1 NAT rule. The no command forwards the matched packets. Subcommands cannot be used with secure-policy6.
`[no] description` *`description`*	Sets a descriptive name (up to 60 printable ASCII characters) for a secure policy 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 / USG to create a log (and optionally an alert) when packets match this rule. The no command sets the ZyWALL / USG not to create a log or alert when packets match this rule.
`[no] schedule` *`schedule_object`*	Sets the schedule that the rule uses. The no command removes the schedule settings from the rule.

Table 94 firewall Sub-commands (continued)

COMMAND	DESCRIPTION
[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 secure policy rule. The no command removes the source port from the rule.
[no] to {*zone_object*|ZyWALL}	Sets the zone to which the packets are sent. The no command removes the zone to which the packets are sent and resets it to the default (any). any means all interfaces or VPN tunnels.
[no] user *user_name*	Sets a user-aware secure policy 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. Subcommands cannot be used with secure-policy6.
secure-policy <*profile name*>	Creates a secure policy rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
[no] cf-profile <*profile name*> {[no log]|[log by-profile]} {activate | deactivate}	Applies the (already-created) named anti- x profile to traffic that matches the secure-policy rule. Log by-profile generates a log for all traffic that matches criteria in the anti- x profile. no log does turns off logging and overrides the anti- x profile log setting. The no command does not apply the named anti- x profile to traffic that matches the secure-policy rule.
[no] as-profile <*profile name*> {[no log]|[log by-profile]} {activate | deactivate}	Applies the (already-created) named anti- x profile to traffic that matches the secure-policy rule. Log by-profile generates a log for all traffic that matches criteria in the anti- x profile. no log does turns off logging and overrides the anti- x profile log setting. The no command does not apply the named anti- x profile to traffic that matches the secure-policy rule.
[no] av-profile <*profile name*>{[no log]|[log by-profile]} {activate | deactivate}	Applies the (already-created) named anti- x profile to traffic that matches the secure-policy rule. Log by-profile generates a log for all traffic that matches criteria in the anti- x profile. no log does turns off logging and overrides the anti- x profile log setting. The no command does not apply the named anti- x profile to traffic that matches the secure-policy rule.
[no] idp-profile <*profile name*> {[no log]|[log by-profile]} {activate | deactivate}	Applies the (already-created) named anti- x profile to traffic that matches the secure-policy rule. Log by-profile generates a log for all traffic that matches criteria in the anti- x profile. no log does turns off logging and overrides the anti- x profile log setting. The no command does not apply the named anti- x profile to traffic that matches the secure-policy rule.

Table 94 firewall Sub-commands (continued)

COMMAND	DESCRIPTION
[no] ssl-profile <*profile name*> {[no log]|[log by-profile]} {activate | deactivate}	Applies the (already-created) named anti- x profile to traffic that matches the secure-policy rule. Log by-profile generates a log for all traffic that matches criteria in the anti- x profile. no log does turns off logging and overrides the anti- x profile log setting. The no command does not apply the named anti- x profile to traffic that matches the secure-policy rule.
[no] app-profile <*profile name*> {[no log]|[log by-profile]} {activate | deactivate}	Applies the (already-created) named anti- x profile to traffic that matches the secure-policy rule. Log by-profile generates a log for all traffic that matches criteria in the anti- x profile. no log does turns off logging and overrides the anti- x profile log setting. The no command does not apply the named anti- x profile to traffic that matches the secure-policy rule.

27.2.2 Secure Policy Command Examples

These are IPv4 secure policy configuration examples. The IPv6 secure policy commands are similar.

The following example shows you how to add an IPv4 secure policy 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 secure policy sub-command mode to add a secure policy rule.
- Set the direction of travel of packets to which the rule applies.
- Set the destination IP address(es).
- Set the service to which this rule applies.
- Set the action the ZyWALL / USG is to take on packets which match this rule.

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

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

```
Router(config)# show secure-policy WAN ZyWALL

secure-policy rule: 11
  name: WAN_to_Device
  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
  content-filter profile: none
                 enable: no, log: by-profile
  anti-spam      profile: none
                 enable: no, log: by-profile
  anti-virus     profile: none
                 enable: no, log: by-profile
  idp            profile: none
                 enable: no, log: by-profile
  ssl-inspection profile: none
                 enable: no, log: by-profile
  app-patrol     profile: none
                 enable: no, log: by-profile
```

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

```
Router(config)# show secure-policy6 WAN ZyWALL

secure-policy rule: 1
  name: Device_Default_Allow_Service
  description:
  user: any, schedule: none
  from: any, to: ZyWALL
  source IP: any, source port: any
  destination IP: any, service: Default_Allow_v6_any_to_ZyWALL
  log: no, action: allow, status: yes
  content-filter profile: none
                 enable: no, log: by-profile
  anti-spam      profile: none
                 enable: no, log: by-profile
  anti-virus     profile: none
                 enable: no, log: by-profile
  idp            profile: none
                 enable: no, log: by-profile
  ssl-inspection profile: none
                 enable: no, log: by-profile
  app-patrol     profile: none
                 enable: no, log: by-profile
secure-policy rule: 11
  name: WAN_to_Device
  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
  content-filter profile: none
                 enable: no, log: by-profile
  anti-spam      profile: none
                 enable: no, log: by-profile
  anti-virus     profile: none
                 enable: no, log: by-profile
  idp            profile: none
                 enable: no, log: by-profile
  ssl-inspection profile: none
                 enable: no, log: by-profile
  app-patrol     profile: none
                 enable: no, log: by-profile
```

27.3 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 95 Input Values for General Session Limit Commands

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

Table 95 Input Values for General Session Limit Commands (continued)

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

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

Table 96 Command Summary: Session Limit

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

Table 96 Command Summary: Session Limit (continued)

COMMAND	DESCRIPTION
`[no] address6 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.

27.4 ADP Commands Overview

Anomaly Detection and Prevention (ADP) protects against anomalies based on violations of protocol standards (RFCs – Requests for Comments) and abnormal flows such as port scans. This section introduces ADP, anomaly profiles and applying an ADP profile to a traffic direction.

Traffic Anomalies

Traffic anomaly policies look for abnormal behavior or events such as port scanning, sweeping or network flooding. They operate at OSI layer-2 and layer-3. Traffic anomaly policies may be updated when you upload new firmware.

Protocol Anomalies

Protocol anomalies are packets that do not comply with the relevant RFC (Request For Comments). Protocol anomaly detection includes:

- TCP Decoder
- UDP Decoder
- ICMP Decoder
- IP Decoder

Protocol anomaly policies may be updated when you upload new firmware.

27.4.1 ADP 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 97 Input Values for ADP Commands

LABEL	DESCRIPTION
zone-rule	The name of a zone. For some ZyWALL / USG models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case- sensitive. For other ZyWALL / USG models use pre-defined zone names like DMZ, LAN1, SSL VPN, WLAN, IPSec VPN, OPT, and WAN
adp-profile	The name of an ADP profile. It can consist of alphanumeric characters, the underscore, and the dash, and it is 1-31 characters long. Spaces are not allowed.

27.4.2 ADP Activation Commands

Use these commands to activate ADP and see status.

Table 98 ADP Activation Commands

LABEL	DESCRIPTION
[no] idp anomaly activate	Anomaly detection does not require registration. The no command disables the specified service.
show idp anomaly activation	Displays anomaly detection service status.

27.4.3 ADP Global Profile Commands

These commands apply to all ADP profiles on the ZyWALL / USG.

Table 99 ADP Global Profile Commands

LABEL	DESCRIPTION
`idp rename anomaly` *<profile1> <profile2>*	Rename an ADP anomaly profile originally named profile1 to profile2.
`no idp anomaly` *<profile3>*	Delete an ADP profile named profile3.
`show idp anomaly base profile`	Displays all anomaly detection base profiles.
`show idp anomaly profiles`	Displays all ADP anomaly profiles.
`show idp anomaly rules`	Displays all ADP anomaly rules.

27.4.4 ADP Zone-to-Zone Rule Commands

These commands bind ADP profiles to traffic directions.

Table 100 ADP Zone-to-Zone Rule Commands

LABEL	DESCRIPTION
`idp anomaly rule {append | <1..32> | insert <1..32>}`	Creates an ADP anomaly rule and enters the sub-command mode.
`bind profile`	Binds the ADP anomaly profile to the entry’s traffic direction.
`no bind`	Removes the ADP anomaly profile’s binding.
`from-zone zone_rule`	Specifies the zone the traffic is coming from.
`[no] activate`	Turns on the ADP anomaly profile to traffic direction binding. The no command turns it off.
`idp  anomaly rule {delete <1..32> | move <1..32> to <1..32>}`	Removes or moves an ADP anomaly profile to traffic direction entry.
`no idp anomaly rule <1..32>`	Removes an ADP anomaly profile to traffic direction entry.
`show idp anomaly rules`	Displays the ADP anomaly zone to zone rules.

27.4.5 ADP Add/Edit Profile Sub Commands

These commands create or edit ADP profiles.

Table 101 ADP Add/Edit Profile Commands

LABEL	DESCRIPTION
idp anomaly *adp-profile* [base {all | everything | none}]	Creates a new IDP anomaly profile called *adp-profile*. *adp-profile* 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.
description *description*	*description:* Use up to 60 printable ASCII characters
`no description`	The no command removes the descriptive name from the profile.
`base {all | everything | none}`	Use the base profile you specify. You cannot change the base profile after you specify it.
`scan-detection sensitivity {low | medium | high}`	Sets scan-detection sensitivity.
`no scan-detection sensitivity`	Clears scan-detection sensitivity. The default sensitivity is medium.
`scan-detection block-period <1..3600>`	Sets for how many seconds the ZyWALL / USG blocks all packets from being sent to the victim (destination) of a detected anomaly attack.
`[no] scan-detection {tcp-xxx} {activate | log [alert] | block}`	Activates TCP scan detection options where {tcp-xxx} ={tcp-portscan | tcp-portscan-fin | tcp-portscan-syn tcp-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-portscan} {activate | log [alert] | block}`	Activates or deactivates UDP port scan . Also sets UDP scan-detection logs or alerts and blocking. no deactivates UDP scan detection, its logs, alerts or blocking.
`flood-detection block-period <1..3600>`	Sets for how many seconds the ZyWALL / USG blocks all packets from being sent to the victim (destination) of a detected anomaly attack.

Table 101 ADP Add/Edit Profile Commands (continued)

LABEL	DESCRIPTION
[no] flood-detection {tcp-flood | udp-flood | icmp-flood | igmp-flood} {activate | log [alert] | block}	Activates or deactivates TCP, UDP,IGMP or ICMP flood detection. Also sets flood detection logs or alerts and blocking. no deactivates flood detection, its logs, alerts or blocking.
[no] tcp-decoder {tcp-xxx} activate	Activates or deactivates tcp decoder options where {tcp-xxx} = {bad-tcp-flag | bad-tcp-l4-size | tcp-fragment | tcp-land}
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 {bad-udp-l4-size | udp-land | udp-smurf} activate	Activates or deactivates udp decoder options.
udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} log [alert]	Sets udp decoder log or alert options.
no udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} log	Deactivates udp decoder log options.
udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} action {drop | reject-sender | reject-receiver | reject-both}	Sets udp decoder action.
no udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} action	Deactivates udp decoder actions.
[no] icmp-decoder {bad-icmp-l4-size | icmp-fragment | icmp-smurf} activate	Activates or deactivates icmp decoder options.
icmp-decoder {bad-icmp-l4-size | icmp-fragment | icmp-smurf} log [alert]	Sets icmp decoder log or alert options.
no icmp-decoder {bad-icmp-l4-size icmp-fragment | icmp-smurf} log	Deactivates icmp decoder log options.
icmp-decoder {bad-icmp-l4-size | icmp-fragment | icmp-smurf} action {drop | reject-sender | reject-receiver | reject-both}	Sets icmp decoder action.
no icmp-decoder {bad-icmp-l4-size | icmp-fragment | icmp-smurf} action	Deactivates icmp decoder actions.
[no] ip-decoder {ip-spoof | ip-teardrop} activate	Activates or deactivates ip decoder options.

Table 101 ADP Add/Edit Profile Commands (continued)

LABEL	DESCRIPTION
`[no] ip-decoder {ip-spoof | ip-teardrop} log`	Activates or deactivates ip decoder log options.
`[no] ip-decoder {ip-spoof | ip-teardrop} action {drop | reject-sender | reject-receiver | reject-both}`	Activates or deactivates ip decoder actions.
`exit`	Use exit to quit sub-command mode.
`show idp anomaly profile scan-detection [all details]`	Shows all scan-detection settings of the specified ADP profile.
`show idp anomaly profile scan-detection {tcp-portscan | tcp-portscan-syn | tcp-portsweep | tcp-portscan-fin} details`	Shows selected TCP scan-detection settings for the specified ADP profile.
`show idp anomaly profile scan-detection {udp-portscan} details`	Shows UDP scan-detection settings for the specified ADP profile.
`show idp anomaly profile flood-detection [all details]`	Shows all flood-detection settings for the specified ADP profile.
`show idp anomaly profile flood-detection {tcp-flood | udp-flood | icmp-flood | icmp-flood} details`	Shows flood-detection settings for the specified ADP profile.
`show idp anomaly profile tcp-decoder all details`	Shows tcp-decoder settings for the specified ADP profile.
`show idp anomaly profile tcp-decoder {bad-tcp-flag | bad-tcp-l4-size | tcp-land} details`	Shows tcp-decoder settings for the specified ADP profile.
`show idp anomaly profile udp-decoder all details`	Shows udp-decoder settings for the specified ADP profile.
`show idp anomaly profile udp-decoder {bad-udp-l4-size | udp-land | udp-smurf} details`	Shows specific udp-decoder settings for the specified ADP profile.
`show idp anomaly profile icmp-decoder all details`	Shows all icmp-decoder settings for the specified ADP profile.
`show idp anomaly profile icmp-decoder {bad-icmp-l4-size | icmp-smurf} details`	Shows specific icmp-decoder settings for the specified ADP profile.
`show idp anomaly` *`adp-profile`* `ip-decoder all details`	Shows all ip-decoder settings for the specified ADP profile.
`show idp anomaly` *`adp-profile`* `ip-decoder {ip-spoof | ip-teardrop} details`	Shows specific ip-decoder settings for the specified ADP profile.

28

Web Authentication

28.1 Web Authentication Overview

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

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

28.2 Web Authentication Commands

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

Table 102 web-auth Commands

COMMAND	DESCRIPTION
`[no] web-auth activate`	Enables force user authentication that force users to log in to the ZyWALL / USG before the ZyWALL / USG routes traffic for them. The no command means the user authentication is not required.
`web-auth default-rule authentication {required | unnecessary} {no log | log [alert]}`	Sets the default authentication policy that the ZyWALL / USG uses on traffic that does not match any exceptional service or other authentication policy. `required`: Users need to be authenticated. They must manually go to the ZyWALL / USG's login screen. The ZyWALL / USG will not redirect them to the login screen. `unnecessary`: Users do not need to be authenticated. `no log | log [alert]`: Select whether to have the ZyWALL / USG generate a log (`log`), log and alert (`log alert`) or not (`no log`) for packets that match this default policy.
`web-auth [no] exceptional-service` *`service_name`*	Sets a service which you want users to be able to access without user authentication. The `no` command removes the specified service from the exceptional list.
`web-auth login setting`	Sets the login web page through which the user authenticates his or her connection before he or she can then connect to the rest of the network or Internet. See Table 103 on page 202 for the sub-commands.
`web-auth method portal`	Sets a client to authenticate with the ZyWALL / USG through the specifically designated web portal.
`web-auth policy <1..1024>`	Creates the specified condition for forcing user authentication, if necessary, and enters sub-command mode. The conditions are checked in sequence, starting at 1. See Table 103 on page 202 for the sub-commands.

Table 102 web-auth Commands (continued)

COMMAND	DESCRIPTION
`web-auth policy append`	Creates a new condition for forcing user authentication at the end of the current list and enters sub-command mode. See Table 103 on page 202 for the sub-commands.
`web-auth policy insert <1..1024>`	Creates a new condition for forcing user authentication at the specified location, renumbers the other conditions accordingly, and enters sub-command mode. See Table 103 on page 202 for the sub-commands.
`web-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.
`web-auth policy flush`	Deletes every condition.
`web-auth policy move <1..1024> to <1..1024>`	Moves the specified condition to the specified location and renumbers the other conditions accordingly.
`show web-auth activation`	Displays whether forcing user authentication is enabled or not.
`show web-auth default-rule`	Displays settings of the default web authentication policy.
`show web-auth exceptional-service`	Displays services that users can access without user authentication.
`show web-auth method`	Displays whether a client is to authenticate with the ZyWALL / USG through the specifically designated web portal when web authentication is enabled.
`show web-auth policy {<1..1024> | all}`	Displays details about the policies for forcing user authentication.
`show web-auth portal status`	Displays the web portal page settings.
`show web-auth status`	Displays the web portal page settings.

28.2.1 web-auth policy Sub-commands

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

Table 103 web-auth policy Sub-commands

COMMAND	DESCRIPTION
`[no] activate`	Activates the specified condition. The no command deactivates the specified condition.
`[no] authentication {force | required}`	Selects the authentication requirement for users when their traffic matches this policy. The no command means user authentication is not required. `force`: Users need to be authenticated and the ZyWALL / USG automatically display the login screen when users who have not logged in yet try to send HTTP traffic. `required`: Users need to be authenticated. They must manually go to the login screen. The ZyWALL / USG will not redirect them to the login screen.
`[no] description` *`description`*	Sets the description for the specified condition. The no command clears the description. *`description`*: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 printable ASCII characters long.
`[no] destination {`*`address_object`*` | `*`group_name`*`}`	Sets the destination criteria for the specified condition. The no command removes the destination criteria, making the condition effective for all destinations.
`[no] force`	Forces users to log in to the ZyWALL / USG if the specified condition is satisfied. The no command means that users do not log in to the ZyWALL / USG.

Table 103 web-auth policy Sub-commands (continued)

COMMAND	DESCRIPTION
`interface` *`interface_name`*	Sets an interface on which packets for the policy must be received.
`[no] schedule` *`schedule_name`*	Sets the time criteria for the specified condition. The no command removes the time criteria, making the condition effective all the time.

`[no] source {`*`address_object`*` |`
`group_name``}`
	Sets the source criteria for the specified condition. The no command removes the source criteria, making the condition effective for all sources.

`[no] sso`	Enables SSO web authentication. The no command disables SSO web authentication.

`show sso { agent | port |`
`presharekey}`
	Displays information about the specified condition.

28.3 SSO Overview

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

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

28.3.1 SSO Configuration Commands

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

Table 104 SSO Commands and Subcommnds

COMMAND	DESCRIPTION
`sso agent primary`	Enters SSO primary agent subcommand mode.
`sso agent secondary`	Enters secondary agent subcommand mode. A secondary agent is an optional backup SSO agent.

`router(config-sso-primary)#`
`router(config-sso-secondary)#`
`[no] ip <w.x.y.z>`
	Sets the primary or ssecondary SSO agent *`ipv4 address.`* Use *`[no]`* to disable the IPv4 address.
	Type the IPv4 address of the SSO agent. The ZyWALL / USG and the SSO agent must be in the same domain and be able to communicate with each other.

`router(config-sso-primary)#`
`router(config-sso-secondary)#`
`[no] port <1025..65535>`
	Sets the primary or ssecondary agent port *`<1025..65535>.`* Use *`[no]`* to disable the port. Type the same port number here as in the **Agent Listening Port** field on the SSO agent. Type a number ranging from 1025 to 65535.

`sso presharekey <preshared key>`	Sets the SSO preshared key. Type 8-32 printable ASCII characters or exactly 32 hex characters (0-9; a-f). The Agent PreShareKey is used to encrypt communications between the ZyWALL / USG and the SSO agent
`sso encrypted-presharekey <ciphertext>`	Sets the SSO encrypted preshared key.
`sso_port <1025..65535>`	Sets the SSO listening port. This port is used to wait for receiving information from Agent. Type a number ranging from 1025 to 65535.

28.3.2 SSO Show Commands

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

Table 105 SSO Show Commands

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

28.3.3 Command Setup Sequence Example

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

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

29

Hotspot

29.1 Hotspot Overview

At the time of writing, the following models support Hotspot management:

- ZyWALL 310
- ZyWALL 1100
- USG310
- USG1100
- USG1900
- USG2200-VPN

29.2 Billing Overview

You can use the built-in billing function to set up billing profiles. A billing profile describes how to charge users. This chapter also shows you how to select an accounting method or configure a discount price plan.

29.3 Billing Commands

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

Table 106 billing Commands

COMMAND	DESCRIPTION
`billing accounting-method {accumulation | time-to-finish }`	Sets how the ZyWALL / USG accounts the time. `accumulation`: to allow each user a one-time login. Once the user logs in, the system starts counting down the pre-defined usage even if the user stops the Internet access before the time period is finished. If a user disconnects and reconnects before the allocated time expires, the user does not have to enter the user name and password to access the Internet again `time-to-finish`: to allow each user multiple re-login until the time allocated is used up. The ZyWALL / USG accounts the time that the user is logged in for Internet access
`billing accumulation idle-detection timeout <1..60>`	Specifies the idle timeout between 1 and 60 minutes. The ZyWALL / USG automatically disconnects a computer from the network after a period of inactivity. The user may need to enter the username and password again before access to the network is allowed.

Table 106 billing Commands (continued)

COMMAND	DESCRIPTION
`billing accumulation-expire {day <1..360> | hour <1..24>}`	Specifies a time unit and number to set how long to wait before the ZyWALL / USG deletes an idle account.
`billing currency {eur | gbp | usd | user-define` *`currency_code`* `}`	Sets the appropriate currency unit. *`currency_code`*: enter a three-letter alphabetic code, such as TWD or JPY.
`billing decimal-places <2>`	Sets the number of decimal places to be used for billing.
`billing decimal-symbol {comma | dot}`	Sets the ZyWALL / USG to use a dot (.) or a comma (,) for the decimal point.
`[no] billing discount activate`	Activates the discount price plan. The no command disables the discount price plan.
`billing discount button {a | b | c} [charge-by-level]`	Specifies a button to assign the base charge. `charge-by-level`: to charge the rate at each successive level from the first level (most expensive per unit) to the highest level (least expensive per unit) that the total purchase reaches.
`[no] billing discount unit <2..10> price` *`price`*	Creates a new discount level by setting the duration of the billing period that should be reached before the ZyWALL / USG charges users at this level and defining this level's charge per time unit. The no command removes this discount level.
`[no] billing profile` *`profile_name`*	Creates a billing profile and enters the `billing profile` sub-command mode to set the price and the duration of the billing period. See Table 107 on page 207 for the sub-commands. The no command removes the specified profile. *`profile_name`*: use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter.
`billing profile rename` *`profile_name profile_name`*	Renames the specified billing profile (first *`profile_name`*) to the specified name (second *`profile_name`*).
`billing tax-rate <0..100>`	Sets the tax rate. For example, type 6 for a 6% sales tax.
`[no] billing tax-rate activate`	Sets the ZyWALL / USG to charge sales tax for the account. The no command sets the ZyWALL / USG to not charge sales tax for the account.
`billing unused-expire {minute <30..60> | hour <1..24> | day <1..365>}`	Specifies a time unit and number to set how long to wait before the ZyWALL / USG deletes an account that has not been used.
`billing username-password-length <4..6>`	Sets how manay characters the username and password of a newly-created dynamic guest account will have.
`[no] billing wlan-ssid-profile` *`profile_name`*	Sets the name of the SSID profile to which you can apply the general billing settings. The no command sets the ZyWALL / USG to not apply the billing settings to the SSID profile.
`show billing discount default rule`	Displays settings of the default discount price plan.
`show billing discount rule`	Displays settings of the custom discount price plan(s).
`show billing discount status`	Displays billing discount settings.
`show billing profile [`*`profile_name`*`]`	Displays settings for all or the specified billing profile.
`show billing status`	Displays the general billing settings, such as the accounting method or tax rate.

29.3.1 Billing Profile Sub-commands

The following table describes the sub-commands for the `billing profile` command.

Table 107 billing profile Sub-commands

COMMAND	DESCRIPTION
`[no] activate`	Enables the billing profile. The no command disables the profile.
`bandwidth {upload | download} <0..1048576> priority <1..7>`	Specifies the maximum bandwidth allowed for the user account in kilobits per second and types a number between 1 and 7 to set the priority for the user's traffic. The smaller the number, the higher the priority. `upload` refers to the traffic the ZyWALL / USG sends out from a user. `download` refers to the traffic the ZyWALL / USG sends to a user.
`[no] bandwidth activate`	Turns on bandwidth management for the user account. The no command disables bandwidth management for the user account.
`price` *`price`*	Defines each profile's price, up to 999999.99, per time unit.
`quota {total | upload | download} megabytes <0..1023>`	Sets how much downstream and/or upstream data in Megabytes can be transmitted through the external interface before the account expires. 0 means there is no data limit for the user account.
`quota {total | upload | download} gigabytes <0..100>`	Sets how much downstream and/or upstream data in Gigabytes can be transmitted through the external interface before the account expires. 0 means there is no data limit for the user account.
`quota type {total | upload-download}`	Sets a limit for the user account. This only applies to user's traffic that is received or transmitted through the external interface. Note: When the limit is exceeded, the user is not allowed to access the Internet through the ZyWALL / USG. `total`: set a limit on the total traffic in both directions. `upload-download`: set a limit on the upstream traffic and downstream traffic respectively.
`time-period {day <1..365> | hour <1..24> | minute <30..60>}`	Sets the duration of the billing period. When this period expires, the user's access will be stopped.

29.3.2 Billing Command Example

This example sets the accounting method to `time-to-finish` and configures the idle timeout that elapses before the ZyWALL / USG disconnects a user.

```
Router# configure terminal
Router(config)# billing accounting-method time-to-finish
Router(config)# billing accumulation idle-detection timeout 30
Router(config)#
```

This example enables and creates a custom discount pricing plan. It uses button A to assign the base charge and also shows the discount status and plan settings.

```
Router# configure terminal
Router(config)# billing discount activate
Router(config)# billing discount button a charge-by-level
Router(config)# billing discount unit 3 price 1.9
Router(config)# show billing discount status
Billing discount status:
  activate: yes
  button: a
  charge_by_level: yes
Router(config)#show billing discount rule
No.  Conditions           Unit            Unit price
===============================================================================
1    when >=              3               eur  1,90
Router(config)#
```

This example creates a billing profile named `billing_1hour` and displays the profile settings.

```
Router# configure terminal
Router(config)# billing profile billing_1hour
Router(billing profile button-a)# activate
Router(billing profile button-a)# price 2
Router(billing profile button-a)# time-period hour 1
Router(billing profile button-a)# exit
Router(config)# show billing profile
Billing Profile: billing_30mins
  activate: yes
  time period: 30 minute
  price: eur 0,00
Billing Profile: billing_1hour
  activate: yes
  time period: 1 hour
  price: eur 2,00
Router(config)#
```

This example applies the billing profile `billing_1hour` to button A of the web-based account generator and button A on a connected statement printer. It also displays the default discount price plan settings, that is, the billing profile settings for button A when it is selected as the button to assign the base charge.

```
Router# configure terminal
Router(config)# printer-manager button a billing_1hour
Router(config)# show billing discount default rule
No.        Conditions           Unit            Unit price
===============================================================================
default    when >=              1               eur  2,00
Router(config)#
```

29.3.3 Payment Service

Use these commands to use a credit card service to authorize, process, and manage credit card transactions directly through the Internet. You must register with the supported credit card service before you can configure the ZyWALL / USG to handle credit card transactions.

This table lists the payment-service commands. You must use the configure terminal command to enter the configuration mode before you can use these commands.

Table 108 payment-service Commands

COMMAND	DESCRIPTION
payment-service provider select *provider*	Selects a payment provider. For example, payment-service provider select *paypal*.
payment-service provider paypal	Enters payment-service sub-command mode for PayPal.
payment-service provider paypal exit	Exits payment-service sub-command mode.
[no] payment-service activate	Activates payment service to use PayPal to authorize credit card payments. The no command disables payment service.
payment-service account-delivery *delivery_method* {deactivate | activate}	Enables or disables how the ZyWALL / USG provides dynamic guest account information after the user's online payment is done. *delivery_method*: type *onscreen* or *sms*. *onscreen* displays the user account information in the web configurator screen. *sms* uses Short Message Service (SMS) to send account information in a text message to the user's mobile device. You should have enabled SMS to send text messages to the user's mobile device.
[no] payment-service page-customization	Enables customization of desktop online payment service pages that displays after an unauthorized user clicks the link in the Web Configurator login screen to purchase access time. The no commands disables customization and uses the default page.
[no] payment-service mobile-page-customization	Enables customization of mobile online payment service pages that displays after an unauthorized user clicks the link in the Web Configurator login screen to purchase access time. The no commands disables customization and uses the default page.
payment-service fail-page failed-message *message*	Creates a message if a desktop payment transaction fails. *message*: The message must be from 1 to 256 characters long and can contain spaces and the following characters ([0-9a-zA-Z '`()+,/ :;=~!*#@$_%-\.\&\?\[\]\{\}*\\|\^\\\<\>\+\"]) The default message is "Sorry! We can't handle your payment transaction at this time."
payment-service mobile-fail-page failed-message *message*	Creates a message if a mobile payment transaction fails. *message*: The message must be from 1 to 256 characters long and can contain spaces and the following characters ([0-9a-zA-Z '`()+,/ :;=~!*#@$_%-\.\&\?\[\]\{\}*\\|\^\\\<\>\+\"]) The default message is "Sorry! We can't handle your payment transaction at this time."
payment-service mobile-profile-page selection-message *message*	Creates a message prompting mobile payment service plan selection. *message*: The message must be from 1 to 256 characters long and can contain spaces and the following characters ([0-9a-zA-Z '`()+,/ :;=~!*#@$_%-\.\&\?\[\]\{\}*\\|\^\\\<\>\+\"]) The default message is "Please choose the service plan from the following profile table."

Table 108 payment-service Commands (continued)

<table>
<tr><th>COMMAND</th><th>DESCRIPTION</th></tr>
<tr><td>payment-service mobile-sms-page info-message message</td><td>Creates a mobile view customized SMS page when a new account is created.
message: The message must be from 1 to 256 characters long and can contain spaces and the following characters ([0-9a-zA-Z '`()+,/ :;=~!*#@$_%-\.\&\?\[\]\{\}*\|\^\\\<\>\+\"])
The default message is “Please check your mobile phone for the account information.”</td></tr>
<tr><td>payment-service mobile-success-page {notification-message | successful-message | notification-message-color {#00FF00 | color_name | rgb(0,0,255)}</td><td>Creates custom colored mobile view messages when a new account is created successfully.
message: The message must be from 1 to 256 characters long and can contain spaces and the following characters ([0-9a-zA-Z '`()+,/ :;=~!*#@$_%-\.\&\?\[\]\{\}*\|\^\\\<\>\+\"])
The default notification-message is “IMPORTANT! Make a note for your case-sensitive username and password for logging later. This will be your only opportunity to do so.”
The default successful-message is “You may now use the Internet.“
notification-message-color: Defines the message color by selecting RGB (0,0,255), or type a color_name such as red, or enter the hex color format (#00FF00).</td></tr>
<tr><td>payment-service profile-page selection-message message</td><td>Creates a message prompting payment service plan selection.
message: The message must be from 1 to 256 characters long and can contain spaces and the following characters ([0-9a-zA-Z '`()+,/ :;=~!*#@$_%-\.\&\?\[\]\{\}*\|\^\\\<\>\+\"])
The default message is “Please choose the service plan from the following profile table.”</td></tr>
<tr><td>payment-service success-page {account-message message | format-date {dd-mm-yyyy | mm-dd-yyyy | yyyy-mm-dd} | notification-message message | notification-message-color {#00FF00 | color_name | rgb(0,0,255)} | successful-message message}</td><td>Creates custom colored, date-formatted desktop view messages when a new account is created successfully.
message: The message must be from 1 to 256 characters long and can contain spaces and the following characters ([0-9a-zA-Z '`()+,/ :;=~!*#@$_%-\.\&\?\[\]\{\}*\|\^\\\<\>\+\"])
The default account-message is ”This is your account information, please keep this for your internet service.”
The default notification-message is “IMPORTANT! Make a note for your case-sensitive username and password for logging later. This will be your only opportunity to do so.”
The default successful-message is “You may now use the Internet.“
notification-message-color: Defines the message color by selecting RGB (0,0,255), or type a color_name such as red, or enter the hex color format (#00FF00).</td></tr>
<tr><td>show payment-service account-delivery</td><td>Displays how the ZyWALL / USG provides dynamic guest account information after the user’s online payment is done (onscreen or sms).</td></tr>
<tr><td>show payment-service check payment-all-currency</td><td>Checks if the billing currency is different from the payment currency configured.</td></tr>
<tr><td>show payment-service activation</td><td>Displays if payment service is active.</td></tr>
<tr><td>show payment-service provider select</td><td>Displays the payment service provider selected.</td></tr>
<tr><td>show payment-service provider paypal</td><td>Displays account, currency, identity token, and payment gateway details of the PayPal payment service provider.</td></tr>
</table>

Table 108 payment-service Commands (continued)

COMMAND	DESCRIPTION
`show payment-service page-customization`	Displays whether customization of desktop online payment service is enabled.
`show payment-service profile-page settings`	Displays the message prompting payment service plan selection
`show payment-service success-page settings`	Displays the settings for messages for when a new account is created successfully.
`show payment-service fail-page settings`	Displays the message for if a desktop payment transaction fails.
`show payment-service sms-page settings`	Displays the SMS message in Desktop View when a new account is created.
`show payment-service mobile-page-customization`	Displays whether customization of mobile online payment service pages that displays after an unauthorized user clicks the link in the Web Configurator login screen to purchase access time, is enabled.
`show payment-service mobile-profile-page settings`	Displays the message prompting mobile payment service plan selection.
`show payment-service mobile-success-page settings`	Displays whether customization for mobile view messages when a new account is created successfully is enabled.
`show payment-service mobile-fail-page settings`	Displays the settings for messages if a mobile payment transaction fails.
`show payment-service mobile-sms-page settings`	Displays the SMS message in Mobile View when a new account is created.

The following table describes the sub-commands for the payment-service command.

Table 109 payment-service paypal Sub-commands

COMMAND	DESCRIPTION
`payment-service provider paypal account` *`e-mail`*	Configures an e-mail address for the PayPal account. *`e-mail`*: type a valid e-mail address for this account
`payment-service provider paypal no account`	Removes the PayPal account.
`payment-service provider paypal currency` *`paypal_currency`*	Defines the currency in which payments are made *`paypal_currency`*: Select the currency that PayPal supports. For example, *`aud, cad, chf, czk, dkk, eur, gbp, hkd, huf, ils, jpy, mxn, nok, nzd, php, pln, sek, sgd, thb, twd, usd`*.
`payment-service provider paypal identity-token` *`paypal_token`*	Defines the PayPal ID token. *`paypal_token`*: Enter the ID token provided to you by PayPal after successfully applying for your PayPal account.
`payment-service provider paypal no identity-token`	Removes the PayPal ID token.
`payment-service provider paypal gateway` *`payment_gw_url`*	Defines the PayPal gateway. *`payment_gw_url`*: Enter the address of the PayPal gateway provided to you by PayPal after applying for your PayPal account.
`payment-service check paypal-currency`	Displays the currency in which PayPal payments are made.

29.4 Printer Manager Overview

You can create dynamic guest accounts and print guest account information by pressing the button on an external statement printer, such as SP350E. Make sure that the printer is connected to the appropriate power and the ZyWALL / USG, and that there is printing paper in the printer. Refer to the printer's documentation for details.

29.5 Printer-manager Commands

This table lists the `printer-manager` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 110 printer-manager Commands

COMMAND	DESCRIPTION
`[no] printer-manager activate`	Allows the ZyWALL / USG to manage and moniter the printer status. The no command disables printer management on the ZyWALL / USG.
`printer-manager discover`	Detects the printer(s) that is connected to the ZyWALL / USG and display the printer information.
`printer-manager button {a | b | c}` *`profile_name`*	Applies the specified billing profile to a button of the web-based account generator and/or the button on a connected statement printer
`[no] printer-manager encrypt activate`	Turns on data encryption. Data transmitted between the ZyWALL / USG and the printer will be encrypted with a secret key. The no command disables data encryption.
`printer-manager encrypt secret-key` *`secret_key`*	Sets a key for data encryption. *`secret_key`*: four alphanumeric characters (A-Z, a-z, 0-9)
`printer-manager multi-printout <1..3>`	Sets how many copies of subscriber statements you want to print (1 is the default).
`printer-manager port <1..65535>`	Sets the number of port on which the ZyWALL / USG sends data to the printer for it to print.
`[no] printer-manager printer <1..10>`	Enters the `printer-manager printer` sub-command mode to configure a printer that can be managed by the ZyWALL / USG. See Table 107 on page 207 for the sub-commands. The no command removes the specified printer from the printer list.
`printer-manager printer append`	Enters the `printer-manager printer` sub-command mode to add a printer to the end of the printer list. See Table 107 on page 207 for the sub-commands.
`printer-manager printout-type {customized | default}`	Sets to use the default account printout format built into the ZyWALL / USG or use a custom account printout format.
`show printer-manager button`	Displays the name of billing profile that is applied to each button.
`show printer-manager discover-printer-status`	Displays information of the printer that is connected to and detected by the ZyWALL / USG.
`show printer-manager printer [<1..10>]`	Displays settings of all or the specified printer that can be managed by the ZyWALL / USG.
`show printer-manager printer-status`	Displays information about the printers that are connected and can be managed by the ZyWALL / USG.

Table 110 printer-manager Commands (continued)

COMMAND	DESCRIPTION
`show printer-manager printerfw version`	Displays the version of the printer firmware currently uploaded to the ZyWALL / USG. The ZyWALL / USG automatically installs it in the connected printers to make sure the printers are upgraded to the same version.
`show printer-manager printout-type`	Displays the current account printout format.
`show printer-manager settings`	Displays the printer management settings.
`show printer-manager workableIP`	Displays the number and IP address(s) of printer(s) that can synchronize with the ZyWALL / USG successfully.

29.5.1 Printer-manager Printer Sub-commands

The following table describes the sub-commands for the `printer-manager printer` command.

Table 111 printer-manager printer Sub-commands

COMMAND	DESCRIPTION
`activate`	Enables the entry.
`deactivate`	Disables the entry.
`description` *`description`*	Sets a descriptive name for the printer.
`printer-ip` *`ipv4_address`*	Sets the IP address of the printer.

29.5.2 Printer-manager Command Example

This example adds a printer to the managed printer list and displays the printer settings.

```
Router# configure terminal
Router(config)# printer-manager printer 1
Router(printer-manager)# activate
Router(printer-manager)# description cafe
Router(printer-manager)# printer-ip 172.16.0.123
Router(printer-manager)# exit
Router(config)# show printer-manager printer
printer: 1
  activate: yes
  IPv4 address: 172.16.0.123
  description:  cafe
Router(config)#
```

29.6 Free Time Overview

With Free Time, the ZyWALL / USG can create dynamic guest accounts that allow users to browse the Internet free of charge for a specified period of time.

29.7 Free-Time Commands

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

Table 112 free-time Commands

COMMAND	DESCRIPTION
`[no] free-time activate`	Turns on the free time feature to allow users to get a free account for Internet surfing during the specified time period. The no command disables the free time feature.
`[no] free-time auto-login`	Allow users to log into their free account directly without having to enter their user name and password. The no command requires users to enter their user name and password, and click login to access their free account.
`[no] free-time deliver-method onscreen`	Sets the ZyWALL / USG to display the user account information in the web screen. The no command sets the ZyWALL / USG to not display the user account information in the web screen.
`[no] free-time deliver-method sms`	Sets the ZyWALL / USG to send account information in an SMS text message to the user’s mobile device. The no command sets the ZyWALL / USG to not send account information in an SMS text message to the user’s mobile device.
`[no] free-time maximum-register-number <1..5>`	Specifies the maximum number of the users that are allowed to log in for Internet access with a free guest account before the time specified using the `free-time reset-register` command. The no command resets the setting to its default value (`1`).
`[no] free-time reset-register` *`hh:mm`*	Sets the time in 24-hour format at which the new free time account is allowed to access the Internet. The no command resets the setting to its default value (`00:00`).
`[no] free-time time-period` *`time_period`*	Sets the duration of time period (in minutes) for which the free time account is allowed to access the Internet. *`time_period`*: x - y, where x and y depend on the ZyWALL / USG model. The no command resets the setting to its default value (`30`).
`show free-time status`	Displays the free time settings.

29.8 Free-Time Commands Example

The following example enables the free time feature and sets the ZyWALL / USG to provide user account information in the web screen and also sent account information via SMS text messages. It then displays the free time settings.

```
Router# configure terminal
Router(config)# free-time activate
Router(config)# free-time deliver-method onscreen
Router(config)# free-time deliver-method sms
Router(config)# show free-time status
Activate: yes
Time Period: 30
Reset Time: 00:00
Maximum registration number before reset time: 1
Delivery Method: onscreen-sms
Router(config)#
```

29.9 SMS Overview

The ZyWALL / USG supports Short Message Service (SMS) to send short text messages to mobile devices. At the time of writing, the ZyWALL / USG uses ViaNett as the SMS gateway to help forward SMS messages. You must already have a Vianett account in order to use the SMS service.

29.10 SMS Commands

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

Table 113 sms-service Commands

COMMAND	DESCRIPTION
`sms-service account-send phone` *phone_number* `account` *user_name* `password` *password*	Specifies the guest account information and the number of mobile device to which you want to send a text message.
`[no] sms-service activate`	Enables the SMS service on the ZyWALL / USG. The no command disabled the SMS service.
`sms-service default-country-code` *country_code*	Sets the default country code for the mobile phone number to which you want to send SMS messages. *country_code*: one to four digits
`sms-service provider vianett`	Enters the `sms-service-vianett` sub-command mode to configure your ViaNett account information.
`[no] password` *password*	Sets the password for your ViaNett account.
`[no] username` *e-mail*	Sets the user name for your ViaNett account.
`sms-service provider-select vianett`	Selects to use ViaNett as the SMS gateway to help forward SMS messages.
`sms-service test-send phone` *phone_number* `msg` *message*	Specifies the mobile phone number and message to test whether the ZyWALL / USG can use SMS to send a text message.

Table 113 sms-service Commands (continued)

COMMAND	DESCRIPTION
`show sms-service`	Displays the SMS settings.
`show sms-service activation`	Displays whether the SMS service is enabled.
`show sms-service default-country-code`	Displays the default country code for the mobile phone number to which you want to send SMS messages.
`show sms-service provider vianett`	Displays the ViaNett account information.

29.11 SMS Commands Example

The following example enables the SMS service on the ZyWALL / USG to provide and configures the ViaNett account information. It then displays the SMS settings.

```
Router# configure terminal
Router(config)# sms-service activate
Router(config)# sms-service provider vianett
Router(sms-service-vianett)# username test@example.com
Router(sms-service-vianett)# password 12345
Router(sms-service-vianett)# exit
Router(config)# show sms-service
enable sms service: yes
SMS Country-Code: 0
SMS Provider-Selected: vianett
SMS Service: Vianett
  username: test@example.com
  password: 12345
Router(config)#
```

29.12 IPnP Overview

IP Plug and Play (IPnP) allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the ZyWALL / USG are not in the same subnet.

When you disable the IPnP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the ZyWALL / USG’s LAN IP address can connect to the ZyWALL / USG or access the Internet through the ZyWALL / USG.

The IPnP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the ZyWALL / USG's IP address.

Note: You must enable NAT to use the IPnP feature.

29.13 IPnP Commands

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

Table 114 ipnp Commands

COMMAND	DESCRIPTION
`[no] ip ipnp activate`	Enables IPnP on the ZyWALL / USG. The no command disables IPnP.
`ip ipnp config`	Enters the IPnP sub-command mode to enable IPnP on specific internal interface(s).
`[no] interface` *`interface_name`*	Enables IPnP on a specific internal interface. The no command disables IPnP for the specified interface.
`show ip ipnp activation`	Displays whether IPnP is enabled on the ZyWALL / USG.
`show ip ipnp interface`	Displays whether IPnP is enabled on an interface.

29.14 IPnP Commands Example

The following example enables IPnP on the ZyWALL / USG and interface lan1. It also displays the IPnP settings.

```
Router# configure terminal
Router(config)# ip ipnp activate
Router(config)# ip ipnp config
Router(ipnp)# interface lan1
Router(ipnp)# exit
Router(config)# show ip ipnp activation
IPnP Status: yes
Router(config)# show ip ipnp interface
interface
===============================================================================
lan1
Router(config)#
```

29.15 Walled Garden Overview

A user must log in before the ZyWALL / USG allows the user’s access to the Internet. However, with a walled garden, you can define one or more web site addresses that all users can access without logging in. These can be used for advertisements for example.

29.16 Walled Garden Commands

This table lists the walled-garden commands. You must use the configure terminal command to enter the configuration mode before you can use these commands.

Table 115 walled-garden Commands

COMMAND	DESCRIPTION
[no] walled-garden activate	Enables the walled garden feature. The no command disables the walled garden feature.
[no] walled-garden rule <1..50>	Creates a walled garden URL link entry (URLs that use the HTTP or HTTPS protocol) for web site that all users are allowed to access without logging in, and enters sub-command mode. See Section Table 116 on page 218 for the rule sub-commands.
walled-garden rule append	Creates a new walled garden URL entry at the end of the current list and enters sub-command mode. See Table 116 on page 218 for the sub-commands.
walled-garden rule flush	Deletes all walled garden URL entries.
walled-garden rule insert <1..50>	Creates a new walled garden URL entry at the specified location, renumbers the other entries accordingly, and enters sub-command mode. See Table 116 on page 218 for the sub-commands.
walled-garden rule move <1..50> to <1..50>	Moves the specified walled garden URL entry to the specified location and renumbers the other entries accordingly.
walled-garden domain-ip rule <1..50>	Creates a walled garden web site link entry, which uses a (wildcard) domain name or an IP address for web site that all users are allowed to access without logging in, and enters sub-command mode. See Section Table 117 on page 219 for the rule sub-commands.
walled-garden domain-ip rule append	Creates a new walled garden domain name or IP address entry at the end of the current list and enters sub-command mode. See Table 117 on page 219 for the sub-commands.
walled-garden domain-ip rule flush	Deletes all walled garden domain name or an IP address entries.
show walled-garden activation	Displays whether the walled garden feature is enabled or not.
show walled-garden rule <1..50>	Displays settings of the specified walled garden URL entry.

29.16.1 walled-garden rule Sub-commands

The following table describes the sub-commands for several walled-garden rule commands. Note that not all rule commands use all the sub-commands listed here.

Table 116 walled-garden rule Sub-commands

COMMAND	DESCRIPTION
[no] activate	Enables this entry. The no command disables the entry.
[no] name *description*	Sets a descriptive name for the walled garden link to be displayed in the login screen. The no command clears the description. *description*: You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter.

Table 116 walled-garden rule Sub-commands (continued)

COMMAND	DESCRIPTION
[no] hidden	Sets the ZyWALL / USG to not display the web site link in the user login screen. This is helpful if a user’s access to a specific web site is required to stay connected but he or she does not need to visit that web site. The no command displays the web site link in the user login screen.
[no] url *url*	Sets the URL or IP address of the web site. Use “http://” followed by up to 262 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%). For example, http://www.example.com or http://172.16.1.35. The no command removes the web site address.

29.16.2 walled-garden domain-ip rule Sub-commands

The following table describes the sub-commands for several `walled-garden domain-ip rule` commands. Note that not all rule commands use all the sub-commands listed here.

Table 117 walled-garden domain-ip rule Sub-commands

COMMAND	DESCRIPTION
[no] activate	Enables this entry. The no command disables the entry.
[no] name *description*	Sets a descriptive name for the walled garden link to be displayed in the login screen. The no command clears the description. *description*: You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter.
[no] type {domain|ip}	Sets the rule type to be a domain name or an IPv4 IP address.
[no] domain-name *walled_garden_fqdn*	Sets a fully qualified name for the domain type rule. *walled_garden_fqdn*: Type a valid fully qualified name for this rule. The no command removes the fully qualified name.
[no] ip-address *<w.x.y.z>/<1..32>*	Sets the IPv4 subnet in CIDR format for the ip type rule. For example, 192.168.1.0/32. The no command removes the web site address.

29.16.3 Walled Garden Command Example

This example shows how to enable the walled garden feature and insert a walled garden link rule at position 1 of the checking order. This example also displays the rule settings. The link rule uses the following settings:

- Activate: yes
- Name: Example1

- URL: www.example.com

```
Router# configure terminal
Router(config)# walled-garden activate
Router(config)# walled-garden rule insert 1
Router(walled-garden)# activate
Router(walled-garden)# name Example1
Router(walled-garden)# url http://www.example.com
Router(walled-garden)# exit
Router(config)# show walled-garden
walled garden rule: 1
  active: yes
  url: http://www.example.com
  name: Example1
Router(config)#
```

29.17 Advertisement Overview

You can set the ZyWALL / USG to display an advertisement web page as the first web page whenever the user connects to the Internet.

29.18 Advertisement Commands

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

Table 118 advertisement Commands

COMMAND	DESCRIPTION
`[no] advertisement activate`	Enables the advertisement feature. The no command disables the advertisement feature.
`advertisement flush`	Deletes all advertisement rules.
`[no] advertisement name` *`description`* `url` *`url`*	Sets a descriptive name for the advertisement web page and enters the web site address to create a new rule. The no command removes the advertisement rule. *`description`*: You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter. *`url`*: the URL or IP address of the web site. Use “http://” followed by up to 262 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%). For example, http://www.example.com or http://172.16.1.35.
`advertisement rename` *`description_old description_new`*	Gives an existing rule a new name.
`show advertisement`	Displays settings of advertisement rule(s).
`show advertisement activation`	Displays whether the advertisement feature is enabled or not.

29.18.1 Advertisement Command Example

This example shows how to set an advertisement rule and displays the rule settings.

```
Router# configure terminal
Router(config)# advertisement activate
Router(config)# advertisement name example url http://www.example.com
Router(config)# show advertisement
advertisement rule: 1
  name: example
  url: http://www.example.com
Router(config)#
```

30

RTLS

30.1 RTLS Overview

Ekahau RTLS (Real Time Location Service) tracks battery-powered Wi-Fi tags attached to APs managed by the ZyWALL / USG to create maps, alerts, and reports.

The Ekahau RTLS Controller is the centerpiece of the RTLS system. This server software runs on a Windows computer to track and locate Ekahau tags from Wi-Fi signal strength measurements. Use the ZyWALL / USG with the Ekahau RTLS system to take signal strength measurements at the APs (Integrated Approach / Blink Mode).

You need:

- At least three APs managed by the ZyWALL / USG (the more APs the better since it increases the amount of information the Ekahau RTLS Controller has for calculating the location of the tags)
- IP addresses for the Ekahau Wi-Fi tags
- A dedicated RTLS SSID is recommended
- Ekahau RTLS Controller in blink mode with TZSP Updater enabled
- Secure policies to allow RTLS traffic if the ZyWALL / USG Secure Policy control is enabled or the Ekahau RTLS Controller is behind a firewall.

For example, if the Ekahau RTLS Controller is behind a firewall, open ports 8550, 8553, and 8569 to allow traffic the APs send to reach the Ekahau RTLS Controller.

The following table lists default port numbers and types of packets RTLS uses.

Table 119 RTLS Traffic Port Numbers

PORT NUMBER	TYPE	DESCRIPTION
8548	TCP	Ekahau T201 location update.
8549	UDP	Ekahau T201 location update.
8550	TCP	Ekahau T201 tag maintenance protocol and Ekahau RTLS Controller user interface.
8552	UDP	Ekahau Location Protocol
8553	UDP	Ekahau Maintenance Protocol
8554	UDP	Ekahau T301 firmware update.
8560	TCP	Ekahau Vision web interface
8562	UDP	Ekahau T301W firmware update.
8569	UDP	Ekahau TZSP Listener Port

30.1.1 RTLS Configuration Commands

Use these commands to configure RTLS on the ZyWALL / USG.

Table 120 RTLS Commands

COMMAND	DESCRIPTION
[no] rtls ekahau activate	Enables RTLS to use Wi-Fi to track the location of Ekahau Wi-Fi tags. The no command disables tracking.
rtls ekahau ip address *<ip>*	Specifies the IP address of the Ekahau RTLS Controller.
rtls ekahau ip port *<1..65535>*	Specifies the server port of the Ekahau RTLS Controller.
show rtls ekahau config	Displays RTLS configuration details.
show rtls ekahau cli	Displays commands run on the AP. The AP runs the flush command before executing other commands.

30.1.2 RTLS Configuration Examples

The following commands show how to enable RTLS to use Wi-Fi to track the location of Ekahau Wi-Fi tags, specify the IP address of the Ekahau RTLS Controller and then show the configuration settings.

```
Router# configure terminal
Router(config)# rtls ekahau activate
Router(config)# rtls ekahau ip address 1.1.1.1
Router(config)# exit
Router# show rtls ekahau config
ekahau activate: yes
ekahau address: 1.1.1.1
ekahau port: 8569
Router#
```

The following command displays the commands run on the AP.

```
Router(config)# show rtls ekahau cli
!
rtls ekahau flush
!
rtls ekahau ip port 11111
rtls ekahau ip address 1.1.1.1
rtls ekahau activate
!
Router(config)#
```

IPSec VPN

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

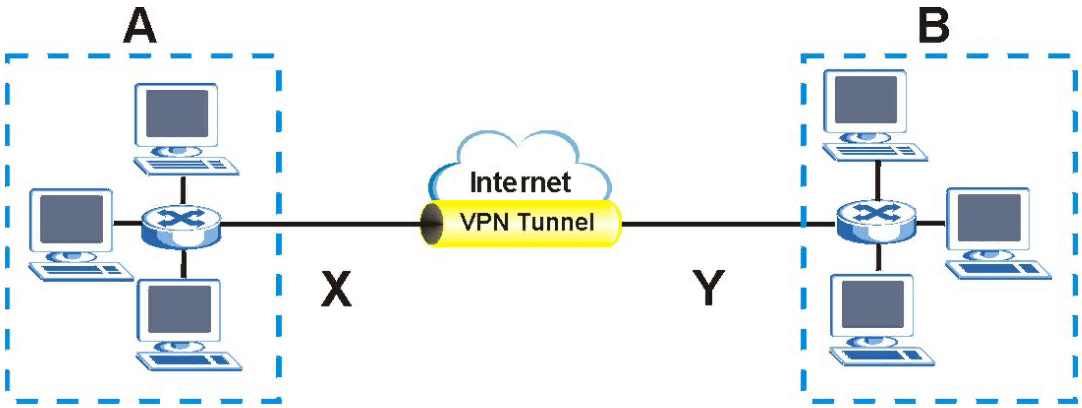
31.1 IPSec VPN Overview

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

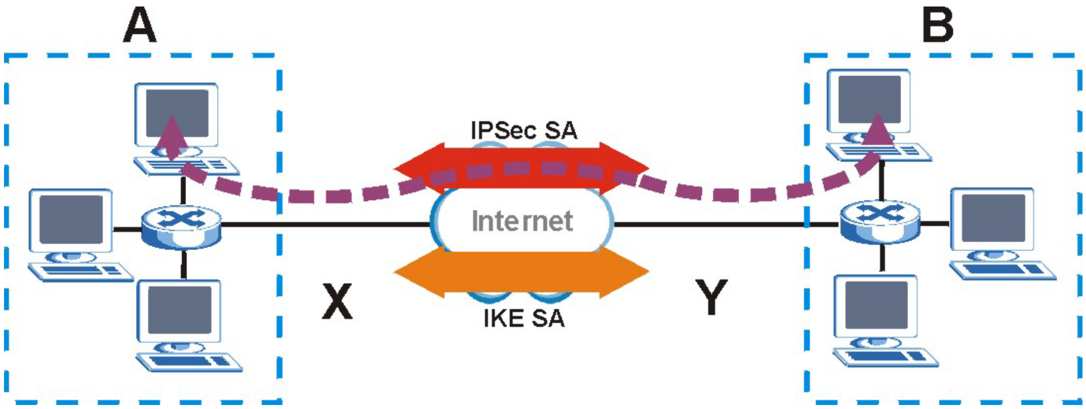


The VPN tunnel connects the ZyWALL / USG (**X**) and the remote IPSec router (**Y**). These routers then connect the local network (**A**) and remote network (**B**).

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

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

Figure 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.

31.2 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 121 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.
distinguished_name	A domain name. You can use up to 511 alphanumeric, characters, spaces, or .@=,_- characters.

Table 121 Input Values for IPSec VPN Commands (continued)

LABEL	DESCRIPTION
sort_order	Sort the list of currently connected SAs by one of the following classifications. algorithm encapsulation inbound name outbound policy timeout uptime
auth_method	The name of the authentication profile.

The following sections list the IPSec VPN commands.

31.2.1 IPv4 IKEv1 SA Commands

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

Table 122 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.
[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 | user-base-psk }	Specifies whether to use a pre-shared key, a certificate, or a user-based pre-shared key 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.
dpd-interval <15..60>	Sets the Dead Peer Detection (DPD) period.
[no] fall-back	Set this to have the ZyWALL / USG reconnect to the primary address when it becomes available again and stop using the secondary connection, if the connection to the primary address goes down and the ZyWALL / USG changes to using the secondary connection. Users will lose their VPN connection briefly while the ZyWALL / USG changes back to the primary connection. To use this, the peer device at the secondary address cannot be set to use a nailed-up VPN connection.
fall-back-check-interval <60..86400>	Sets how often (in seconds) the ZyWALL / USG checks if the primary address is available.
mode {main | aggressive}	Sets the negotiating mode.
transform-set isakmp-algo [isakmp_algo [*isakmp_algo*]]	Sets the encryption and authentication algorithms for each IKE SA proposal. *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 122 isakmp Commands: IKE SAs (continued)

COMMAND	DESCRIPTION
group1 group2 group5 group14	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.
xauth type {server *auth_method* [user-id {*username* | any}] | client name *username* password *password*} [deactivate]	Enables extended authentication and specifies whether the ZyWALL / USG is the server or client. If the ZyWALL / USG is the server, it also specifies the extended authentication method (aaa authentication *profile_name*); if the ZyWALL / USG is the client, it also specifies the username and password to provide to the remote IPSec router. The deactivate command disables extended authentication. *auth_method:* The name of the authentication profile the VPN configuration provisioning service uses to authenticate users. user-id: A user or user group allowed to use the IKE SA. any allows any user with a valid user account and password on the ZyWALL / USG to use the IKE SA. *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*).

31.2.2 IPv4 IPSec SA Commands (except Manual Keys)

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

Table 123 crypto Commands: IPSec SAs

COMMAND	DESCRIPTION
`[no] crypto ignore-df-bit`	Fragment packets larger than the MTU (Maximum Transmission Unit) that have the "don't" fragment" bit in the header turned on. The no command has the ZyWALL / USG drop packets larger than the MTU that have the "don't" fragment" bit in the header turned on.
`show crypto map [`*map_name*`]`	Shows the specified IPSec SA or all IPSec SAs.
`crypto map dial` *map_name*	Dials the specified IPSec SA manually. This command does not work for IPSec SAs using manual keys or for IPSec SAs where the remote gateway address is 0.0.0.0.
`[no] crypto map` *map_name*	Creates the specified IPSec SA if necessary and enters sub-command mode. The no command deletes the specified IPSec SA.
`crypto map rename` *map_name map_name*	Renames the specified IPSec SA (first *map_name*) to the specified name (second *map_name*).
`crypto map` *map_name*	
`activate` `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

Table 123 crypto Commands: IPSec SAs (continued)

COMMAND	DESCRIPTION
`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 / USG 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`: Connects to an IPSec server. This ZyWALL / USG is the client (dial-in user) and can initiate the VPN tunnel. `vpn-tunnel-interface`: Sets up a VPN tunnel interface to bind with a VPN connection. The ZyWALL / USG can use the interface to do load balancing using a specific Trunk. The remote IPsec router should have a static IP address or a domain name.
`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.
`[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.

Table 123 crypto Commands: IPSec SAs (continued)

COMMAND	DESCRIPTION
`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).
`[no] configuration-payload-provide activate`	Enables configuration payload in server role. The no command disables it.
`configuration-payload-provide address-pool {POOL}`	Sets configuration payload address pool. The no command disables it
`[no] configuration-payload-provide {first-dns IPv6|second-dns IPv6}`	Sets configuration payload address pool dns server. The no command disables it
`[no] narrowed`	Enables policy narrowed. The no command disables it.
`[no] protocol gre`	Enables GRE over IPSec to allow traffic using the Generic Routing Encapsulation (GRE) tunneling protocol through an IPSec tunnel. The no `protocol` command disables it.
`mode-config activate`	Allows the IPSec VPN client to receive an IP address, DNS and WINS information from the ZyWALL / USG when the scenario is Remote Access (Server Role) and VPN Gateway uses IKEv1. `remote-access-server` allows incoming connections from IPSec VPN clients with dynamic IP addresses.
`mode-config address-pool` *profile_name*	Sets the IP address pool to be included in the VPN setup data. *profile_name*: an address or address group object
`[no] mode-config {first-dns | second-dns}`	Specifies the DNS server IP address to assign to the remote users. The `second-dns` server's IP address is checked if `first-dns` is unavailable. The no command removes the setting.
`[no] mode-config {first-wins | second-wins}`	Sets the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the remote users. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. The `second-wins` server's IP address is checked if `first-wins` is unavailable. The no command removes the setting.

31.2.3 IPv4 IPSec SA Commands (for Manual Keys)

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

Table 124 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 / USG automatically ignores any characters above the minimum number of characters required by the algorithm. For example, if you enter 1234567890XYZ for a DES encryption key, the ZyWALL / USG only uses 12345678. The ZyWALL / USG still stores the longer key.
local-ip *ip*	Sets the local gateway address to the specified IP address.
peer-ip *ip*	Sets the remote gateway address to the specified IP address.

31.2.4 VPN Concentrator Commands

This table lists the commands for the VPN concentrator.

Table 125 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 125 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`*).

31.2.5 VPN Configuration Provisioning Commands

This table lists the commands for VPN configuration provisioning.

Table 126 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 / USG’s maximum number of VPN connection rules.
`[no] activate`	Turns the VPN configuration provisioning rule on or off.
`crypto` *`map_name`*	Specifies the name of the IPSec VPN connection (*`map_name`*) to bind to this VPN configuration provisioning rule’s user or group.
`user` *`username`*	Specifies a user or group of users allowed to use the ZyWALL / USG IPSec VPN client to retrieve the associated VPN rule settings. A user may belong to a number of groups. If VPN configuration provisioning rules are configured for different groups, the ZyWALL / USG will allow VPN rule setting retrieval based on the first match found. Admin or limited-admin users are not allowed.
`no user`	Removes the VPN configuration provisioning rule’s user or user group configuration. In other words, any users can match the rule. In the GUI “any” will display in the **Allowed User** field.
`exit`	Leaves 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.
`show vcp allowed users`	Displays available users who can be configured as allowed users (using user *`username`*) of a VPN Configuration Provision (VCP) rule.
`show vcp allowed crypto map`	Displays IPv4 VPN Connection rules which can be used in a VPN Configuration Provision (VCP) rule. Nothing displays if no suitable rules are available.
`show vcp allowed crypto map6`	Displays IPv6 VPN Connection rules which can be used in a VPN Configuration Provision (VCP) rule. Nothing displays if no suitable rules are available.

31.2.6 SA Monitor Commands

This table lists the commands for the SA monitor.

Table 127 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 / USG check the beginning and end and ignore the middle. For example, with "abc*123", any VPN connection or policy name starting with "abc" and ending in "123" matches, no matter how many characters are in between. The whole VPN connection or policy name has to match if you do not use a question mark or asterisk. See Table 121 on page 226 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.

31.2.7 IPv4 IKEv2 SA Commands

This table lists the commands for the IPv4 IKEv2 SA.

Table 128 sa Commands: IPv4 IKEv2

COMMAND	DESCRIPTION
show ikev2 policy [*policy_name*]	Shows the specified IKEv2 SA or all IKEv2 SAs.
[no] ikev2 policy *policy_name*	Creates the specified IKEv2 SA if necessary and enters sub-command mode. The no command deletes the specified IKEv2 SA.
activate deactivate	Activates or deactivates the specified IKEv2 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.

Table 128 sa Commands: IPv4 IKEv2 (continued)

COMMAND	DESCRIPTION
`[no] fall-back`	Set this to have the ZyWALL / USG reconnect to the primary address when it becomes available again and stop using the secondary connection, if the connection to the primary address goes down and the ZyWALL / USG changes to using the secondary connection. Users will lose their VPN connection briefly while the ZyWALL / USG changes back to the primary connection. To use this, the peer device at the secondary address cannot be set to use a nailed-up VPN connection.
`fall-back-check-interval <60..86400>`	Sets how often (in seconds) the ZyWALL / USG checks if the primary address is available.
`transform-set isakmp-algo [isakmp_algo [isakmp_algo]]`	Sets the encryption and authentication algorithms for each IKEv2 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 IKEv2 SA life time to the specified value.

`group1`
`group2`
`group5`
`group14`
`group15`
`group16`
`group17`
`group18`
	Sets the DH group to the specified group.

`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.
`eap auth_method AUTH_METHOD`	Sets auth method for EAP. Default value is `Mschapv2`.
`[no] eap type {server AAA_method user-id {name|any}| client name username {password PASSWORD| encrypted-password PASSWORD}`	Enables extended authentication and specifies whether the ZyWALL/ USG is the server or client. If the ZyWALL / USG is the server, it also specifies the AAA authentication method (aaa authentication profile_name); if the ZyWALL / USG is the client, it also specifies the username and password to provide to the remote IPSec router. The no command disables extended authentication. • 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.
`ikev2 policy rename policy_name policy_name`	Renames the specified IKEv2 SA (first policy_name) to the specified name (second policy_name).

31.2.8 IPv6 IKEv2 SA Commands

This table lists the commands for the IPv4 IKEv2 SA.

Table 129 sa Commands: IPv6 IKEv2

COMMAND	DESCRIPTION
show ikev2 policy6 [*policy_name*]	Shows the specified IKEv2 SA or all IKEv2 SAs.
[no] ikev2 policy6 *policy_name*	Creates the specified IKEv2 SA if necessary and enters sub-command mode. The no command deletes the specified IKEv2 SA.
activate deactivate	Activates or deactivates the specified IKEv2 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] fall-back	Set this to have the ZyWALL / USG reconnect to the primary address when it becomes available again and stop using the secondary connection, if the connection to the primary address goes down and the ZyWALL / USG changes to using the secondary connection. Users will lose their VPN connection briefly while the ZyWALL / USG changes back to the primary connection. To use this, the peer device at the secondary address cannot be set to use a nailed-up VPN connection.
fall-back-check-interval <60..86400>	Sets how often (in seconds) the ZyWALL / USG checks if the primary address is available.
transform-set isakmp-algo [isakmp_algo [isakmp_algo]]	Sets the encryption and authentication algorithms for each IKEv2 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 IKEv2 SA life time to the specified value.
group1 group2 group5	Sets the DH group to the specified group.
local-ip {ip IPv6}	Sets the local gateway address to the specified IP address.
peer-ip {ip IPv6]	Sets the remote gateway address(es) to the specified IP address(es).
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 IPv6 | 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 IPv6 | 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.
eap auth_method *auth_method*	Sets auth method for EAP. Default value is Mschapv2.

Table 129 sa Commands: IPv6 IKEv2 (continued)

COMMAND	DESCRIPTION
`[no] eap type {server` *auth_method* `user-id {name|any}| client name username {password PASSWORD| encrypted-password` *password*`}`	Enables extended authentication and specifies whether the ZyWALL/ USG is the server or client. If the ZyWALL / USG is the server, it also specifies the AAA authentication method (aaa authentication profile_name); if the ZyWALL / USG is the client, it also specifies the username and password to provide to the remote IPSec router. The no command disables extended authentication. • *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.
`ikev2 policy rename policy_name policy_name`	Renames the specified IKEv2 SA (first policy_name) to the specified name (second policy_name).

31.2.9 IPv6 IPSec SA Commands

This table lists the commands for IPv6 IPSec SAs.

Table 130 crypto Commands: IPv6 IPSec SAs

COMMAND	DESCRIPTION
`show crypto map6 [`*map_name*`]`	Shows the specified IPSec SA or all IPSec SAs.
`crypto map6 dial` *map_name*	Dials the specified IPSec SA manually. This command does not work for IPSec SAs using manual keys or for IPSec SAs where the remote gateway address is 0.0.0.0.
`[no] crypto map` *map_name*	Creates the specified IPSec SA if necessary and enters sub-command mode. The no command deletes the specified IPSec SA.
`crypto map rename` *map_name map_name*	Renames the specified IPSec SA (first *map_name*) to the specified name (second *map_name*).
`crypto map` *map_name*	
`activate` `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

Table 130 crypto Commands: IPv6 IPSec SAs (continued)

COMMAND	DESCRIPTION
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 / USG 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 / USG is the client (dial-in user) and can initiate the VPN tunnel.
set security-association lifetime seconds <180..3000000>	Sets the IPSec SA life time.
set pfs {group1 | group2 | group5 | none}	Enables Perfect Forward Secrecy group.
local-policy *address_name*	Sets the address object for the local policy (local network).
remote-policy *address_name*	Sets the address object for the remote policy (remote network).
[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.
[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] configuration-payload-provide activate	Enables configuration payload in server role. The no command disables it.
configuration-payload-provide address-pool {POOL}	Sets configuration payload address pool. The no command disables it
[no] configuration-payload-provide {first-dns IPv6|second-dns IPv6}	Sets configuration payload address pool dns server. The no command disables it
[no] narrowed	Enables policy narrowed. The no command disables it

31.2.10 IPv6 VPN Concentrator Commands

This table lists the commands for the IPv6 VPN concentrator.

Table 131 vpn-concentrator Commands: VPN Concentrator

COMMAND	DESCRIPTION
show vpn-concentrator6 [*profile_name*]	Shows the specified IPv6 VPN concentrator or all IPv6 VPN concentrators.
[no] vpn-concentrator6 *profile_name*	Creates the specified IPv6 VPN concentrator if necessary and enters sub-command mode. The no command deletes the specified IPv6 VPN concentrator.

Table 131 vpn-concentrator Commands: VPN Concentrator (continued)

COMMAND	DESCRIPTION
[no] crypto *map_name*	Adds the specified IPSec SA to the specified IPv6 VPN concentrator. The no command removes the specified IPSec SA from the specified IPv6 VPN concentrator.
vpn-concentrator6 rename *profile_name* *profile_name*	Renames the specified IPv6 VPN concentrator (first *profile_name*) to the specified name (second *profile_name*).

32

SSL VPN

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

32.1 SSL Access Policy

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

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

32.1.1 SSL Application Objects

SSL application objects specify an application type and server that users are allowed to access through an SSL tunnel. See Chapter 52 on page 355 for how to configure SSL application objects.

32.1.2 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.

32.2 SSL VPN Commands

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

Table 132 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.
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 SSL VPN commands.

32.2.1 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 133 SSL VPN Commands

COMMAND	DESCRIPTION
`show sslvpn policy [`*`profile_name`*`]`	Displays the settings of the specified SSL VPN access policy.
`show ssl-vpn network-extension local-ip`	Displays the IP address that the ZyWALL / USG uses in setting up the SSL VPN.
`show sslvpn monitor`	Displays a list of the users who are currently logged into the VPN SSL client portal.
`sslvpn network-extension local-ip` *`ip`*	Sets the IP address that the ZyWALL / USG uses in setting up the SSL VPN.
`sslvpn policy {`*`profile_name`*` | `*`profile_name`*` append | `*`profile_name`*` insert <1..16>}`	Enters the SSL VPN sub-command mode to add or edit an SSL VPN access policy.
`[no] activate`	Turns the SSL VPN access policy on or off.
`[no] application` *`application_object`*	Adds the SSL application object to the SSL VPN access policy.
`[no] description` *`description`*	Adds information about the SSL VPN access policy. Use up to 60 characters (“0-9”, “a-z”, “A-Z”, “-” and “_”).
`[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] network-extension netbios-broadcast`	Allows netbios broadcast packets to pass through the SSL VPN tunnel.
`[no] user` *`user_name`*	Specifies the user or user group that can use the SSL VPN access policy.
`sslvpn policy move <1..16> to <1..16>`	Moves the specified SSL VPN access policy to the number that you specified.
`sslvpn no connection username` *`user_name`*	Terminates the user’s SSL VPN connection and deletes corresponding session information from the ZyWALL / USG.
`no sslvpn policy` *`profile_name`*	Deletes the specified SSL VPN access policy.
`sslvpn policy rename` *`profile_name profile_name`*	Renames the specified SSL VPN access policy.
`show workspace application`	Displays the SSLVPN resources available to each user when logged into SSLVPN.
`show workspace cifs`	Displays the shared folders available to each user when logged into SSLVPN.

32.2.2 Setting an SSL VPN Rule Tutorial

Here is an example SSL VPN configuration. The SSL VPN rule defines:

- Only users using the “tester” account can use the SSL VPN.
- The ZyWALL / USG will assign an IP address from 192.168.100.1 to 192.168.100.10 (defined in object “IP-POOL”) to the computers which match the rule’s criteria.
- The ZyWALL / USG will assign two DNS server settings (172.16.1.1 and 172.16.1.2 defined in objects DNS1 and DNS2) to the computers which match the rule’s criteria.
- The SSL VPN users are allowed to access the ZyWALL / USG’s local network, 172.16.10.0/24 (defined in object “Network1”).

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 the SSL VPN user account named tester with password 1234.

```
Router(config)# username tester password 1234 user-type user
```

4 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)# exit
```

5 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
  traffic enforcement:no
  netbios broadcast: no
  ip pool: IP-POOL
  dns server 1: DNS1
  dns server 2: DNS2
  wins server 1: none
  wins server 2: none
  network: NETWORK1

  reference count: 0
```

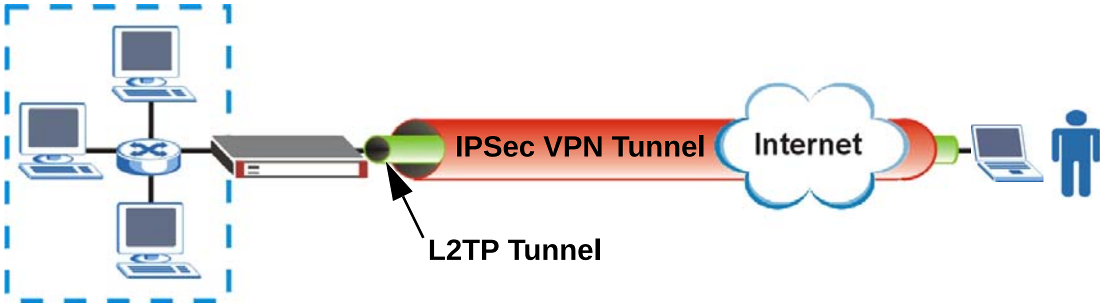
L2TP VPN

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

33.1 L2TP VPN Overview

L2TP VPN lets remote users use the L2TP and IPSec client software included with their computers' operating systems to securely connect to the network behind the ZyWALL / USG. The remote users do not need their own IPSec gateways or VPN client software.

Figure 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 31 on page 225 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).

33.2 IPSec Configuration

You must configure an IPSec VPN connection for L2TP VPN to use (see Chapter 31 on page 225 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.

33.2.1 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.

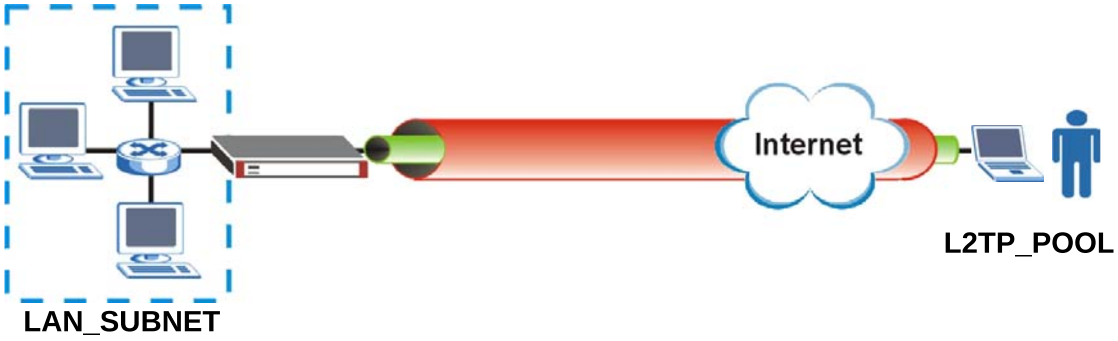
- Configure the **My Address** setting according to your requirements.
- Replace the default **Pre-Shared Key**.

33.3 Policy Route

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

- Set the policy route's **Source Address** to the address object that you want to allow the remote users to access (**LAN_SUBNET** in the following figure).
- Set the **Destination Address** to the IP address pool that the ZyWALL / USG assigns to the remote users (**L2TP_POOL** in the following figure).

Figure 22 Policy Route for L2TP VPN



33.4 L2TP VPN Commands

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

Table 134 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 some ZyWALL / USG models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model. For other ZyWALL / USG models, use a name such as wan1, wan2, opt, lan1, 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 / USG model supports.
ppp_interface	PPPoE/PPTP interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your ZyWALL / USG model supports.
map_name	The name of an IPSec SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
user_name	The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
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.
profile_name	The name of an L2TP VPN account. 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.

33.4.1 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 135 L2TP VPN Commands

COMMAND	DESCRIPTION
`l2tp-over-ipsec recover default-ipsec-policy`	If the default L2TP IPSec policy has been deleted, use this command to recreate it (with the default settings).
`[no] l2tp-over-ipsec activate;`	Turns L2TP VPN on. The no command turns it off.
`l2tp-over-ipsec crypto` *`map_name`*	Specifies the IPSec VPN connection the ZyWALL / USG uses for L2TP VPN. It must meet the requirements listed in Section 33.2 on page 245. Note: Modifying this VPN connection (or the VPN gateway that it uses) disconnects any existing L2TP VPN sessions.
`l2tp-over-ipsec pool` *`address-object`*	Specifies the address object that defines the pool of IP addresses that the ZyWALL / USG uses to assign to the L2TP VPN clients.

Table 135 L2TP VPN Commands

COMMAND	DESCRIPTION
`l2tp-over-ipsec authentication` *authentication profile_name*	Specifies how the ZyWALL / USG authenticates a remote user before allowing access to the L2TP VPN tunnel. The authentication method has the ZyWALL / USG check a user's user name and password against the ZyWALL / USG's local database, a remote LDAP, RADIUS, a Active Directory server, or more than one of these.
`certificate` *cert_name*	Select the certificate to use to identify the ZyWALL / USG for L2TP VPN connections. The certificate is used with the EAP, PEAP, and MSCHAPv2 authentication protocols. The certificate must already be configured.
`[no] l2tp-over-ipsec user user_name`	Specifies the user or user group that can use the L2TP VPN tunnel. If you do not configure this, any user with a valid account and password on the ZyWALL / USG to log in. The no command removes the user name setting.
`[no] l2tp-over-ipsec keepalive-timer <1..180>`	The ZyWALL / USG sends a Hello message after waiting this long without receiving any traffic from the remote user. The ZyWALL / USG disconnects the VPN tunnel if the remote user does not respond. The no command returns the default setting.
`[no] l2tp-over-ipsec first-dns-server {`*ip* `|` *interface_name*`}{1st-dns|2nd-dns|3rd-dns}|{`*ppp_interface*`}{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*`}{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.

33.4.2 L2TP Account Commands

This table lists the commands to create, remove, display and bind L2TP VPN accounts. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

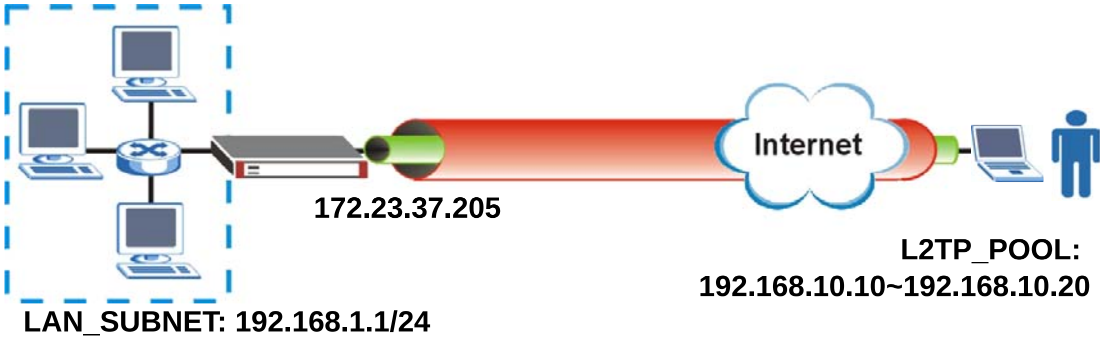
Table 136 L2TP VPN Commands

COMMAND	DESCRIPTION
`[no] account l2tp` *`profile_name`*	Creates an L2TP account and enters sub-command mode.
`authentication {chap	chap-pap	mschap	mschap-v2	pap}`	Selects how the ZyWALL / USG authenticates a remote user before allowing access to the L2TP VPN tunnel. PAP (Password Authentication Protocol) is more readily available than CHAP (Challenge Handshake Authentication Protocol), but CHAP is more secure than PAP. • `chap-pap` - Your ZyWALL / USG accepts either CHAP or PAP when requested by this remote node. • `chap` - Your ZyWALL / USG accepts CHAP only. • `pap` - Your ZyWALL / USG accepts PAP only. • `mschap` - Your ZyWALL / USG accepts MSCHAP only. • `mschap-v2` - Your ZyWALL / USG accepts MSCHAP-V2 only.
`encrypted-password` *`ciphertext`*	Sets the password to encrypt L2TP traffic. *`ciphertext`*: The encryption password.
`idle <0..360>`	Specifies the number of seconds (0 to 360) that must elapse without traffic before the ZyWALL / USG automatically disconnects the L2TP tunnel. 0 (zero) means the timeout is disabled.
`password` *`isp_account_password`*	Sets the password given by the ISP for this account. *`isp_account_password`*: Password as given by ISP.
`server {`*`domain_name`*`	`*`w.x.y.z`*`}`	Specifies the fully-qualified domain name (*`domain_name`*) or IP address for the ISP account.
`user` *`isp_account_username`*	Displays the activity log for the specified user. *`isp_account_username`*: User name as given by ISP.
`show account l2tp [`*`profile_name`*`]`	Displays above details of all L2TP accounts or the one specified.
`Interface` *`interface_name`*	Specifies a PPP interface (see Section 14.2 on page 97) and enters that interface sub-command mode to bind an L2TP account to it.
`account` *`profile_name`*	Specifies the L2TP account to bind to this interface.
`local-address` *`w.x.y.z`*	Specifies the IP address of this interface.
`Interface disconnect`	Disconnects the L2TP tunnel on this interface.
`Interface dial wan1_ppp`	Connects the L2TP tunnel on this interface.
`show interface ppp`	Displays details of each PPP interface connection.

33.5 L2TP VPN Examples

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 / USG has a static IP address of 172.23.37.205 for the ge3 interface.
- The remote user has a dynamic public IP address and connects through the Internet.
- You configure an IP address pool object named **L2TP_POOL** to assign the remote users IP addresses from 192.168.10.10 to 192.168.10.20 for use in the L2TP VPN tunnel.
- The VPN rule allows the remote user to access the **LAN_SUBNET** which covers the 192.168.1.1/ 24 subnet.

33.5.1 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)#
```

33.5.2 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)#
```

33.5.3 Configuring the L2TP VPN Settings Example

The following commands configure and display the L2TP VPN settings.

- Set it to use the **Default_L2TP_VPN_Connection** VPN connection.
- Configure an IP address pool for the range of 192.168.10.10 to 192.168.10.20. In this example it is already created and called **L2TP_POOL**.
- This example uses the default authentication method (the ZyWALL / USG's local user data base).
- Select a user or group of users that can use the tunnel. Here a user account named **L2TP-test** has been created.
- The other settings are left to the defaults in this example.
- Enable the connection.

```
Router(config)# l2tp-over-ipsec crypto Default_L2TP_VPN_Connection
Router(config)# l2tp-over-ipsec pool L2TP_POOL
Router(config)# l2tp-over-ipsec authentication default
Router(config)# l2tp-over-ipsec user L2TP-test
Router(config)# l2tp-over-ipsec activate
Router(config)# show l2tp-over-ipsec
L2TP over IPSec:
  activate          : yes
  crypto            : Default_L2TP_VPN_Connection
  address pool      : L2TP_POOL
  authentication    : default
  user              : L2TP-test
  keepalive timer   : 60
  first dns server  : aux 1st-dns
  second dns server : aux 1st-dns
  first wins server :
  second wins server:
```

33.5.4 Configuring the Policy Route for L2TP Example

The following commands configure and display the policy route for the L2TP VPN connection entry.

- Set the policy route's **Source Address** to the address object that you want to allow the remote users to access (**LAN_SUBNET** in this example).
- Set the **Destination Address** to the IP address pool that the ZyWALL / USG assigns to the remote users (**L2TP_POOL** in this example).
- Set the next hop to be the **Default_L2TP_VPN_Connection** tunnel.

- Enable the policy route.

```
Router(config)# policy 3
Router(policy-route)# source LAN_SUBNET
Router(policy-route)# destination L2TP_POOL
Router(policy-route)# service any
Router(policy-route)# next-hop tunnel Default_L2TP_VPN_ConnectionRouter(policy-
route)# no deactivate
Router(policy-route)# exit
Router(config)# show policy-route 3
index: 3
  active: yes
  description: WIZ_VPN
  user: any
  schedule: none
  interface: ge1
  tunnel: none
  sslvpn: none
  source: PC_SUBNET
  destination: L2TP_POOL
  service: any
  nexthop type: Tunnel
  nexthop: Default_L2TP_VPN_Connection
  bandwidth: 0
  bandwidth priority: 0
  maximize bandwidth usage: no
  SNAT: none
  amount of port trigger: 0
```

34

Bandwidth Management

34.1 Bandwidth Management Overview

Bandwidth management provides a convenient way to manage the use of various services on the network. It manages general protocols (for example, HTTP and FTP) and applies traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

34.1.1 BWM Type

The ZyWALL / USG supports two types of bandwidth management: **shared**, **per-user** and **per-source-ip**.

The **shared** BWM type is selected by default in a bandwidth management rule. All users to which the rule is applied need to share the bandwidth configured in the rule. If the BWM type is set to **per-user** in a rule, every user that matches the rule can use up to the configured bandwidth by his/her own. Set the BWM type set to **per-source-ip** in a rule,when you want to set the maximum bandwidth for traffic from an individual source IP address.

34.2 Bandwidth Management Commands

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

Table 137 bwm Commands

COMMAND	DESCRIPTION
`bwm <1..127>`	Enters the config-bwm sub-command mode to configure a bandwidth management policy. See Table 138 on page 254 for the sub-commands.
`[no] bwm activate`	Enables bandwidth management on the ZyWALL / USG. The no command disabled bandwidth management.
`bwm append`	Enters the config-bwm sub-command mode to add a policy to the end of the policy list. See Table 138 on page 254 for the sub-commands.
`bwm default inbound priority <1..7>`	Specifies a number between 1 and 7 to set the priority for incoming traffic that matches the default policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority.
`bwm default outbound priority <1..7>`	Specifies a number between 1 and 7 to set the priority for outgoing traffic that matches the default policy.
`bwm delete <1..127>`	Removes a policy.
`bwm insert <1..127>`	Enters the config-bwm sub-command mode to add a policy before the specified policy number. See Table 138 on page 254 for the sub-commands.

Table 137 bwm Commands (continued)

COMMAND	DESCRIPTION
`bwm <1..127>`	Enters the `config-bwm` sub-command mode to create a bandwidth management policy. See Table 138 on page 254 for the sub-commands.
`bwm modify <1..127>`	Enters the `config-bwm` sub-command mode to edit a bandwidth management policy. See Table 138 on page 254 for the sub-commands.
`bwm move <1..127> to <1..127>`	Moves a policy to the number that you specified.
`show bwm activation`	Displays whether bandwidth management is enabled.
`show bwm all`	Displays all bandwidth management policies.
`show bwm default`	Displays the default bandwidth management policy.

34.2.1 Bandwidth Sub-Commands

The following table describes the sub-commands for several `bwm` commands.

Table 138 bwm Sub-commands

COMMAND	DESCRIPTION
`[no] activate`	Enables a policy. The `no` command disables the policy.
`[no] description` *description*	Sets a descriptive name (up to 60 printable ASCII characters) for a policy. The `no` command removes the descriptive name from the policy.
`[no] destination` *address_object*	Sets the destination IP address or address group for whom this policy applies. The `no` command resets the destination IP address(es) to the default (`any`). `any` means all IP addresses.
`[no] dscp {<0..63> | any | class {af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | wmm_be0 | wmm_be24 | wmm_bk16 | wmm_bk8 | wmm_vi32 | wmm_vi40 | wmm_vo48 | wmm_vo56}}`	Specifies a DSCP code point value or sets an AF class or QoS access class of incoming or outgoing packets to which this policy applies. `any` means all DSCP value or no DSCP marker. The `no` command resets the DSCP code to the default (`any`).
`[no] inbound ceiling {<0..1048576> | maximize-bandwidth-usage}`	Sets the maximum bandwidth allowed for incoming traffic or enables maximize bandwidth usage to let the traffic matching this policy "borrow" any unused bandwidth on the incoming interface. The `no` command resets the inbound maximum bandwidth to the default (`0`).
`[no] inbound guarantee-bandwidth <0..1048576> priority <1..7>`	Sets how much inbound bandwidth, in kilobits per second, this policy allows the traffic to use and also sets a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority. Inbound refers to the traffic the ZyWALL / USG sends to a connection's initiator. The `no` command resets the inbound guarantee bandwidth to the default (`0`).

Table 138 bwm Sub-commands (continued)

COMMAND	DESCRIPTION
`[no] inbound-dscp-mark {<0..63> | class {af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | wmm_be0 | wmm_be24 | wmm_bk16 | wmm_bk8 | wmm_vi32 | wmm_vi40 | wmm_vo48 | wmm_vo56}}`	Sets the DSCP value to apply to the incoming packets that match this policy. `default`: to have the ZyWALL / USG set the DSCP value of the packets to 0. The no command resets the incoming DSCP code to the default (`preserve`) and have the ZyWALL / USG keep the packets' original DSCP value.
`[no] incoming-interface {interface` *`interface_name`* `| trunk` *`group_name`*`}`	Sets the source interface of the traffic to which this policy applies. *`interface_name`*: The name of the interface. This depends on the ZyWALL / USG model. See Table 38 on page 97 for detailed information about the interface name. *`group_name`*: A descriptive name for the trunk. The name cannot start with a number. This value is case-sensitive. The no command resets the incoming interface to the default (`any`).
`[no] log [alert]`	Sets the ZyWALL / USG to generate a log (and alert) for packets that match the policy. The no command sets the ZyWALL / USG to not generate a log and alert for packets that match the policy.
`[no] outbound ceiling {<0..1048576> | maximize-bandwidth-usage}`	Sets the maximum bandwidth allowed for outgoing traffic or enables maximize bandwidth usage to let the traffic matching this policy "borrow" any unused bandwidth on the out-going interface. The no command resets the outbound maximum bandwidth to the default (`0`).
`[no] outbound guarantee-bandwidth <0..1048576> priority <1..7>`	Sets how much outbound bandwidth, in kilobits per second, this policy allows the traffic to use and also sets a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority. Outbound refers to the traffic the UAG sends out from a connection's initiator. The no command resets the outbound guarantee bandwidth to the default (`0`).
`[no] outbound-dscp-mark {<0..63> | class {af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | wmm_be0 | wmm_be24 | wmm_bk16 | wmm_bk8 | wmm_vi32 | wmm_vi40 | wmm_vo48 | wmm_vo56}}`	Sets the DSCP value to apply to the outgoing packets that match this policy. `default`: to have the ZyWALL / USG set the DSCP value of the packets to 0. The no command resets the outgoing DSCP code to the default (`preserve`) and have the ZyWALL / USG keep the packets' original DSCP value.

Table 138 bwm Sub-commands (continued)

COMMAND	DESCRIPTION
`[no] outgoing-interface {interface` *`interface_name`* `| trunk` *`group_name`*`}`	Sets the destination interface of the traffic to which this policy applies. *interface_name*: The name of the interface. This depends on the ZyWALL / USG model. See Table 38 on page 97 for detailed information about the interface name. *group_name*: A descriptive name for the trunk. The name cannot start with a number. This value is case-sensitive. The no command resets the outgoing interface to the default (any).
`[no] schedule` *`schedule_object`*	Specifies a schedule that defines when the policy applies. The no command resets the schedule to the default (none) to make the policy always effective.
`[no] service service-object {`*`service_name`* `| any}`	Specifies a service or service group to identify the type of traffic to which this policy applies. any: the policy is effective for every service. The no command resets the service to the default (any).
`show`	Displays the policy settings.
`[no] source` *`address_object`*	Sets the source IP address or address group for whom this policy applies. The no command resets the source IP address(es) to the default (any). any means all IP addresses.
`[no] type {per-user | shared | per-ip-source}`	Sets the type of bandwidth management. per-user: to allow every user that matches this policy to use up to the bandwidth configured in this policy. shared: to have users that match this policy to share the bandwidth configured in this policy. per-ip-source: tset the maximum bandwidth for traffic from an individual source IP address. The no command resets the bandwidth management type to the default (shared).
`[no] user` *`user_name`*	Sets a user name or user group to which to apply the policy. The no command resets the user name to the default (any). any means all users.
`priority-code <0..7>`	Priority code is applied to outgoing traffic. The BWM policy priority code setting overwrites the VLAN priority code setting. Sets the priority code for the specfied VLAN from 0 (lowest, background traffic) to 7 (highest, network control traffic). This is the priority code for packets in the specfied VLAN that don’t match the BWM rule.
`vlan-priority-code <0..7>`	Sets the priority code for matching outgoing traffic in the specfied VLAN.

Table 138 bwm Sub-commands (continued)

COMMAND	DESCRIPTION
`marked-interface interface vlan<1..4064>`	When a packet matches BWM criteria, choose the VLAN interface(s) to which to apply the priority code using a `marked-interface` command. Marks matching outgoing traffic from the specfied VLAN with the configured priority code.
`marked-interface any`	Marks matching outgoing traffic from any VLAN with the configured priority code.
`marked-interface trunk` *`trunk_name`*	Marks matching outgoing traffic from the specfied trunk with the configured priority code.
`marked-interface none`	Doesn’t mark outgoing traffic with priority code for this BWM rule.

34.3 Bandwidth Management Commands Examples

The following example sets the priority code to 3 for packets in VLAN 1 that don’t match any other BWM rule. BWM rule 1 marks matching outgoing traffic from VLAN 1 to priority code 4.

```
Router(config)# interface vlan1
Router(config-if-vlan)# priority-code 3
Router(config-bwm modify 1)# exit
Router(config)# bwm 1
Router(config-bwm modify 1)# vlan-priority-code 4
Router(config-bwm modify 1)# marked-interface interface vlan1
Router(config-bwm modify 1)# exit
Router(config)#
```

The following example adds a new bandwidth management policy for trial-users to limit incoming and outgoing bandwidth and sets the traffic priority to 3. It then displays the policy settings.

```
Router# configure terminal
Router(config)# bwm append
Router(config-bwm append 6)# activate
Router(config-bwm append 6)# description example
Router(config-bwm append 6)# user trial-users
Router(config-bwm append 6)# inbound guarantee-bandwidth 800 priority 3
Router(config-bwm append 6)# outbound guarantee-bandwidth 700 priority 3
Router(config-bwm append 6)# show
Current Configuration:
index: 6
   Activate: yes
   Description: example
   BWM Type: shared
   Schedule: none
   User: trial-users
   Incoming_Type: any
   Incoming_Interface: any
   Outgoing_Type: any
   Outgoing_Interface: any
   Src: any
   Dst: any
   Service_Type: service-object
   Service_Name: any
   Inbound_Excess: no
   Inbound_Prio: 3
   Inbound: 800
   Inbound_Ceiling: 0
   Outbound_Excess: no
   Outbound_Prio: 3
   Outbound: 700
   Outbound_Ceiling: 0
   DSCP_Code: any
   DSCP_Inbound: preserve
   DSCP_Outbound: preserve
   Log: no
Router(config-bwm append 6)# exit
Router(config)#
```

35

Application Patrol

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

35.1 Application Patrol Overview

Application patrol provides a convenient way to manage the use of various applications on the network. It manages general protocols (for example, http and ftp) and instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), and streaming (RSTP) applications. You can even control the use of a particular application's individual features (like text messaging, voice, video conferencing, and file transfers). Application patrol also has powerful bandwidth management including traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

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

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

35.2 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 139 Input Values for Application Patrol Commands

LABEL	DESCRIPTION
<profile-name>	Type the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
description	This is a description of the App Patrol Profile.

The following sections list the application patrol commands.

35.2.1 Application Patrol Commands

This table lists the application patrol commands.

Table 140 app Commands: Application Patrol

COMMAND	DESCRIPTION
`app rename` *`<profile-name>`* *`<profile-name>`*	Renames an existing profile
`[no] app log_sid`	Generate a log when traffic matches a signature in this category. The no command disables it.
`show app statistics summary`	Shows a summary of application patrol statistics (if any).
`show app statistics collect`	Shows if application patrol statistics gathering is enabled and if yes, when.
`[no] app statistics collect`	Enables application patrol statistics gathering. The no command disables it.
`app statistics flush`	Clears all application patrol statistics.
`show app signatures version`	Displays the App Patrol signature set version number. This number gets larger as the set is enhanced.
`show app signatures date`	Displays the date (yyyy-mm-dd) and time the set was released.
`show app profiles` *`<profile-name>`*	Shows the description, application name, and object reference number associated with the named profile.
`show app profiles` *`<profile-name>`* `application`	Shows the application name, action and log associated with the named profile.
`[no] app` *`<profile-name>`*	Creates a profile with the specified name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. The no command disables it.
`[no] description DESCRIPTION`	Write a description of the App Patrol Profile.
`application` *`<profile-name>`* `action {forward|drop|reject} {no log|log [alert]}`	Sets the action and generates a log, log and alert or neither (no) when traffic matches a signature in this profile. Actions are: • **forward** - routes packets that matches these signatures. • **Drop** - silently drops packets that matches these signatures without notification. • **Reject** - drops packets that matches these signatures and sends notification.
`no application-object` *`<profile-name>`*	Removes the application object from the named profile.

35.2.1.1 Application Patrol Command Examples

This command shows details of an application patrol profile created.

```
Router# show app profiles
APP-patrol: 1
  profile name: app1
  description:
  application: ultrasurf_app
  ref: 1
```

These are some other example application patrol usage commands

```
Router(config)# show app statistics collect
collect statistics: yes
collect statistics time: since 2014-06-03 05:39:59 to 2014-06-10 06:20:17
Router(config)# show app signatures version
version: 3.1.4.049
Router(config)# show app signatures date
date: 2013-12-05 18:09:51
Router(config)# app john
Router(config-app-patrol-profile-john)# description this is a dummy profile
Router(config-app-patrol-profile-john)# exit
Router(config)# show app profiles
APP-patrol: 1
  profile name: testfb
  description:
  application: tests
  ref: 0
APP-patrol: 2
  profile name: test
  description: this is a test
  application:
  ref: 0
APP-patrol: 3
  profile name: john
  description: this is a dummy profile
  application:
  ref: 0
Router(config)#
```

36

Anti-Virus

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

36.1 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.

36.2 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 141 Input Values for General Anti-Virus Commands

LABEL	DESCRIPTION
<profile-name>	The name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
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 / USG check the beginning and end of the file name and ignore the middle. For example, with “abc*.zip”, any file starting with “abc” and ending in “.zip” matches, no matter how many characters are in between. 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 / USG checks up to the first 80 characters of a file name.

36.2.1 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 51).

Table 142 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.
`show anti-virus eicar activation`	Displays anti-virus eicar status.
`[no] anti-virus eicar activate`	Turns detection of the EICAR test file on or off.
`anti-virus reload signatures`	Recovers the anti-virus signatures. You should only need to do this if instructed to do so by a support technician.
`[no] anti-virus skip-unknown-file-type activate`	Sets whether or not anti-virus checks files for which the ZyWALL / USG cannot identify a type.
`show anti-virus skip-unknown-file-type activation`	Displays whether or not anti-virus checks files for which the ZyWALL / USG cannot identify a type.
`anti-virus mail-infect-ext activate`	Has the ZyWALL / USG add a notification text file to an e-mail after destroying a virus-infected e-mail attachment.
`no anti-virus mail-infect-ext activate`	Has the ZyWALL / USG not add a notification text file to an e-mail after destroying a virus-infected e-mail attachment.

36.2.2 Anti-Virus Profile

This table lists the AV profile-related commands.

Table 143 anti-virus profile Commands

COMMAND	DESCRIPTION
`anti-virus rename old_profile_name new_profile_name`	Renames the AV profile.
`anti-virus profile_name`	Enters the anti-virus sub-command mode to edit the specified direction specific profile.
`[no] infected-action destroy`	Sets the action to take when the ZyWALL / USG finds a virus in a file.
`[no] file-decompression [unsupported destroy]`	Enable file decompression to have the ZyWALL / USG attempt to to decompress zipped files for further scanning. You can also have it destroy the zipped files it cannot decompress due to encryption or system resource limitations.
`[no] log [alert]`	Sets if the ZyWALL / USG should create a log or alert if it finds a virus in a file.
`description`	Describes the profile.
`[no] scan {http | ftp | imap4 | smtp | pop3}`	Sets the protocols of traffic to scan for viruses.
`[no] infected-action {destroy | send-win-msg}`	Sets the action to take when the ZyWALL / USG detects a virus in a file. The file can be destroyed (filled with zeros from the point where the virus was found). The ZyWALL / USG can also send a message alert to the file's intended user using a Microsoft Windows computer connected to the to interface.

Table 143 anti-virus profile Commands

COMMAND	DESCRIPTION
`[no] bypass {white-list | black-list}`	Have the ZyWALL / USG not check files against a pattern list.
`[no] file-decompression [unsupported destroy]`	Enable file decompression to have the ZyWALL / USG attempt to to decompress zipped files for further scanning. You can also have it destroy the zipped files it cannot decompress due to encryption or system resource limitations.
`show [all]`	Displays the details of the anti-virus rule you are configuring or all the rules.
`anti-virus rule move <1..32> to <1..32>`	Moves a direction specific anti-virus rule to the number that you specified.
`anti-virus rule delete <1..32>`	Removes a direction specific anti-virus rule.
`show anti-virus profile [ profile_name ]`	Shows details of the named profile.

36.2.2.1 Anti-Virus Profile Command Example

This is an example of anti-virus profile commands.

```
Router(config)# anti-virus office1
Router(config-av-profile-office1)# infected-action destroy
Router(config-av-profile-office1)# file-decompression
Router(config-av-profile-office1)# no file-decompression unsupported destroy
Router(config-av-profile-office1)# exit
Router(config)# show an
anti-spam    anti-virus
Router(config)# show anti-virus profile office1
Anti-Virus Rule: 3
  name: office1
  description:
  log: log
  file decompression: yes
  destroy unsupported compressed file: no
  destroy infected compressed file: yes
  reference count: 0
```

36.2.3 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 144 Commands for Anti-virus White and Black Lists

COMMAND	DESCRIPTION
`[no] anti-virus white-list activate`	Turn on the white list to have the ZyWALL / USG not perform the anti-virus check on files with names that match the white list patterns.
`[no] anti-virus white-list file-pattern` *`av_file_pattern`* `{activate|deactivate}`	Adds or removes a white list file pattern. Turns a file pattern on or off.
`anti-virus white-list replace` *`old_av_file_pattern new_av_file_pattern`* `{activate|deactivate}`	Replaces the specified white list file pattern with a new file pattern.
`[no] anti-virus black-list activate`	Turn on the black list to log and delete files with names that match the black list patterns.

Table 144 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.

36.2.3.1 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
```

36.2.4 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 145 Command for Anti-virus Signature Search

COMMAND	DESCRIPTION
show anti-virus search signature { all | name virus_name} [{from id to id}]	Searches for signatures by name.Type the ID or part of the ID that you want to find.

36.2.4.1 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 name: MSN
```

36.3 Update Anti-virus Signatures

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

Table 146 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.

36.3.1 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: 686000
SSII (signature) number: 6000
SSII(md5 checksum) number: 680000
```

36.4 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 147 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 | destination6 | source | source6 | 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(6)`: lists the source IP addresses (IPv4 or IPv6) of the most virus-infected files. `destination(6)`: lists the most common destination IP addresses (IPv4 or IPv6) for virus-infected files.

36.4.1 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
virus detected: 0
Router(config)# show anti-virus statistics ranking destination
```

IDP Commands

This chapter introduces IDP-related commands.

37.1 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 148 Input Values for IDP Commands

LABEL	DESCRIPTION
zone_profile	The name of a zone. For some ZyWALL / USG models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other ZyWALL / USG models, use pre-defined zone names like DMZ, LAN1, SSL VPN,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.

37.2 General IDP Commands

37.2.1 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 51.

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

Table 149 IDP Activation

COMMAND	DESCRIPTION
`[no] idp {signature | 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. The `no` command disables the specified service.
`idp system-protect deactivate`	Disables system-protect.

Table 149 IDP Activation

COMMAND	DESCRIPTION
`show idp {signature | system-protect} activation`	Displays IDP signature, 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.

37.2.1.1 Activate/Deactivate IDP Example

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

```
Router# configure terminal
Router(config)# idp signature activate
Router(config)# show idp signature activation
idp signature activation: yes
Router(config)# no idp signature activate
Router(config)# show idp signature activation
idp signature activation: no
```

37.3 IDP Profile Commands

37.3.1 Global Profile Commands

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

Table 150 Global Profile Commands

COMMAND	DESCRIPTION
idp rename signature *profile1 profile2*	Rename an IDP signature originally named *profile1* to *profile2*.
no idp signature *profile3*	Delete an IDP signature or system protect profile named *profile3*.
idp signature profile signature sid { activate | log [alert] | action { drop | reject-sender | reject-receiver | reject-both } }	Sets the action and log for the specified signature
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 signature profiles	Displays IDP profiles created.
show idp engine version	Displays the IDP engine version.
show idp signature profile signature sid details	Displays specified signature details.

37.3.1.1 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)#
```

37.3.2 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 151 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.
`description description2`	Describes the signature profile.

37.3.3 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 152 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.
`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.

37.3.3.1 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 153 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 = Botnet
		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 154 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		

37.3.3.2 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
```

37.4 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 > UTM Profile > Custom Signatures** screen.

Note: You must use the web configurator to import a custom signature file.

Table 155 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.
idp customize_import name sig_name	Edits an existing 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.

37.4.1 Custom Signature Examples

These examples show how to create a custom signature, edit one, display details of one, all and show the total number of custom signatures.

```
Router# configure terminal
Router(config)# idp customize signature "alert tcp any any <> any any  (msg:
\"test\"; sid: 9000000 ;  )"
sid: 9000000
  message: test
  policy type:
  severity:
  platform:
    all: no
    Win95/98: no
    WinNT: no
    WinXP/2000: no
    Linux: no
    FreeBSD: no
    Solaris: no
    SGI: no
    other-Unix: no
    network-device: no
  service:
  outbreak: no
```

This example shows you how to edit a custom signature.

```
Router(config)# idp customize signature edit "alert tcp any any <> any any  (msg :
\"test edit\"; sid: 9000000 ;  )"
sid: 9000000
  message: test edit
  policy type:
  severity:
  platform:
    all: no
    Win95/98: no
    WinNT: no
    WinXP/2000: no
    Linux: no
    FreeBSD: no
    Solaris: no
    SGI: no
    other-Unix: no
    network-device: no
  service:
  outbreak: no
```

This example shows you how to display custom signature details.

```
Router(config)# show idp signatures custom-signature 9000000 details
sid: 9000000
  message: test edit
  policy type:
  severity:
  platform:
    all: no
    Win95/98: no
    WinNT: no
    WinXP/2000: no
    Linux: no
    FreeBSD: no
    Solaris: no
    SGI: no
    other-Unix: no
    network-device: no
  service:
  outbreak: no
```

This example shows you how to display custom signature contents.

```
Router(config)# show idp signatures custom-signature 9000000 contents
sid: 9000000
Router(config)# show idp signatures custom-signature 9000000 non-contents
sid: 9000000
  ack:
  dport: 0
  dsize:
  dsize_rel:
  flow_direction:
  flow_state:
  flow_stream:
  fragbits_reserve:
  fragbits_dontfrag:
  fragbits_morefrag:
  fragoffset:
  fragoffset_rel:
  icmp_id:
  icmp_seq:
  icode:
  icode_rel:
  id:
  ipopt:
  itype:
  itype_rel:
  sameip:
  seq:
  sport: 0
  tcp_flag_ack:
  tcp_flag_fin:
  tcp_flag_push:
  tcp_flag_r1:
  tcp_flag_r2:
  tcp_flag_rst:
  tcp_flag_syn:
  tcp_flag_urg:
  threshold_type:
  threshold_track:
  threshold_count:
  threshold_second:
  tos:
  tos_rel:
  transport: tcp
  ttl:
  ttl_rel:
  window:
  window_rel:
```

This example shows you how to display all details of a custom signature.

```
Router(config)# show idp signatures custom-signature all details
sid: 9000000
  message: test edit
  policy type:
  severity:
  platform:
    all: no
    Win95/98: no
    WinNT: no
    WinXP/2000: no
    Linux: no
    FreeBSD: no
    Solaris: no
    SGI: no
    other-Unix: no
    network-device: no
  service:
  outbreak: no
```

This example shows you how to display the number of custom signatures on the ZyWALL / USG.

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

37.5 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 156 Update Signatures

COMMAND	DESCRIPTION
`idp signature update signatures`	Immediately downloads IDP signatures from an update server.
`[no] idp signature update auto`	Enables (disables) automatic signature downloads at regular times and days.
`idp signature update hourly`	Enables automatic signature download every hour.
`idp signature update daily <0..23>`	Enables automatic signature download every day at the time specified.
`idp signature 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 update`	Displays signature update schedule.
`show idp signature update status`	Displays signature update status.
`show idp signature signatures {version | date | number}`	Displays signature information

37.5.1 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 signature update auto
Router(config)# no idp signature update auto
Router(config)# idp signature update hourly
Router(config)# idp signature update daily 10
Router(config)# idp signature update weekly fri 13
Router(config)# show idp signature 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
```

37.6 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 157 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 collect status`	Displays the status of collected statistics.
`show idp statistics ranking {signature-name | source | source6 | destination |destination6}`	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(6)`: lists the source IP addresses (IPv4 or IPv6) from which the ZyWALL / USG has detected the most intrusion attempts. `destination(6)`: lists the most common destination IP addresses (IPv4 or IPv6) for detected intrusion attempts.

37.6.1 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
```

38

Content Filtering

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

38.1 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.

38.2 External Web Filtering Service

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

38.3 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.

38.4 Content Filter Command Input Values

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

Table 158 Content Filter Command Input Values

LABEL	DESCRIPTION
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. {advertisements-pop-ups | job-search | alcohol-tobacco | leisure-recreation | anonymizers | malware | arts | network-errors | botnets | news | business | non-profits-ngos | chat | nudity | child-abuse-images | parked-domains | compromised | peer-to-peer | computers-technology | personal-sites | criminal-activity | phishing-fraud |cults | politics | dating-personals | pornography-sexually-explicit | download-sites | private-ip-addresses | education | real-estate | entertainment | religion | fashion-beauty | restaurants-dining | finance | school-cheating | forums-newsgroups | search-engines-portals | gambling | sex-education | games | shopping | general | social-networking | government | spam-sites | greeting-cards | sports | hacking | streaming-media-downloads | hate-intolerance | tasteless | health-medicine | translators | illegal-drugs | transportation | illegal-software | travel | image-sharing | violence | information-security | weapons | instant-messaging | web-based-email }
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. IPv6 support format like: Single ip - 2001::1 Range format - 2001::1-2001::5 Prefix format - 2001::1/64

Table 158 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. IPv6 support format like: Single ip - 2001::1 Range format - 2001::1-2001::5 Prefix format - 2001::1/64
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". IPv6 format support: http://[2001::1]/blocked_access
service_timeout	The value specifies the maximum querying time in seconds <1...60>
url	The URL of a web site in http://xxx.xxx.xxx format.
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.

38.5 General Content Filter Commands

The following table lists the commands that you can use for general content filter configuration such as 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 158 on page 282 for details about the values you can input with these commands.

Table 159 content-filter General Commands

COMMAND	DESCRIPTION
[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.
content-filter passed warning flush	Clears the ZyWALL / USG's record of sessions for which it has given the user a warning before allowing access.
content-filter passed warning timeout <1..1440>	Sets how long to keep records of sessions for which the ZyWALL / USG has given the user a warning before allowing access.
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 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.
[no] {*ipv4* | *ipv4_cidr* | *ipv4_range* | *wildcard_domainname* | *tld* |*ipv6* | *ipv6_range* | *ipv6_prefix* }	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. ipv6: IPv6 address, i.e. 2001::1 ipv6_range: Range of IPv6 address, < IPv6 Address >-< IPv6 Address > ipv6_prefix: IPv6 prefix formant, <IPv6 Address>/<Prefix Length>
exit	Leaves the sub-command mode.
content-filter cf-queue flush	clears content filter queuing packets.
[no] content-filter https-domain-filter activate	Enables HTTPs Domain Filter which lets the ZyWALL/USG take action on HTTPS web pages using the CommTouch category service. In an HTTPS connection, the ZyWALL / USG can extract the Server Name Indication (SNI) from a client request, check if it matches a category in the CommTouch content filter and then take appropriate action. The keyword match is for the domain name only. The no command disables the HTTPs Domain Filter.

Table 159 content-filter General Commands (continued)

COMMAND	DESCRIPTION
`show content-filter passed warning`	Displays the ZyWALL / USG's record of sessions for which it has given the user a warning before allowing access.
`show content-filter settings`	Displays the general content filtering settings.
`show content-filter common-list {trust|forbid}`	Displays the common list of trusted or forbidden web sites.
`show content-filter https-domain-filter status`	Displays HTTPs Domain Filter content filtering settings.

38.6 Content Filter Filtering Profile Commands

The following table lists the commands that you can use to configure a content filtering profile. Use the `configure terminal` command to enter the configuration mode to be able to use these commands. See Table 158 on page 282 for details about the values you can input with these commands.

Table 160 content-filter Filtering Profile Commands Summary

COMMAND	DESCRIPTION
[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.
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.

Table 160 content-filter Filtering Profile Commands Summary (continued)

COMMAND	DESCRIPTION
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 service-timeout *service_timeout*	Sets how many seconds the ZyWALL / USG is to wait for a response from the external content filtering server. The no command clears the setting.
[no] content-filter profile *filtering_profile* commtouch-url category {category_name}	Sets a CommTouch content filtering profile to check for specific web site categories. The no command has the profile not check for the specified categories.
content-filter profile *filtering_profile* commtouch-url match-unsafe {block | log | warn |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 | 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 / USG not log attempted access to web pages that match the CommTouch profile's selected unsafe categories.
no content-filter profile *filtering_profile* commtouch-url match {log}	Has the ZyWALL / USG not log attempted access to web pages that match the CommTouch profile's selected managed categories.
no content-filter profile *filtering_profile* commtouch-url offline {log}	Has the ZyWALL / USG not log access to web pages if the CommTouch external content filtering database is unavailable.
no content-filter profile *filtering_profile* commtouch-url unrate {log}	Has the ZyWALL / USG not log access to web pages that the CommTouch external web filtering service has not categorized.
[no] content-filter sslv3 action block	Has the ZyWALL / USG block HTTPS web pages using SSL V3 or a previous version. The no command allows HTTPS web pages using SSL V3 or a previous version.

Table 160 content-filter Filtering Profile Commands Summary (continued)

COMMAND	DESCRIPTION
`[no] content-filter https-domain-filter block-page activate`	Has the ZyWALL/USG display a warning page instead of a blank page when an HTPPS connection is redirected. The `no` command has the ZyWALL/USG display a blank page when an HTTPS connection is blocked.
`content-filter https-domain-filter block-page port <port>`	Changes the port number of the HTTPS Domain Filter blocking page. The default port is 54088.
`content-filter https-domain-filter block-cache-ttl <1~60>`	Sets how many seconds (1-60) to keep blocked HTTPS pages in the cache. The default value is 5.
`content-filter https-domain-filter forward-cache-ttl <1~1440>`	Sets how many minutes (1-1440) to keep forwarded HTTPS pages in the cache. The default value is 60.
`[no] content-filter profile <filtering_profile> safesearch`	Enables SafeSearch in the specified content filter profile. SafeSearch is a feature of a search engine that can automatically filter sexually explicit videos and images from the search result without overloading the ZyWALL / USG. It does this by adding a parameter in the search URL: https://www.google.com.tw/?gws_rd=ssl#q=porn&safe=active. Supported search engines at the time of writing are: Yahoo, Google, MSN Live Bing, Yandex
`[no] content-filter safesearch <name>`	Creates a content-filter safesearch rule and enters sub-command mode. The `no` command removes the rule.
`    domain match <string>`	Sets a string that the domain name should (partially) match in a safesearch rule. For example, domain-match: .google.
`    domain not-match <string>`	Sets a string that the domain name should not match in a safesearch rule.
`    url match <string>`	Sets a string that the URL should (partially) match in a safesearch rule. For example, url-match: search
`    url not-match <string>`	Sets a string that the URL should not match in a safesearch rule.
`    url parameter <string>`	Sets a parameter that updates the URL when there is a safesearch rule match. Values in URL Parameters are set dynamically in a page’s URL. Example url-parameter: safe=
`    url value <string>`	Sets a value that updates the URL when there is a safesearch rule match. Example url-value: active
`    cookie match <string>`	Sets a string that the cookie should (partially) match in a safesearch rule. A cookie is a small piece of data sent from a website and stored in the user's web browser.
`    cookie parameter <string>`	Sets a parameter that updates the cookie when there is a safesearch rule match. Parameters store information such as the cookie’s expiration, domain, and flags.
`    cookie value <string>`	Sets a value that updates the cookie when there is a safesearch rule match. The value of a cookie can be modified by the server in response to a page request.
`show content-filter safesearch`	Displays all safesearch rules created and their sub-command contents.
`show content-filter profile [filtering_profile] commtouch`	Displays the specified content filtering profile’s settings or the settings of all them if you don’t specify one.

38.7 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 161 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.

38.7.1 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 passed                   : 0

  unsafe web pages                     : 0
  other web pages                      : 0
```

38.8 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 51).

6 You can also customize the filtering profile. The following commands block active-X, java and proxy access.

7 Append a Secure Policy with content filter profile.

```
Router# configure terminal
Router(config)# address-object sales 172.2.3.0/24
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 commtouch-url category job-search
Router(config)# content-filter profile sales_CF_PROFILE commtouch-url category business
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)# secure-policy insert 1
Router(config)# name UTM
Router(config)# from LAN1
Router(config)# schedule all_day
Router(config)# sourceip sales
Router(config)# no app-profile
Router(config)# cf-profile sales_CF_PROFILE log by-profile activate
Router(config)# exit
```

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: action:   warn, log:  no
url match other : action:  block, log:  no
url unrate      : action:   warn, log:  no
service offline : action:   warn, log:  no

category settings:
Advertisements and Pop-Ups   :  no, Alcohol and Tobacco          :  no
Anonymizers                  : yes, Arts                         :  no
Business                     : yes, Transportation               :  no
Chat                         :  no, Forums and Newsgroups        :  no
Compromised                  : yes, Computers and Technology     :  no
Criminal Activity            :  no, Dating and Personals         :  no
Download Sites               :  no, Education                    :  no
Entertainment                :  no, Finance                      :  no
Gambling                     :  no, Games                        :  no
Government                   :  no, Hate and Intolerance         :  no
Health and Medicine          :  no, Illegal Drugs                :  no
Job Search                   : yes, Streaming Media and Downloads:  no
News                         :  no, Non-profits and NGOs         :  no
Nudity                       :  no, Personal Sites               :  no
Phishing and Fraud           : yes, Politics                     :  no
Pornography/Sexually Explicit:  no, Real Estate                  :  no
Religion                     :  no, Restaurants and Dining       :  no
Search Engines and Portals   :  no, Shopping                     :  no
Social Networking            :  no, Spam Sites                   : yes
Sports                       :  no, Malware                      : yes
Translators                  :  no, Travel                       :  no
Violence                     :  no, Weapons                      :  no
Web-based Email              :  no, General                      :  no
Leisure and Recreation       :  no, Botnets                      : yes
Cults                        :  no, Fashion and Beauty           :  no
Greeting cards               :  no, Hacking                      :  no
Illegal Software             :  no, Image Sharing                :  no
Information Security         :  no, Instant Messaging            :  no
Network Errors               : yes, Parked Domains               : yes
Peer-to-Peer                 :  no, Private IP Addresses         :  no
School Cheating              :  no, Sex Education                :  no
Tasteless                    :  no, Child Abuse Images           :  no

custom active                      : yes
allow traffic to trusted hosts only:  no
allow features to trusted hosts    :  no
block activex                      : yes
block java                         : yes
block cookie                       :  no
block proxy                        : yes
check common list                  : yes
```

39

Anti-Spam

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

39.1 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.

39.2 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 162 Input Values for General Anti-Spam Commands

LABEL	DESCRIPTION
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.

39.2.1 Anti-spam Profile 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 163 Commands for Anti-Spam Profile Rules

COMMAND	DESCRIPTION
`anti-spam profile append`	Enters the anti-spam sub-command mode to append a profile.
`anti-spam profile insert` *rule_number*	Enters the anti-spam sub-command mode to insert a profile.
`anti-spam profile` *rule_number*	Enters the anti-spam sub-command mode to edit the specified direction specific rule.
`[no] log [alert]`	Sets the ZyWALL / USG to create a log (and optionally an alert) when packets match this rule and are found to be spam. The `no` command sets the ZyWALL / USG not to create a log or alert when packets match this rule.

Table 163 Commands for Anti-Spam Profile Rules (continued)

COMMAND	DESCRIPTION
[no] scan {smtp | pop3}	Sets the protocols of traffic to scan for spam.
[no] match-action pop3 {forward | forward-with-tag}	Sets the action to take when the ZyWALL / USG detects a spam POP3 e-mail. The file can be forwarded or forwarded with a spam tag.
[no] match-action smtp {drop | forward | forward-with-tag}	Sets the action to take when the ZyWALL / USG detects a spam SMTP e-mail. The file can be deleted, forwarded, or forwarded with a spam tag.
[no] bypass {white-list | black-list | dnsbl}	Bypassing has the ZyWALL / USG not check files against your configured white (allowed) list, black (spam) list, or DNSBL servers list.
[no] bypass {ip-reputation | mail-content | virus-outbreak}	Have the ZyWALL / USG not check mail's IP reputation, content, or for viruses.
show	Displays the details of the anti-spam rule you are configuring.
anti-spam profile move *rule_number* to *rule_number*	Moves an anti-spam profile to the number that you specified.
anti-spam profile delete *rule_number*	Removes an anti-spam profile.
show anti-spam profile [*rule_number*]	Displays the details of all the configured anti-spam profiles.
[no] anti-spam ip-reputation activate	Set whether or not to use IP reputation to identify spam by the sender's IP address.
anti-spam ip-reputation query-timeout time [*timeout*]	Set how many seconds the ZyWALL / USG waits for a reply when checking the IP reputation of a sender's IP address.
show anti-spam ip-reputation query-timeout time	Display how many seconds the ZyWALL / USG waits for a reply when checking the IP reputation of a sender's IP address.
[no] anti-spam ip-reputation private-check activate	Set whether or not to check the IP reputation of private sender IP addresses.
show anti-spam ip-reputation private-check	Display the setting for checking the IP reputation of private sender IP addresses.
[no] anti-spam mail-content activate	Set whether or not to identify spam by content, such as malicious content.
[no] anti-spam virus-outbreak activate	Set whether or not to scan emails for attached viruses.
anti-spam tag {mail-content | virus-outbreak} [*tag*]	Specify the labels to add to the beginning of the mail subject if content-analysis identified it as spam or it contains a virus.
[no] anti-spam xheader {mail-content | virus-outbreak} *xheader-name xheader-value*	Specify the name and value for the X-Header to add to content-analysis identified spam or e-mails containing a virus.
show anti-spam tag {mail-content | virus-outbreak}	Display the labels for content-analysis identified spam or e-mails containing a virus.
show anti-spam xheader {mail-content | virus-outbreak}	Display the name and value for the X-Header to add to content-analysis identified spam or e-mails containing a virus.
anti-spam mail-scan query-timeout pop3 {forward | forward-with-tag}	Select how to handle POP3 mail if querying the mail scan server times out. Use forward to send it or forward-with-tag to add a tag to the mail subject and send it.
anti-spam mail-scan query-timeout smtp {drop | forward | forward-with-tag}	Select how to handle SMTP mail if querying the mail scan server times out. Use drop to discard the SMTP mail, forward to send it, or forward-with-tag to add a tag to the mail subject and send it.
anti-spam mail-scan query-timeout time [*timeout*]	Set how many seconds the ZyWALL / USG waits for a reply from the mail scan server before taking the relevant timeout action.
anti-spam tag query-timeout [*tag*]	Specify the label to add to the mail subject of e-mails the ZyWALL / USG tags and forwards when queries to the mail scan servers time out.
[no] anti-spam xheader query-timeout *xheader-name xheader-value*	Specify the name and value for the X-Header to add to e-mails the ZyWALL / USG forwards when queries to the mail scan servers time out.
show anti-spam mail-scan query-timeout smtp	Display the action the ZyWALL / USG takes on SMTP mail if querying the mail scan server times out.

Table 163 Commands for Anti-Spam Profile Rules (continued)

COMMAND	DESCRIPTION
`show anti-spam mail-scan query-timeout pop3`	Display the action the ZyWALL / USG takes on POP3 mail if querying the mail scan server times out.
`show anti-spam mail-scan query-timeout time`	Display how many seconds the ZyWALL / USG waits for a reply from the mail scan server before taking the relevant timeout action.
`show anti-spam mail-scan status`	Displays the ZyWALL / USG's settings for IP reputation, mail content, and virus outbreak checking.
`show anti-spam tag query-timeout`	Display the label the ZyWALL / USG adds to the mail subject of e-mails that it tags and forwards when queries to the mail scan servers time out.
`show anti-spam xheader query-timeout`	Display the name and value for the X-Header the ZyWALL / USG adds to e-mails that it tags and forwards when queries to the mail scan servers time out.

39.2.1.1 Anti-spam Profile Example

This example shows how to configure (and display) a WAN to DMZ anti-spam profile to scan POP3 and SMTP traffic. SMTP spam is forwarded. POP3 spam is marked with a spam tag. The ZyWALL / USG logs the event when an e-mail matches the DNSBL (see Section 39.2.3 on page 296 for more on DNSBL). The white and black lists are ignored.

```
Router(config)# anti-spam 1
Router(config-as-rule-1)# activate
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 1
Anti-Spam Rule: 1
  profile name: AS_profile_default_SXI
  description:
  log: log
  scan protocols:
    smtp: yes
    pop3: yes
  match action:
    smtp: forward-with-tag
    pop3: forward-with-tag
  bypass white list: no
  bypass black list: no
  bypass ip reputation: no
  bypass mail content: no
  bypass virus outbreak: no
  bypass dnsbl: no
  ref: 0
```

39.2.2 White and Black Lists

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

Table 164 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 39.2.2.2 on page 295 for more details.
rule_number	The index number of an anti-spam white or black list entry. 1 - *X* where *X* is the highest number of entries the ZyWALL / USG model supports. See the ZyWALL / USG’s User’s Guide for details.
subject	A keyword in the content of the e-mail Subject headers. Use up to 63 ASCII characters. Spaces are not allowed, although you could substitute a question mark (?). See Section 39.2.2.2 on page 295 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 165 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 IPv4 address. Also turns the entry on or off.
`[no] anti-spam white-list [rule_number] ip6-address ipv6_subnet {activate|deactivate}`	Adds, edits, or removes a white list entry to check e-mail for a specific source or relay IPv6 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 IPv4 address. Also turns the entry on or off.
`[no] anti-spam black-list [rule_number] ip6-address ipv6_subnet {activate|deactivate}`	Adds, edits, or removes a black list entry to check e-mail for a specific source or relay IPv6 address. Also turns the entry on or off.

Table 165 Commands for Anti-spam White and Black Lists (continued)

COMMAND	DESCRIPTION
`[no] anti-spam black-list [`*`rule_number`*`] e-mail `*`email`*` {activate|deactivate}`	Adds, edits, or removes a black list entry to check e-mail for a specific source e-mail address or domain name. Also turns the entry on or off.
`[no] anti-spam black-list [`*`rule_number`*`] mail-header `*`mail-header mail-header-value`*` {activate|deactivate}`	Adds, edits, or removes a black list entry to check e-mail for specific header fields and values. Also turns the entry on or off.
`[no] anti-spam black-list [`*`rule_number`*`] subject `*`subject`*` {activate|deactivate}`	Adds, edits, or removes a black list entry to check e-mail for specific content in the subject line. Also turns the entry on or off.
`anti-spam tag black-list [`*`tag`*`]`	Configures a message or label (up to 15 ASCII characters) to add to the mail subject of e-mails that match an anti-spam black list entry.
`show anti-spam white-list [status]`	Displays the current anti-spam white list. Use `status` to show the activation status only.
`show anti-spam black-list [status]`	Displays the current anti-spam black list. Use `status` to show the activation status only.
`show anti-spam tag black-list`	Show the configured anti-spam black list tag.
`[no] anti-spam xheader {white-list | black-list} `*`mail-header mail-header-value`*	Specify the name and value for the X-Header to add to e-mails that match the ZyWALL / USG's spam white list or black list.
`show anti-spam xheader {white-list | black-list}`	Display the name and value for the X-Header to add to e-mails that match the ZyWALL / USG's spam white list or black list.

39.2.2.1 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
```

39.2.2.2 Regular Expressions in Black or White List Entries

The following applies for a black or white list entry based on an e-mail subject, e-mail address, or e-mail header value.

- Use a question mark (?) to let a single character vary. For example, use "a?c" (without the quotation marks) to specify abc, acc and so on.
- You can also use a wildcard (*). For example, if you configure *def.com, any e-mail address that ends in def.com matches. So "mail.def.com" matches.

- The wildcard can be anywhere in the text string and you can use more than one wildcard. You cannot use two wildcards side by side, there must be other characters between them.
- The ZyWALL / USG checks the first header with the name you specified in the entry. So if the e-mail has more than one “Received” header, the ZyWALL / USG checks the first one.

39.2.3 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 166 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 167 DNSBL Commands

COMMAND	DESCRIPTION
`[no] anti-spam dnsbl activate`	Turns DNSBL checking on or off.
`anti-spam dnsbl [1..5] domain` *`dnsbl_domain`* `{activate|deactivate}`	Adds or edits a DNSBL domain for checking e-mail header IP addresses.
`no anti-spam dnsbl domain` *`dnsbl_domain`*	Removes the specified DNSBL domain.
`anti-spam dnsbl query-timeout smtp {drop | forward | forward-with-tag}`	Sets how the ZyWALL / USG handles SMTP mail (mail going to an e-mail server) if the queries to the DNSBL domains time out.
`anti-spam dnsbl query-timeout pop3 {forward | forward-with-tag}`	Sets how the ZyWALL / USG handles POP3 mail (mail coming to an e-mail client) if the queries to the DNSBL domains time out.
`anti-spam dnsbl max-query-ip [1..5]`	Sets up to how many sender and relay server IP addresses in the mail header to check against the DNSBL.
`anti-spam dnsbl ip-check-order {forward | backward}`	Configures the order in which anti-spam checks e-mail header IP addresses against the DNSBLs. • `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 / USG. `dnsbl-timeout` configures the message or label to add to the mail subject of e-mails that the ZyWALL / USG forwards if queries to the DNSBL domains time out. 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.

Table 167 DNSBL Commands

COMMAND	DESCRIPTION
`show anti-spam dnsbl domain`	Displays the ZyWALL / USG's configured anti-spam DNSBL domain entries.
`show anti-spam dnsbl max-query-ip`	Displays how many sender and relay server IP addresses in the mail header anti-spam checks against the DNSBL.
`show anti-spam dnsbl ip-check-order`	Displays the order in which anti-spam checks e-mail header IP addresses against the DNSBLs.
`show anti-spam dnsbl query-timeout {smtp | pop3}`	Displays how the ZyWALL / USG handles SMTP or POP3 mail if the queries to the DNSBL domains time out.
`show anti-spam tag {dnsbl | dnsbl-timeout}`	`dnsbl` displays the anti-spam tag for e-mails that have a sender or relay IP address in the header that matches a blacklist maintained by a DNSBL domain. `dnsbl-timeout` displays the message or label to add to the mail subject of e-mails that the ZyWALL / USG forwards if queries to the DNSBL domains time out.
`show anti-spam dnsbl statistics`	Displays anti-spam DNSBL statistics for each configured DNSBL domain.
`anti-spam dnsbl statistics flush`	Clears the anti-spam DNSBL statistics for each configured DNSBL domain.
`anti-spam dnsbl query-timeout time [1..10]`	Sets how long the ZyWALL / USG waits for a reply from the DNSBL domains.
`show anti-spam dnsbl query-timeout time`	Displays how long the ZyWALL / USG waits for a reply from the DNSBL domains.
`[no] anti-spam xheader dnsbl` *`mail-header mail-header-value`*	Specify the name and value for the X-Header to add to e-mails with a sender or relay IP address in the header that matches a black list maintained by a DNSBL domain in the ZyWALL / USG's list
`show anti-spam xheader dnsbl`	Display the name and value for the X-Header to add to e-mails with a sender or relay IP address in the header that matches a black list maintained by a DNSBL domain in the ZyWALL / USG's list

39.2.3.1 DNSBL Example

This example:

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

- Displays the DNSBL statistics.

```
Router(config)# anti-spam dnsbl domain DNSBL-example.com activate
Router(config)# show anti-spam dnsbl domain
No.   Status
Domain
===========================================================================
1     yes
DNSBL-example.com
Router(config)# anti-spam dnsbl activate
Router(config)# show anti-spam  dnsbl status
anti-spam dnsbl status: yes
Router(config)# anti-spam dnsbl query-timeout pop3 forward-with-tag
Router(config)# show anti-spam  dnsbl query-timeout pop3
dnsbl query timeout action: forward-with-tag
Router(config)# anti-spam dnsbl max-query-ip 4
Router(config)# show anti-spam  dnsbl max-query-ip
dnsbl max query ip: 4
Router(config)# anti-spam dnsbl ip-check-order forward
Router(config)# show anti-spam  dnsbl ip-check-order
anti-spam dnsbl IP check order: forward
Router(config)# anti-spam tag dnsbl DNSBL
Router(config)# show anti-spam tag dnsbl
dnsbl tag: DNSBL
Router(config)# anti-spam tag dnsbl-timeout DNSBL-timeout
Router(config)# show anti-spam tag dnsbl-timeout
dnsbl-timeout tag: DNSBL-timeout
Router(config)# show anti-spam dnsbl statistics
DNSBL domain: 1
  domain: DNSBL-example.com
  average time: 0.00
  total query: 0
    spam: 0
    clear: 0
    no timeout: 0
    timeout: 0
    no response: 0
```

39.3 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 168 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.

Table 168 Commands for Anti-spam Statistics (continued)

COMMAND	DESCRIPTION
`show anti-spam ip-reputation statistics`	Displays the mail sender IP reputation checking statistics.
`show anti-spam mail-scan statistics`	Displays the mail scan statistics.

39.3.1 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
```

40

SSL Inspection

This chapter describes how to set up SSL Inspection for the ZyWALL / USG.

40.1 SSL Inspection Overview

Secure Socket Layer (SSL) traffic, such as https://www.google.com/HTTPS, FTPs, POP3s, SMTPs, etc. is encrypted, and cannot be inspected using Unified Threat Management (UTM) profiles such as App Patrol, Content Filter, Intrusion, Detection and Prevention (IDP), or Anti-Virus. The ZyWALL / USG uses SSL Inspection to decrypt SSL traffic, sends it to the UTM engines for inspection, then encrypts traffic that passes inspection and forwards it to the destination server, such as Google.

The ZyWALL / USG supports the following in SSL Inspection:

- Supported Cipher Suite
  - RC4 (Rivest Cipher 4)
  - DES (Data Encryption Standard)
  - 3DES
  - AES (Advanced Encryption Standard)
- SSLv3/TLS1.0 (Transport Layer Security) Support
  - SSLv3/TLS1.0 is currently supported with option to pass or block SSLv2 traffic
- Traffic using TLS1.1 (Transport Layer Security) or TLS1.2 is downgraded to TLS1.0 for SSL Inspection
- No Compression Support at time of writing
- No Client Authentication Request Support at time of writing

40.2 SSL Inspection Commands Summary

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

Table 169 Input Values for SSL Inspection Commands

LABEL	DESCRIPTION
ssi_profile_name	This is the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
description	This is additional information about this SSL Inspection profile. You can enter up to 60 characters ("0-9", "a-z", "A-Z", "-" and "_").
cert_name	This is a name of a certificate.

The following sections list the commands.

40.2.1 SSL Inspection Exclusion Commands

There may be privacy and legality issues regarding inspecting a user's encrypted session. The legal issues may vary by locale, so it's important to check with your legal department to make sure that it’s OK to intercept SSL traffic from your ZyWALL / USG users.

To ensure individual privacy and meet legal requirements, you can configure an exclusion list to exclude matching sessions to destination servers. This traffic is not intercepted and is passed through uninspected.

This table lists the SSL Inspection exclusion-related commands.

Table 170 SSL Inspection Exclusion Commands

COMMAND	DESCRIPTION
`ssl-inspection exclude-list-settings`	Use these commands to create a log for traffic that bypasses SSL Inspection.
`[no] log`	The no command disables SSL exclusion list logs.
`ssl-inspection exclude-list`	SSL traffic to a server to be excluded from SSL Inspection is identified by its certificate.
`[no] entry {IPv4 | IPv4_CIDR | IPv4_RANGE | IPv6 | IPv6_PREFIX | IPv6_RANGE | SSL_INSPECTION_WILDCARD_CNAME}`	Identify the certificate in one of the following ways: • Type an IPv4 or IPv6 address. For example, type 192.168.1.35, or 2001:7300:3500::1 • Type an IPv4/IPv6 in CIDR notation. For example, type 192.168.1.1/24, or 2001:7300:3500::1/64 • Type an IPv4/IPv6 address range. For example, type 192.168.1.1-192.168.1.35, or 2001:7300:3500::1-2001:7300:3500::35 • Type a DNS name or a common name (wildcard char: '*', escape char: '\'). Use up to 127 case-insensitive characters (0-9a-zA-Z`~!@#$%^&*()-_=+[]{}\\|;:',.<>/?). ‘*’ can be used as a wildcard to match any string. Use ‘*’ to indicate a single wildcard character. • Type an email address. For example, type abc@zyxel.com.tw The no command disables the SSL entry.
`show ssl-inspection exclude-list [settings]`	Displays SSL exclusion list settings.

40.2.2 SSL Inspection Profile Settings

This table lists the SSL Inspection profile setting commands.

Table 171 SSL Inspection Profile Commands

COMMAND	DESCRIPTION
`ssl-inspection profile SSI_profile_name`	Creates an SSL Inspection profile. Use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`description description`	Enter additional information about this SSL Inspection entry. You can enter up to 60 characters ("0-9", "a-z", "A-Z", "-" and "_").
`no description`	Deletes the description in a profile.
`certificate cert_name`	Enter the default certificate or one already created for this profile.
`no certificate`	Removes the certificate from this profile.

Table 171 SSL Inspection Profile Commands

COMMAND	DESCRIPTION
`follow-real-client-routing {yes | no}`	When a new SSL session is found by SSL inspection, it will create another independent session from the ZyWALL / USG to get information such as the certificate chain. However, since this traffic is sent from the ZyWALL / USG, it may not match the same routing policy of the original SSL session and may not reach the destination server. Enable this command to allow the session sent from the ZyWALL / USG to follow the routing policy of the original session. The no command does not allow the session sent from the ZyWALL / USG to follow the routing policy of the original session.
`sslv2 action {pass | block} {no log | log [alert]}`	SSL Inspection supports SSLv3 and TLS1.0. This command sets the action and log for SSLv2 traffic.
`unsupported-suite action {pass | block} {no log | log [alert]}`	Sets the action and log for unsupported suite traffic.
`untrusted-cert-chain action {pass | block} {no log | log [alert]}`	As a SSL session is being established, servers send their certificate chain to clients. The ZyWALL / USG trusts its own certificates and imported (trusted) certificates to verify the certificate chain. This command sets the action and log for traffic from a server with an untrusted certificate chain.
`ssl-inspection profile rename` *`ssi_profile_name1 ssi_profile_name2`*	Renames an SSL Inspection profile.
`no ssl-inspection profile` *`ssi_profile_name`*	Deletes an SSL Inspection profile.
`show ssl-inspection profile [`*`ssi_profile_name`*`]`	Displays SSL Inspection profile settings.

40.2.3 SSL Inspection Certificate Cache

This table lists the SSL Inspection certificate cache commands.

Table 172 SSL Inspection Certificate Cache Commands

COMMAND	DESCRIPTION
`ssl-inspection cache flush`	Clears SSL Inspection cached entries.
`show ssl-inspection cert-list`	Displays certificates used in SSL Inspection.

40.2.4 SSL Inspection Certificate Update

Use these commands to update the latest certificates of servers using SSL connections to the ZyWALL / USG network. You should have Internet access and have activated SSL Inspection on the ZyWALL / USG at myZyXEL.com.

This table lists the SSL Inspection certificate cache commands.

Table 173 SSL Inspection Certificate Update Commands

COMMAND	DESCRIPTION
`[no] ssl-inspection cert-update auto`	ZyWALL / USG automatically updates the certificate set when a new one becomes available on myZyXEL.com.
`ssl-inspection cert-update now`	Download the latest certificate set from the myZyXEL.com and updates it on the ZyWALL / USG.

Table 173 SSL Inspection Certificate Update Commands

COMMAND	DESCRIPTION
`show ssl-inspection default-cert version`	Displays the default certificate update status.
`show ssl-inspection default-cert update`	Shows the current certificate update status.
`show ssl-inspection cert-update status`	Shows if automatically updating the certificate set is configured on the ZyWALL / USG.

These are some example SSL Inspection certificate update usage commands.

```
Router(config)# show ssl-inspection cert-update status
update auto     : no
Router(config)# ssl-inspection cert-update auto
Router(config)# show ssl-inspection cert-update status
update auto     : yes
Router(config)# show ssl-inspection default-cert update
/tmp/sslinsp_certs/default_trusted /
current status: Connecting to update server to get SSL certificate. at Fri Apr 10 03:47:37
2015

Router(config)# show ssl-inspection default-cert update
current status: SSL Certificate update has succeeded. (success) at Fri Apr 10 03:47:49 2015
Router(config)#
```

40.2.5 SSL Inspection Statistics

This table lists the SSL Inspection statistics commands.

Table 174 SSL Inspection Statistics Commands

COMMAND	DESCRIPTION
`[no] ssl-inspection statistics collect`	Enables SSL inspection statistics collection. The no command disables SSL exclusion statistics collection.
`ssl-inspection statistics flush`	Clears SSL inspection statistics.
`show ssl-inspection statistics collect`	Shows if SSL inspection statistics collection is enabled.
`show ssl-inspection statistics summary`	Shows SSL inspection statistics such as concurrent sessions, total ssl sessions, sessions inspected, decrypted Kbytes, encrypted Kbytes, sessions blocked, and sessions passed.

40.2.6 SSL Inspection Command Examples

These are some other example SSL Inspection usage commands

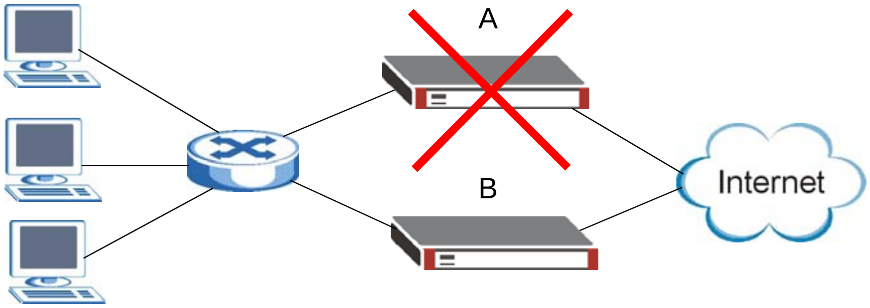
```
Router(config)#Router(config)# ssl-inspection exclude-list-settings
Router(ssl-inspection-exclude-list-settings)# no log
Router(ssl-inspection-exclude-list-settings)# exit
Router(config)# ssl-inspection exclude-list
Router(ssl-inspection-exclude-list)# entry 1.1.1.1
Router(ssl-inspection-exclude-list)# entry abc@zyxel.com.tw
Router(ssl-inspection-exclude-list)# exit
Router(config)# show ssl-inspection exclude-list settings
SSL Inspection Exclude List Global Information
  Log: no
Router(config)# show ssl-inspection exclude-list
No.  Exclude list of Certificate Identity
===============================================================================
0    1.1.1.1
1    abc@zyxel.com.tw
Router(config)# ssl-inspection profile dummy
Router(config-ssl-inspection-profile-dummy)# description this is a dummy profile
Router(config-ssl-inspection-profile-dummy)# certificate default
Router(config-ssl-inspection-profile-dummy)# sslv2 action block log
Router(config-ssl-inspection-profile-dummy)# unsupported-suite action block log
Router(config-ssl-inspection-profile-dummy)# untrusted-cert-chain action block log
Router(config-ssl-inspection-profile-dummy)# exit
Router(config)# show ssl-inspection profile dummy
SSL-Inspection: 3
  profile name: dummy
  description: this is a dummy profile
  Certificate: default
  Follow_real_client_routing: yes
  SSLv2_action: block
  SSLv2_log: log
  Unsupported_suite_action: block
  Unsupported_suite_log: log
  Untrusted_cert_chain_action: block
  Untrusted_cert_chain_action_log: log
  Reference: 0
Router(config)# ssl-inspection statistics collect
Router(config)# show ssl-inspection statistics collect
collect statistics: yes
collect statistics time: since 2014-06-20 05:47:37 to 2014-06-20 05:47:55
Router(config)# show ssl-inspection statistics summary
maximum concurrent sessions  : 1000
concurrent sessions          : 0

total ssl sessions           : 0
  sessions inspected         : 0
     decrypted Kbytes        : 0
     encrypted Kbytes        : 0
  sessions blocked           : 0
  sessions passed            : 0

Router(config)#
```

41

Device HA

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

Figure 24 Device HA Backup Taking Over for the Master



41.1 Device HA Overview

Active-Passive Mode

- Active-passive mode lets a backup ZyWALL / USG take over if the master ZyWALL / USG fails.
- The ZyWALL / USGs must all support and be set to use the same device HA mode (either active-passive or legacy).

Management Access

You can configure a separate management IP address for each interface. You can use it to access the ZyWALL / USG for management whether the ZyWALL / USG is the master or a backup. The management IP address should be in the same subnet as the interface IP address.

Synchronization

Use synchronization to have a backup ZyWALL / USG copy the master ZyWALL / USG's configuration, signatures (anti-virus, IDP/application patrol, and system protect), and certificates.

Note: Only ZyWALL / USGs of the same model and firmware version can synchronize.

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

41.1.1 Before You Begin

- Configure a static IP address for each interface that you will have device HA monitor.

Note: Subscribe to services on the backup ZyWALL / USG before synchronizing it with the master ZyWALL / USG.

- Synchronization includes updates for services to which the master and backup ZyWALL / USGs are both subscribed. For example, a backup subscribed to IDP/AppPatrol, but not anti-virus, gets IDP/AppPatrol updates from the master, but not anti-virus updates. It is highly recommended to subscribe the master and backup ZyWALL / USGs to the same services.

41.2 General Device HA Commands

This table lists the general commands for device HA.

Table 175 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`	Sets the ZyWALL / USG to use active-passive device HA.

41.3 Active-Passive Mode Device HA

Virtual Router

The master and backup ZyWALL / USG form a single ‘virtual router’.

Cluster ID

You can have multiple ZyWALL / USG virtual routers on your network. Use a different cluster ID to identify each virtual router.

Monitored Interfaces in Active-Passive Mode Device HA

You can select which interfaces device HA monitors. If a monitored interface on the ZyWALL / USG loses its connection, device HA has the backup ZyWALL / USG take over.

Enable monitoring for the same interfaces on the master and backup ZyWALL / USGs. Each monitored interface must have a static IP address and be connected to the same subnet as the corresponding interface on the backup or master ZyWALL / USG.

Virtual Router and Management IP Addresses

- If a backup takes over for the master, it uses the master’s IP addresses. These IP addresses are know as the virtual router IP addresses.

- Each interface can also have a management IP address. You can connect to this IP address to manage the ZyWALL / USG regardless of whether it is the master or the backup.

41.4 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 176 Input Values for device-ha Commands

LABEL	DESCRIPTION
interface_name	The name of the interface. This depends on the ZyWALL / USG model. For some ZyWALL / USG models, use ge*x*, *x* = 1 ~ N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model. For other ZyWALL / USG models, use a name such as wan1, wan2, opt, lan1, 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.

41.4.1 Active-Passive Mode Device HA Commands

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

Table 177 device-ha ap-mode Commands

COMMAND	DESCRIPTION
[no] device-ha ap-mode preempt	Turn on preempt if this ZyWALL / USG should become the master ZyWALL / USG if a lower-priority ZyWALL / USG is the master when this ZyWALL / USG is enabled.
device-ha ap-mode role {master|backup}	Sets the ZyWALL / USG to be the master or a backup in the virtual router.
device-ha ap-mode cluster-id <1..32>	Sets the cluster ID number. A virtual router consists of a master ZyWALL / USG and all of its backup ZyWALL / USGs. If you have multiple ZyWALL / USG virtual routers on your network, use a different cluster ID for each virtual router.
device-ha ap-mode priority <1..254>	Sets backup ZyWALL / USG's priority. The backup ZyWALL / USG with the highest value takes over the role of the master ZyWALL / USG if the master ZyWALL / USG becomes unavailable. The priority must be between 1 and 254. (The master interface has priority 255.)
[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 (+-/*= :; .! @$&%#~ ‘ \ ()). ah-md5: Use an encrypted MD5 password for authentication. *key* - Use up to eight characters including alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ ()).
[no] device-ha ap-mode *interface_name* manage-ip *ip subnet_mask*	Sets the management IP address for an interface.

Table 177 device-ha ap-mode Commands (continued)

COMMAND	DESCRIPTION
`[no] device-ha ap-mode` *`interface_name`* `activate`	Has device HA monitor the status of an interface's connection.
`[no] device-ha ap-mode master sync authentication password` *`password`*	This is for a master ZyWALL / USG. It specifies the password to require from synchronizing backup ZyWALL / USGs. Every router in the virtual router must use the same password. The `no` command sets the password setting to blank (which means no backups can synchronize with this master). *`password`*: Use 4-63 alphanumeric characters, underscores (_), dashes (-), and `#%^*={}:,.~` characters.
`[no] device-ha ap-mode backup sync authentication password` *`password`*	Sets the password the backup ZyWALL / USG uses when synchronizing with the master. The `no` command sets the password setting to blank (which means this backup ZyWALL / USG cannot synchronize with the master). *`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 <5..1440>`	When you use automatic synchronization, this sets how often (in minutes) the ZyWALL / USG synchronizes with the master.
`[no] device-ha ap-mode backup sync from` *`master_address`* `port` *`port`*	Sets the address of the master ZyWALL / USG with which this backup ZyWALL / USG is to synchronize. *`master_address`*: The master ZyWALL / USG's IP address or fully-qualified domain name (FQDN). *`port`*: The master ZyWALL / USG's FTP port number.
`device-ha ap-mode backup sync now`	Synchronize now.
`show device-ha ap-mode interfaces`	Displays the device HA AP mode interface settings and status.
`show device-ha ap-mode next-sync-time`	Displays the next time and date (in hh:mm yyyy-mm-dd format) the ZyWALL / USG will synchronize with the master.
`show device-ha ap-mode status`	Displays the ZyWALL / USG's key device HA settings.
`show device-ha ap-mode master sync`	Displays the master ZyWALL / USG's synchronization settings.
`show device-ha ap-mode backup sync`	Displays the backup ZyWALL / USG's synchronization settings.
`show device-ha ap-mode backup sync status`	Displays the backup ZyWALL / USG's current synchronization status.
`show device-ha ap-mode backup sync summary`	Displays the backup ZyWALL / USG's synchronization settings.
`show device-ha ap-mode forwarding-port` *`interface_name`*	If you apply Device HA on a bridge interface on a backup ZyWALL / USG, you can use this command to see which port in the bridge interface is chosen to receive VRRP packets used to monitor if the master ZyWALL / USG goes down. *`interface_name`*: This is a bridge interface, For example, brx.

41.4.2 Active-Passive Mode Device HA Command Example

This example configures a ZyWALL / USG to be a master ZyWALL / USG for active-passive mode device HA. There is a management IP address of 192.168.1.3 on lan1. wan1 and lan1 are monitored. The synchronization password is set to “mySyncPassword”.

```
Router(config)# device-ha ap-mode lan1 manage-ip 192.168.1.3 255.255.255.0
Router(config)# device-ha ap-mode role master
Router(config)# device-ha ap-mode master sync authentication password mySyncPassword
Router(config)# device-ha ap-mode wan1 activate
Router(config)# device-ha ap-mode lan1 activate
Router(config)# device-ha activate
```

41.5 Device HA Pro

You need a license to use Device HA Pro. Device HA Pro is easier to deploy than Device HA, is more reliable (no risk of overloading), and faster (Device HA causes a connection break of 10~30 seconds while Device HA Pro just has 1~2 seconds). In addition to configuration file backup in Device HA, device time, TCP sessions (IPv4/IPv6), IPSec VPN sessions, login/logout information and license status can also be backed up using Device HA Pro.

Active and Passive Devices

Device HA Pro uses a dedicated heartbeat link between an active device (‘master’) and a passive device (‘backup’) for status syncing and backup to the passive device. On the passive device, all ports are disabled except for the port with the heartbeat link.

Note: The dedicated heartbeat link port must be the highest-numbered port on each ZyWALL / USG for Device HA Pro to work.

Failover from the active ZyWALL / USG to the passive ZyWALL / USG is activated when:

- A monitored interface is down
- A monitored service (daemon) is down
- The hearbeat link exceeds the failure tolerance.

After failover, the initial active ZyWALL / USG becomes the passive ZyWALL / USG after it recovers.

41.5.1 Deploying Device HA Pro

1 Register either the active or passive ZyWALL / USG with a Device HA Pro license at MyZyXEL.com. Check that it’s properly licensed in **Licensing > Registration > Service** in the active ZyWALL / USG.

2 Make sure the passive ZyWALL / USG is offline, then enable Device HA in **Device HA > General** in the passive ZyWALL / USG.

3 Must make sure the FTP port in **System > FTP** (default 21) is the same on both ZyWALL / USGs. FTP is used for transferring files in the event of failover from active to passive ZyWALL / USG.

4 Connect the passive ZyWALL / USG to the active ZyWALL / USG using the highest-numbered ports on both ZyWALL / USGs.

Note: If both ZyWALL / USGs are turned on at the same time with Device HA enabled, then they may send the heartbeat at the same time. In this case, the ZyWALL / USG with the bigger MAC address becomes the passive ZyWALL / USG.

41.5.2 Device HA Pro Commands

This table lists the commands for Device HA Pro (device-ha2).

Table 178 device-ha2 (Device HA Pro) Commands

COMMAND	DESCRIPTION
`[no] device-ha2 activate`	Turns Device HA Pro on or off (no).
`[no] device-ha2` *`interface_name`* `activate`	Turns Device HA Pro monitoring on or off (no) on the specified interface.
`[no] device-ha2 manage-ip` *`ip1 ip2 subnet_mask`*	Sets or removes (no) the IPv4 address and subnet mask of the heartbeat dedicated link port (the highest-numbered port) on the active and passive ZyWALL / USG. *`ip1`*: IPv4 address of the active ZyWALL / USG. *`ip2`*: IPv4 address of the passive ZyWALL / USG.
`device-ha2 sync password` *`password`*	Sets a synchronization password of between 1 and 32 single-byte printable characters.
`[no] device-ha2 sync password`	Enables or disables (no) being prompted for the password before synchronization takes place.
`[no] device-ha2 srv-monitor`	Enables or disables (no) service monitoring. When enabled, the passive ZyWALL / USG takes over when a monitored service daemon on the active ZyWALL / USG fails.
`[no] device-ha2 connchk-monitor`	Enables or disables (no) connection check monitoring. When enabled, the passive ZyWALL / USG takes over when a monitored interface on the active ZyWALL / USG fails.
`device-ha2 heartbeat period <1..10> fail-tolerance <1..10>`	Sets when failover is activated on the passive ZyWALL / USG. ZyWALL / USG will change to active mode if it doesn't receive a heartbeat after `heartbeat period` x `fail-tolerance` seconds. `heartbeat period`: the number of seconds (1-10) allowed for absence of a heartbeat signal. `fail-tolerance`: the number of heartbeat failures allowed.
`device-ha2 license-sync` *`serial_number`*	Sets the serial number of the ZyWALL / USG (active or passive) with the Device HA Pro subscribed license.
`device-ha2 virtual-mac` *`zynos_style_mac_address`*	Specifies the Virtual MAC address of a port on the active ZyWALL / USG. Virtual MAC is a shared MAC address which is owned by the active ZyWALL / USG. All traffic can communicate with this shared MAC address, allowing the backup ZyWALL / USG to pick up traffic seamlessly. *`zynos_style_mac_address`*: The first (wan0) MAC address of the ZyWALL / USG. A ZyXEL-style MAC address must use the ZyXEL OUI (Organizationally Unique Identifier) such as **00-13-49**-XX-XX-XX.
`device-ha2 failover-count <5 ..50>`	Sets the maximum number of times a ZyWALL / USG can change from active to passive mode. The ZyWALL / USG won't change to passive mode if it's already changed to passive mode `failover-count` times. This is to prevent too many changes between active and passive mode.
`show device-ha2 activation`	Displays whether or not Device HA Pro is activated.

Table 178 device-ha2 (Device HA Pro) Commands (continued)

COMMAND	DESCRIPTION
`show device-ha2 interfaces`	Displays Device HA Pro monitored interfaces.
`show device-ha2 log`	Displays Device HA Pro logs.
`show device-ha2 virtual-mac`	Displays Device HA Pro virtual MAC address.
`show device-ha2 mode`	Displays Device HA Pro mode.
`show device-ha status`	Displays whether or not device HA is activated, the configured device HA mode, and the status of the monitored interfaces.

42

User/Group

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

42.1 User Account Overview

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

42.1.1 User Types

There are the types of user accounts the ZyWALL / USG uses.

Table 179 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
Admin	Change ZyWALL / USG configuration (web, CLI)	WWW, TELNET, SSH, FTP
Limited-Admin	Look at ZyWALL / USG configuration (web, CLI) 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 48 on page 343 for more information about authentication methods.)

42.2 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 180 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.

42.2.1 User Commands

The first table lists the commands for users.

Table 181 username/groupname Commands Summary: Users

COMMAND	DESCRIPTION
`show username [`*`username`*`]`	Displays information about the specified user or about all users set up in the ZyWALL / USG.
`username `*`username`*` nopassword user-type {admin | guest | limited-admin | user}`	Creates the specified user (if necessary), disables the password, and sets the user type for the specified user.
`username `*`username`*` password `*`password`*` user-type {admin | guest | limited-admin | user}`	Creates the specified user (if necessary); enables and sets the password; and sets the user type for the specified user. *`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 mac-address`	Creates the specified user (if necessary) and sets the user type to **mac-address**.
`username `*`username`*` user-type ext-group-user associated-aaa-server `*`server_profile`*` group-id `*`id`*	Specifies 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.
`username username encrypted-password <`*`password`*`>`	Sets the password for the specified user.
`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`*` logon-time-setting <default | manual>`	Sets the account to use the factory default lease and reauthentication times or custom ones.

Table 181 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).

42.2.2 User Group Commands

This table lists the commands for groups.

Table 182 username/groupname Commands Summary: Groups

COMMAND	DESCRIPTION
`show groupname [`*`groupname`*`]`	Displays information about the specified user group or about all user groups set up in the ZyWALL / USG.
`[no] groupname` *`groupname`*	Creates the specified user group if necessary and enters sub-command mode. The `no` command deletes the specified user group.
`[no] description` *`description`*	Sets the description for the specified user group. The `no` command clears the description for the specified user group.
`[no] groupname` *`groupname`*	Adds the specified user group (second *groupname*) to the specified user group (first *groupname*).
`[no] user` *`username`*	Adds the specified user to the specified user group.
`groupname rename` *`groupname groupname`*	Renames the specified user group (first *groupname*) to the specified group-name (second *groupname*).

42.2.3 User Setting Commands

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

Table 183 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 183 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.

42.2.3.1 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
```

42.2.4 MAC Auth Commands

This table lists the commands for mappings MAC addresses to MAC address user accounts.

Table 184 mac-auth Commands Summary

COMMAND	DESCRIPTION
`[no] mac-auth database mac` *`mac_address`* `type ext-mac-address mac-role` *`username`* `description` *`description`*	Maps the specified MAC address authenticated by an external server to the specified MAC role (MAC address user account). The `no` command deletes the mapping between the MAC address and the MAC role.
`[no] mac-auth database mac` *`mac_address`* `type int-mac-address mac-role` *`username`* `description` *`description`*	Maps the specified MAC address authenticated by the ZyWALL / USG's local user database to the specified MAC role (MAC address user account). The `no` command deletes the mapping between the MAC address and the MAC role.
`[no] mac-auth database mac` *`oui`* `type ext-oui mac-role` *`username`* `description` *`description`*	Maps the specified OUI (Organizationally Unique Identifier) authenticated by an external server to the specified MAC role (MAC address user account). The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device. The `no` command deletes the mapping between the OUI and the MAC role.
`[no] mac-auth database mac` *`oui`* `type int-oui mac-role` *`username`* `description` *`description`*	Maps the specified OUI (Organizationally Unique Identifier) authenticated by the ZyWALL / USG's local user database to the specified MAC role (MAC address user account). The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device. The `no` command deletes the mapping between the OUI and the MAC role.

42.2.4.1 MAC Auth Example

This example uses an external server to authenticate wireless clients by MAC address. After authentication the ZyWALL / USG maps the wireless client to a mac-address user account (MAC role). Configure user-aware features to control MAC address user access to network services.

The following commands:

- Create a MAC role (mac-address user type user account) named ZyXEL-mac
- Map a wireless client's MAC address of 00:13:49:11:a0:c4 to the ZyXEL-mac MAC role (MAC address user account)
- Modify the WLAN security profile named secureWLAN1 as follows:
  - Turn on MAC authentication
  - Use the authentication method named Auth1
  - Use colons to separate the two-character pairs within account MAC addresses

- Use upper case letters in the account MAC addresses

```
Router(config)# username ZyXEL-mac user-type mac-address
Router(config)# mac-auth database mac 00:13:49:11:a0:c4 type ext-mac-address mac-role
ZyXEL-mac description zyxel mac

3. Modify wlan-security-profile
Router(config)# wlan-security-profile secureWLAN1
Router(config-wlan-security default)# mac-auth activate
Router(config-wlan-security default)# mac-auth auth-method Auth1
Router(config-wlan-security default)# mac-auth delimiter account colon
Router(config-wlan-security default)# mac-auth case account upper
Router(config-wlan-security default)# exit
```

42.2.5 Additional User Commands

This table lists additional commands for users.

Table 185 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.

42.2.5.1 Additional User Command Examples

The following commands display the users that are currently logged in to the ZyWALL / USG and forces the logout of all logins from a specific IP address.

```
Router# configure terminal
Router(config)# show users all
No: 0
  Name: admin
  Type: admin
  From: console
  Service: console
  Session_Time: 25:46:00
  Idle_Time: unlimited
  Lease_Timeout: unlimited
  Re_Auth_Timeout: unlimited
  User_Info: admin
No: 1
  Name: admin
  Type: admin
  From: 192.168.1.34
  Service: http/https
  Session_Time: 00:02:26
  Idle_Time: unlimited
  Lease_Timeout: unlimited
  Re_Auth_Timeout: unlimited
  User_Info: admin
Router(config)# users force-logout 192.168.1.34
Logout user 'admin'(from 192.168.1.34 ): OK
Total 1 user has been forced logout
Router(config)# show users all
No: 0
  Name: admin
  Type: admin
  From: console
  Service: console
  Session_Time: 25:48:33
  Idle_Time: unlimited
  Lease_Timeout: unlimited
  Re_Auth_Timeout: unlimited
  User_Info: admin
```

The following commands display the users that are currently locked out and then unlocks the user who is displayed.

```
Router# configure terminal
Router(config)# show lockout-users
No.  Username Tried                  From            Lockout Time Remaining
===========================================================================
No.  From            Failed Login Attempt    Record Expired Timer
===========================================================================1
172.16.1.5             2                       46

Router(config)# unlock lockout-users 172.16.1.5
User from 172.16.1.5 is unlocked
Router(config)# show lockout-users
No.  Username Tried                  From            Lockout Time Remaining
===========================================================================
No.  From            Failed Login Attempt    Record Expired Timer
===========================================================================
```

43

Application Object

Check that you have the latest IDP and App Patrol signatures.

43.1 Application Object Commands Summary

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

Table 186 Input Values for Application Object Commands

LABEL	DESCRIPTION
<object>	Type the name of the object.
<description>	This is a description of the object
<sid>	This is the associated IDP and App Patrol signature ID number.

43.1.1 Application Object Commands

This table lists the application object commands.

Table 187 application-object Commands

COMMAND	DESCRIPTION
show application-object *<object>*	Displays information on the named application object.
application-object *<object>*	Creates an object with the specified name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. The no command disables it.
[no] description *<description>*	Write a description of the object.
[no] application *<sid>*	Write a valid signature ID for the object. The no command disables it.
no application-object *<object>*	Deletes the object with the specified name.
application-object rename *<object>* *<object>*	Renames the specified object with a new name.

43.1.1.1 application-object Examples

These are some example usage commands.

```
Router(config)# show application-object
Name
Description                                                  Ref
Content
===============================================================================
tests
New Create                                                   1
Facebook Game (access)
Router(config)# show application-object tests
Name: tests
Description: New Create
Category                        Application
Application ID
===============================================================================
Social Network                  Facebook Game (access)
402685702
Router(config)#
```

43.1.2 Application Object Group Commands

This table lists the application object group commands.

Table 188 object-group application Commands

COMMAND	DESCRIPTION
show object-group application <*object*>	Displays information on the named application object group.
object-group application <*object*>	Creates an object group. with the specified name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. The no command disables it.
[no] description <*description*>	Write a description of the object group.
[no] application-object <*object*>	Adds the named application object to the object group. The no command removes it.
[no] object-group <*object*>	Creates an object group. The no command removes it.
no object-group application <*object*>	Deletes the object group with the specified name.
object-group application rename <*object*> <*object*>	Renames the specified object group with a new name.

43.1.2.1 `object-group application` Examples

These are some example usage commands.

```
Router(config)# show object-group application
Name
Description                                                  Ref
Member
===============================================================================
Router(config)# object-group application may
Router(group-application)# description rinse after use
Router(group-application)# exit
Router(config)# show object-group application
Name
Description                                                  Ref
Member
===============================================================================
may
rinse after use                                              0
tests
Router(config)#
```

44

Addresses

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

44.1 Address Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

You can create IP address objects based on an interface's IP address, subnet, or gateway. The ZyWALL / USG automatically updates these objects whenever the interface's IP address settings change. This way every rule or setting that uses the object uses the updated IP address settings. For example, if you change the LAN1 interface's IP address, the ZyWALL / USG automatically updates the corresponding interface-based, LAN1 subnet address object. So any configuration that uses the LAN1 subnet address object is also updated.

Address objects and address groups are used in dynamic routes, firewall rules, application patrol, content filtering, and VPN connection policies. For example, addresses are used to specify where content restrictions apply in content filtering. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

44.2 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 189 Input Values for Address Commands

LABEL	DESCRIPTION
object_name	The name of the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
group_name	The name of the address group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
interface_name	The name of the interface. This depends on the ZyWALL / USG model. For some modelsFor some models, use ge*x*, *x* = 1 ~ N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model. For other models, use a name such as wan1, wan2, opt, lan1, or dmz.

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

44.2.1 Address Object Commands

This table lists the commands for address objects.

Table 190 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.

44.2.1.1 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
```

44.2.2 Address Group Commands

This table lists the commands for address groups.

Table 191 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 191 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`*.

44.2.2.1 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
```

45

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.

45.1 Services Overview

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

45.2 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 192 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.

45.2.1 Service Object Commands

The first table lists the commands for service objects.

Table 193 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 193 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.

45.2.1.1 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
```

45.2.2 Service Group Commands

The first table lists the commands for service groups.

Table 194 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 194 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*.

45.2.2.1 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
```

Schedules

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

46.1 Schedule Overview

The ZyWALL / USG supports two types of schedules: one-time and recurring. One-time schedules are effective only once, while recurring schedules usually repeat.

Note: Schedules are based on the current date and time in the ZyWALL / USG.

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.

46.2 Schedule Commands Summary

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

Table 195 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 196 schedule Commands

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

Table 196 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

46.2.1 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
```

47

AAA Server

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

47.1 AAA Server Overview

You can use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network.

The following lists the types of authentication server the ZyWALL / USG supports.

- Local user database

  The ZyWALL / USG uses the built-in local user database to authenticate administrative users logging into the ZyWALL / USG's web configurator or network access users logging into the network through the ZyWALL / USG. You can also use the local user database to authenticate VPN users.
- Directory Service (LDAP/AD)

  LDAP (Lightweight Directory Access Protocol)/AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.
- RADIUS

  RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

47.2 Authentication Server Command Summary

This section describes the commands for authentication server settings.

47.2.1 ad-server Commands

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

Table 197 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 197 ad-server Commands (continued)

COMMAND	DESCRIPTION
`[no] ad-server binddn` *`binddn`*	Sets the user name the ZyWALL / USG uses to log into the default AD server. The `no` command clears this setting.
`[no] ad-server cn-identifier` *`uid`*	Sets the unique common name (cn) to identify a record. The `no` command clears this setting.
`[no] ad-server host` *`ad_server`*	Sets the AD server address. Enter the IP address (in dotted decimal notation) or the domain name. The `no` command clears this setting.
`[no] ad-server password` *`password`*	Sets the bind password. This password will be encrypted when you use the show ad-server command to display. The `no` command clears this setting.
`[no] ad-server password-encrypted` *`password`*	Sets the encrypted password (less than 32 alphanumerical characters) in order to hide the real password from people behind you when you are configuring AD server password. This password is displayed as what you typed when you use the show ad-server command.
`[no] ad-server port` *`port_no`*	Sets the AD port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting.
`[no] ad-server search-time-limit` *`time`*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The `no` command clears this setting.
`[no] ad-server ssl`	Enables the ZyWALL / USG to establish a secure connection to the AD server. The `no` command disables this feature.

47.2.2 ldap-server Commands

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

Table 198 ldap-server Commands

COMMAND	DESCRIPTION
`show ldap-server`	Displays current LDAP server settings.
`[no] ldap-server basedn` *`basedn`*	Sets a base distinguished name (DN) for the default LDAP server. A base DN identifies an LDAP directory. The `no` command clears this setting.
`[no] ldap-server binddn` *`binddn`*	Sets the user name the ZyWALL / USG uses to log into the default LDAP server. 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 / USG to establish a secure connection to the LDAP server. The `no` command disables this feature.

47.2.3 radius-server Commands

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

Table 199 radius-server Commands

COMMAND	DESCRIPTION
`show radius-server`	Displays the default RADIUS server settings.
`[no] radius-server host` *`radius_server`* `auth-port` *`auth_port`*	Sets the RADIUS server address and service port number. Enter the IP address (in dotted decimal notation) or the domain name of a RADIUS server. The `no` command clears the settings.
`[no] radius-server key` *`secret`*	Sets a password (up to 15 alphanumeric characters) as the key to be shared between the RADIUS server and the ZyWALL / USG. The `no` command clears this setting.
`[no] radius-server timeout` *`time`*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The `no` command clears this setting.

47.2.4 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)#
```

47.2.5 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 200 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 200 aaa group server ad Commands (continued)

COMMAND	DESCRIPTION
`[no] server alternative-cn-identifier` *`uid`*	Sets the second type of identifier that the users can use to log in if any. For example “name” or “e-mail address”. The no command clears this setting.
`[no] server basedn` *`basedn`*	Sets the base DN to point to the AD directory on the AD server group. The no command clears this setting.
`[no] server binddn` *`binddn`*	Sets the user name the ZyWALL / USG uses to log into the AD server group. The no command clears this setting.
`[no] server cn-identifier` *`uid`*	Sets the user name the ZyWALL / USG uses to log into the AD server group. The no command clears this setting.
`[no] server description` *`description`*	Sets the descriptive information for the AD server group. You can use up to 60 printable ASCII characters. The no command clears the setting.
`[no] server group-attribute` *`group-attribute`*	Sets the name of the attribute that the ZyWALL / USG is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values. For example you could have an attribute named “memberOf” with values like “sales”, “RD”, and “management”. Then you could also create an ext-group-user user object for each group. One with “sales” as the group identifier, another for “RD” and a third for “management”. The no command clears the setting.
`[no] server host` *`ad_server`*	Enter the IP address (in dotted decimal notation) or the domain name of an AD server to add to this group. The no command clears this setting.
`[no] server password` *`password`*	Sets the bind password (up to 15 alphanumerical characters). The no command clears this setting.
`[no] server port` *`port_no`*	Sets the AD port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting.
`[no] server search-time-limit` *`time`*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting and set this to the default setting of 5 seconds.
`[no] server ssl`	Enables the ZyWALL / USG to establish a secure connection to the AD server. The no command disables this feature.

47.2.6 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 201 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 201 aaa group server ldap Commands (continued)

COMMAND	DESCRIPTION
`[no] case-sensitive`	Specify whether or not the server checks the username case. Set this to be the same as the server's behavior.
`[no] server alternative-cn-identifier` *uid*	Sets the second type of identifier that the users can use to log in if any. For example "name" or "e-mail address". The no command clears this setting.
`[no] server basedn` *basedn*	Sets the base DN to point to the LDAP directory on the LDAP server group. The no command clears this setting.
`[no] server binddn` *binddn*	Sets the user name the ZyWALL / USG uses to log into the LDAP server group. The no command clears this setting.
`[no] server cn-identifier` *uid*	Sets the user name the ZyWALL / USG uses to log into the LDAP server group. The no command clears this setting.
`[no] server description` *description*	Sets the descriptive information for the LDAP server group. You can use up to 60 printable ASCII characters. The no command clears this setting.
`[no] server group-attribute` *group-attribute*	Sets the name of the attribute that the ZyWALL / USG is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values. For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create an ext-group-user user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management". The no command clears the setting.
`[no] server host` *ldap_server*	Enter the IP address (in dotted decimal notation) or the domain name of an LDAP server to add to this group. The no command clears this setting.
`[no] server password` *password*	Sets the bind password (up to 15 characters). The no command clears this setting.
`[no] server port` *port_no*	Sets the LDAP port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting.
`[no] server search-time-limit` *time*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting and set this to the default setting of 5 seconds.
`[no] server ssl`	Enables the ZyWALL / USG to establish a secure connection to the LDAP server. The no command disables this feature.

47.2.7 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 202 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 202 aaa group server radius Commands (continued)

COMMAND	DESCRIPTION
`aaa group server radius` *`group-name`*	Enter the sub-command mode.
`[no] case-sensitive`	Specify whether or not the server checks the username case. Set this to be the same as the server's behavior.
`[no] server description` *`description`*	Sets the descriptive information for the RADIUS server group. You can use up to 60 printable ASCII characters. The `no` command clears the setting.
`[no] server group-attribute <1-255>`	Sets the value of an attribute that the ZyWALL / USG is used to determine to which group a user belongs. 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 / USG. The `no` command clears this setting.
`[no] server timeout` *`time`*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The `no` command clears this setting and set this to the default setting of 5 seconds.

47.2.8 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
```

48

Authentication Objects

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

48.1 Authentication Objects Overview

After you have created the AAA server objects, you can specify the authentication objects (containing the AAA server information) that the ZyWALL / USG uses to authenticate users (using VPN or managing through HTTP/HTTPS).

48.2 aaa authentication Commands

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

Table 203 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.
`aaa authentication default` *`member`*`1 [`*`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.

Table 203 aaa authentication Commands (continued)

COMMAND	DESCRIPTION
aaa authentication *profile-name member*1 [*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.
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.

48.2.1 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)#
```

48.3 test aaa Command

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

Table 204 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.

48.3.1 Test a User Account Command Example

The following example shows how to test whether a user account named userABC exists on the AD authentication server which uses the following settings:

- IP address: 172.16.50.1
- Port: 389
- Base-dn: DC=ZyXEL,DC=com
- Bind-dn: zyxel\engineerABC

- Password: abcdefg
- Login-name-attribute: sAMAccountName

The result shows the account exists on the AD server. Otherwise, the ZyWALL / USG responds an error.

```
Router> test aaa server ad host 172.16.50.1 port 389 base-dn DC=ZyXEL,DC=com bind-dn
zyxel\engineerABC password abcdefg login-name-attribute sAMAccountName account
userABC

dn:: Q049MTIzNzco546L5aOr56uRKSxPVT1XaXRoTWFpbCxEQz1aeVhFTCxEQz1jb20=
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn:: MTIzNzco546L5aOr56uRKQ==
sn: User
l: 2341100
--------------------------SNIP!--------------------------------------------
```

49

Authentication Server

This chapter shows you how to configure the ZyWALL / USG as an authentication server for access points.

49.1 Authentication Server Overview

The ZyWALL / USG can also work as a RADIUS server to exchange messages with other APs for user authentication and authorization.

49.2 Authentication Server Commands

The following table lists the authentication server commands you use to configure the ZyWALL / USG's built-in authentication server settings.

Table 205 Command Summary: Authentication Server

COMMAND	DESCRIPTION
[no] auth-server activate	Sets the ZyWALL / USG to act as an authentication server for other RADIUS clients, such as APs. The no command sets the ZyWALL / USG to not act as an authentication server for other APs.
auth-server authentication *auth_method*	Specifies an authentication method used by the authentication server.
no auth-server authentication	Resets the authentication method used by the authentication server to the factory default (default).
[no] auth-server cert *certificate_name*	Specifies a certificate used by the authentication server (ZyWALL / USG). The no command resets the certificate used by the authentication server to the factory default (default). *certificate_name*: The name of the certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
[no] auth-server trusted-client *profile_name*	Creates a trusted RADIUS client profile. The no command deletes the specified profile. *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.
[no] activate	Enables the client profile. The no command disables the profile.
[no] ip address *ip subnet_mask*	Sets the client's IP address and subnet mask. The no command clears this setting.
[no] secret *secret*	Sets a password as the key to be shared between the ZyWALL / USG and the client. The no command clears this setting.

Table 205 Command Summary: Authentication Server (continued)

COMMAND	DESCRIPTION
[no] description *description*	Sets the description for the profile. The no command clears this setting. *description*: You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long.
show auth-server status	Displays the ZyWALL / USG's authentication server settings.
show auth-server trusted-client	Displays all RADIUS client profile settings.
show auth-server trusted-client *profile_name*	Displays the specified RADIUS client profile settings.

49.2.1 Authentication Server Command Examples

The following example shows you how to enable the authentication server feature on the ZyWALL / USG and sets a trusted RADIUS client profile. This example also shows you the authentication server and client profile settings.

```
Router# configure terminal
Router(config)# auth-server activate
Router(config)# auth-server trusted-client AP-1
Router(config-trusted-client-AP-1)# activate
Router(config-trusted-client-AP-1)# ip address 10.10.1.2 255.255.255.0
Router(config-trusted-client-AP-1)# secret 12345678
Router(config-trusted-client-AP-1)# exit
Router(config)# show auth-server status
activation: yes
authentication method: default
certificate: default
Router(config)# show auth-server trusted-client AP-1
Client: AP-1
  Activation: yes
  Description:
  IP: 10.10.1.2
  Netmask: 255.255.255.0
  Secret: VQEq907jWB8=
Router(config)#
```

50

Certificates

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

50.1 Certificates Overview

The ZyWALL / USG can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyWALL / USG to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

50.2 Certificate Commands

This section describes the commands for configuring certificates.

50.3 Certificates Commands Input Values

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

Table 206 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 206 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, 768, 1024, 1536, 2048, 4096). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
password	When you have the ZyWALL / USG enroll for a certificate immediately online, the certification authority may want you to include a key (password) to identify your certification request. Use up to 31 of the following characters. a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
ca_name	When you have the ZyWALL / USG enroll for a certificate immediately online, you must have the certification authority's certificate already imported as a trusted certificate. Specify the name of the certification authority's certificate. It can be up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
url	When you have the ZyWALL / USG enroll for a certificate immediately online, enter the IP address (or URL) of the certification authority server. You can use up to 511 of the following characters. a-zA-Z0-9'()+,/:.=?;!*#@$_%-
ipv4	Enter an IPv4 address.
ipv6	Enter an IPv6 address.

50.4 Certificates Commands Summary

The following table lists the commands that you can use to display and manage the ZyWALL / USG's summary list of certificates and certification requests. You can also create certificates or certification requests. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

Table 207 ca Commands Summary

COMMAND	DESCRIPTION
ca generate pkcs10 name *certificate_name* cn-type {ip cn *ipv4* | ipv6 cn *ipv6* |fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa|rsa-sha256|rsa-sha512|dsa-sha256} 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 *ipv4* | ipv6 cn *ipv6* | fqdn cn *cn_domain_name* | mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa|rsa-sha256|rsa-sha512|dsa-sha256} 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.
ca validation *remote_certificate*	Enters the sub command mode for validation of certificates signed by the specified remote (trusted) certificates.

Table 207 ca Commands Summary (continued)

COMMAND	DESCRIPTION
cdp {activate|deactivate}	Turns certificate revocation on or off. When it is turned on, the ZyWALL / USG validates a certificate by getting a Certificate Revocation List (CRL) through HTTP or LDAP (can be configured after activating the LDAP checking option) and online responder (can be configured after activating the OCSP checking option). You also need to configure the OSCP or LDAP server details.
ldap {activate|deactivate}	Has the ZyWALL / USG check (or not check) incoming certificates that are signed by this certificate against a Certificate Revocation List (CRL) on a LDAP (Lightweight Directory Access Protocol) directory server.
ldap ip {*ip*|*fqdn*} port <1..65535> [id *name* password *password*] [deactivate]	Sets the validation configuration for the specified remote (trusted) certificate where the directory server uses LDAP. *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 / USG may need to authenticate itself in order to access the CRL directory server. Type the login name (up to 31 characters) from the entity maintaining the server (usually a certification authority). You can use alphanumeric characters, the underscore and the dash. Type the password (up to 31 characters) from the entity maintaining the CRL directory server (usually a certification authority). You can use the following characters: a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
ocsp {activate|deactivate}	Has the ZyWALL / USG check (or not check) incoming certificates that are signed by this certificate against a directory server that uses OCSP (Online Certificate Status Protocol).
ocsp url *url* [id *name* password *password*] [deactivate]	Sets the validation configuration for the specified remote (trusted) certificate where the directory server uses OCSP. *url*: Type the protocol, IP address and pathname of the OCSP server. name: The ZyWALL / USG may need to authenticate itself in order to access the OCSP server. Type the login name (up to 31 characters) from the entity maintaining the server (usually a certification authority). You can use alphanumeric characters, the underscore and the dash. password: Type the password (up to 31 characters) from the entity maintaining the OCSP server (usually a certification authority). You can use the following characters: a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
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.
show ca category {local|remote} name *certificate_name* certpath	Displays the certification path of the specified local (my certificates) or remote (trusted certificates) certificate.

Table 207 ca Commands Summary (continued)

COMMAND	DESCRIPTION
`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.

50.5 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
```

51

ISP Accounts

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

51.1 ISP Accounts Overview

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

51.1.1 PPPoE and PPTP Account Commands

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

Table 208 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.
`encrypted-password` *`ciphertext`*	Sets a encrypted secret for the specified account. *`ciphertext`*:
`[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.

Table 208 PPPoE and PPTP ISP Account Commands (continued)

COMMAND	DESCRIPTION
`[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.
`[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 (:).

51.1.2 Cellular Account Commands

The following table lists the cellular ISP account commands.

Table 209 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. *isp_dial_string*: 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.

52

SSL Application

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

52.1 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.

52.1.1 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 210 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 SSL VPN. `owa`: (Outlook Web Access) to allow users to access e-mails, contacts, calenders via an Microsoft Outlook-like interface using supported web browsers. The ZyWALL / USG supports one OWA object. `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, remote 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 210 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 / USG 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 / USG uses a port number from this range to send traffic to the LAN computer that is being remotely managed.
`server-type weblink url` *`url`*	Sets this to create a link to a web site you specified that you expect the SSL VPN users to commonly use. *`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, remote 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.

52.1.2 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
```

53

DHCPv6 Objects

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

53.1 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 211 DHCPv6 Object Command Input Values

LABEL	DESCRIPTION
dhcp6_profile	The name of a DHCPv6 request object. Use a string of less than 31 characters.
interface_name	The name of the interface. This depends on the ZyWALL / USG model. For some models, use ge*x*, *x* = 1 ~ N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model. For other models, use a name such as wan1, wan2, opt, lan1, or dmz.

The following sections list the DHCPv6 object commands.

53.1.1 DHCPv6 Object Commands

This table lists the commands for DHCPv6 objects. Use the `configure terminal` command to enter the configuration mode to be able to use the commands that configure settings.

Table 212 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.
`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.

Table 212 DHCPv6 Object Commands (continued)

COMMAND	DESCRIPTION
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.

53.1.2 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 prefix 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 prefix 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
```

54

Dynamic Guest Accounts

54.1 Dynamic Guest Accounts Overview

Dynamic guest accounts are guest accounts, but are created dynamically and stored in the ZyWALL / USG's local user database. A dynamic guest account has a dynamically-created user name and password. A dynamic guest account user can access the ZyWALL / USG's services only within a given period of time and will become invalid after the expiration date/time.

There are three types of dynamic guest accounts depending on how they are created or authenticated: billing-users, ua-users and trial-users.

billing-users are guest account created with the `dynamic-guest generate` command or the guest manager account or an external printer and paid by cash or created and paid via the on-line payment service.

ua-users are users that log in from the user agreement page.

trial-users are free guest accounts that are created with the `dynamic-guest generate-freeuser` command or the Free Time function.

54.2 Dynamic-guest Commands

This table lists the `dynamic-guest` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 213 dynamic-guest Commands

COMMAND	DESCRIPTION
`dynamic-guest freeuser *user_name*`	Creates a free dynamic guest account (trial-user) with the specified user name and enters the dynamic-guest sub-command mode to set the password and timeout settings. See Table 214 on page 362 for the sub-commands.
`dynamic-guest generate`	Sets the ZyWALL / USG to automatically create a dynamic guest account (billing-user) and enters the dynamic-guest sub-command mode to set the password and timeout settings. See Table 214 on page 362 for the sub-commands.
`dynamic-guest generate-freeuser`	Sets the ZyWALL / USG to automatically create a free dynamic guest account (trial-user) and enters the dynamic-guest sub-command mode to set the password and timeout settings. See Table 214 on page 362 for the sub-commands.

Table 213 dynamic-guest Commands (continued)

COMMAND	DESCRIPTION
[no] dynamic-guest *user_name*	Creates a dynamic guest account (billing-user) with the specified user name and enters the dynamic-guest sub-command mode to set the password and timeout settings. See Table 214 on page 362 for the sub-commands. The no command removes the specified dynamic-guest account.
show dynamic-guest log	Displays all the dynamic guest accounts which are either active or expired.
show dynamic-guest log create-time begin *yyyy-mm-dd hh:mm* end *yyyy-mm-dd hh:mm*	Displays all the active and/or expired dynamic guest accounts that were generated within a specified period of time.
show dynamic-guest users	Displays all the active dynamic guest accounts on the ZyWALL / USG.

54.2.1 dynamic-guest Sub-commands

The following table describes the sub-commands for several dynamic-guest commands. Note that not all rule commands use all the sub-commands listed here.

Table 214 dynamic-guest Sub-commands

COMMAND	DESCRIPTION
bandwidth {upload | download} <0..1048576> priority <1..7>	Specifies the maximum bandwidth allowed for the user account in kilobits per second and types a number between 1 and 7 to set the priority for the user's traffic. The smaller the number, the higher the priority. upload refers to the traffic the ZyWALL / USG sends out from a user. download refers to the traffic the ZyWALL / USG sends to a user.
[no] bandwidth activate	Turns on bandwidth management for the user account. The no command disables bandwidth management for the user account.
charge *price*	Sets the account's price, up to 99999999.99, per time unit.
create-time *yyyy-mm-dd hh:mm*	Sets the date and time the account is created.
expire-time *yyyy-mm-dd hh:mm*	Sets the date and time the account becomes invalid.
password *password*	Sets the password for the account.
payment-info {cash | payment-service}	Sets the method of payment for the account.
phone *phone_number*	Sets the mobile phone number for the account.
quota {total | upload | download} megabytes <0..1023>	Sets how much downstream and/or upstream data in Megabytes can be transmitted through the external interface before the account expires. 0 means there is no data limit for the user account.
quota {total | upload | download} gigabytes <0..100>	Sets how much downstream and/or upstream data in Gigabytes can be transmitted through the external interface before the account expires. 0 means there is no data limit for the user account.
quota type {total | upload-download}	Sets a limit for the user account. This only applies to user's traffic that is received or transmitted through the external interface. Note: When the limit is exceeded, the user is not allowed to access the Internet through the ZyWALL / USG. total: set a limit on the total traffic in both directions. upload-download: set a limit on the upstream traffic and downstream traffic respectively.

Table 214 dynamic-guest Sub-commands (continued)

COMMAND	DESCRIPTION
`remaining-time <1..25920000>`	Sets the amount of Internet access time (in seconds) remaining for the account.
`time-period <1..432000>`	Sets the total account of time (in minutes) the account can use to access the Internet through the ZyWALL / USG.

54.2.2 Dynamic-guest Command Example

This example shows how to create a dynamic guest account, configure the account related settings and displays the account information.

```
Router# configure terminal
Router(config)# dynamic-guest generate
[dynamic guest] username:gn0ti7, password:ihzun7
Router(config-dynamic-guest)# charge 5
Router(config-dynamic-guest)# expire-time 2013-06-26 14:00
Router(config-dynamic-guest)# payment-info cash
Router(config-dynamic-guest)# phone 0912345678
Router(config-dynamic-guest)# time-period 1440
Router(config-dynamic-guest)# remaining-time 86400
Router(config-dynamic-guest)# create-time 2013-06-25 14:03
Router(config-dynamic-guest)# exit
Router(config)# show dynamic-guest users
No.   Status     Username   Create Time            Expiration Time
     Time Period          Remaining Time       Charge        ayment Info   Phone Num
     User Role
====================================================================================
1     Unused     gn0ti7    2013-06-25 14:03        2013-06-26 14:00
     1day 00:00:00        1day 00:00:00        eur 5,00        cash       0912345678
     billing-users
Router(config)#
```

55

System

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

55.1 System Overview

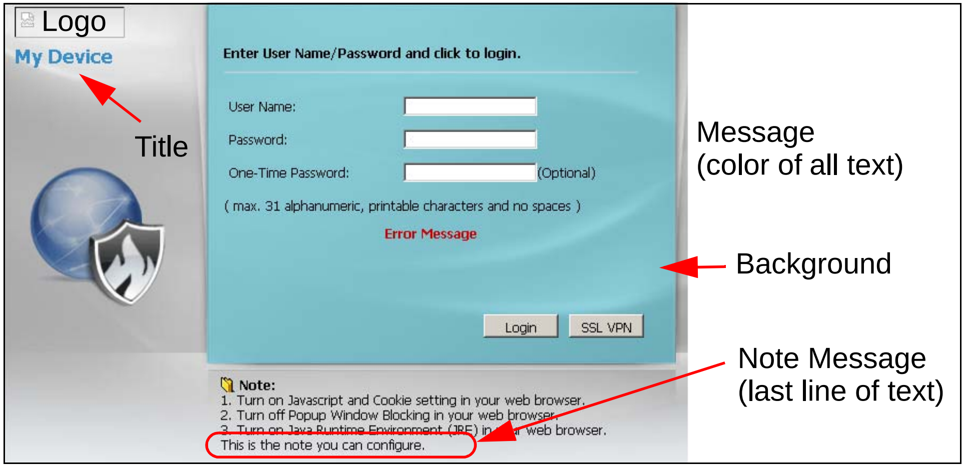
Use these commands to configure general ZyWALL / USG information, the system time and the console port connection speed for a terminal emulation program. They also allow you to configure DNS settings and determine which services/protocols can access which ZyWALL / USG zones (if any) from which computers.

55.2 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 42 on page 315 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



Enter User Name/Password and click to login.

User Name:

Password:

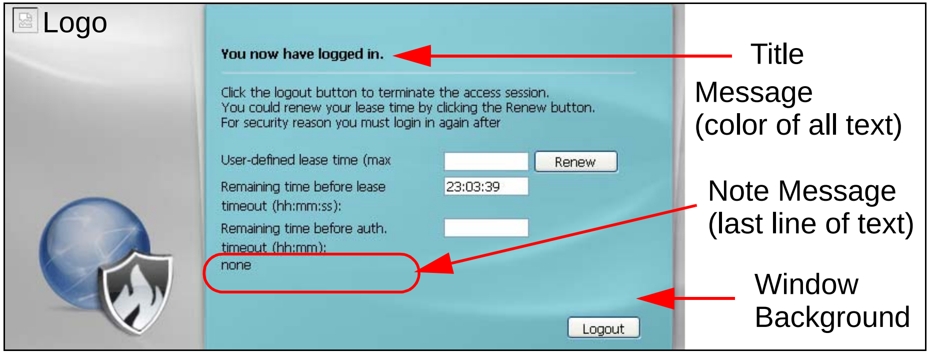
One-Time Password: (Optional)

(max. 31 alphanumeric, printable characters and no spaces)

Error Message

Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
This is the note you can configure.

Figure 26 Access Page Customization



You now have logged in.

Click the logout button to terminate the access session.
You could renew your lease time by clicking the Renew button.
For security reason you must login in again after

User-defined lease time (max

Remaining time before lease timeout (hh:mm:ss): 23:03:39

Remaining time before auth. timeout (hh:mm):

none

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 215 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 215 Command Summary: Customization (continued)

COMMAND	DESCRIPTION
`login-page window-color {`*`color-rgb`*` | `*`color-name`*` | `*`color-number`*`}`	Sets the color of the login page's window border.
`logo background-color {`*`color-rgb`*` | `*`color-name`*` | `*`color-number`*`}`	Sets the color of the logo banner across the top of the login screen and access page.
`show access-page settings`	Lists the current access page settings.
`show login-page default-title`	Lists the factory default title for the login page.
`show login-page settings`	Lists the current login page settings.
`show logo settings`	Lists the current logo background (banner) and floor (line below the banner) settings.
`show page-customization`	Lists whether the ZyWALL / USG is set to use custom login and access pages or the default ones.

55.3 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 216 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 / USG. The `no` command removes the host name.
`show fqdn`	Displays the fully qualified domain name.

55.4 Time and Date

For effective scheduling and logging, the ZyWALL / USG system time must be accurate. The ZyWALL / USG's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server.

55.4.1 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 217 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 savings. 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 savings 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:mm*`} [+|-]HH:MM.`	Sets your time zone where hh: hour `0-14`, mm: minute `0-59`). 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 an NTP time server.
`[no] clock auto-sync-timezone`	Allows the ZyWALL / USG to automatically update its time zone from the cloud server after the set and get commands below are issued. The `no` command disables the ZyWALL / USG from automatically updating its time zone from the cloud server.
`[no] clock auto-sync-daylight-saving`	Allows the ZyWALL / USG to automatically update its daylight savings adjusted time from the cloud server after the set and get commands below are issued. The `no` command disables the ZyWALL / USG from automatically updating daylight savings adjusted time from the cloud server.
`myzyxel-service get-cloud-timezone`	Sends a query to the cloud server to get both time-zone and daylight-savings information for where the ZyWALL / USG is located. The ZyWALL / USG keeps the result in a temporary file.
`myzyxel-service set-timezone-according-cloud`	Applies time-zone and daylight-savings settings according the information received from `myzyxel-service get-cloud-timezone` and if `clock auto-sync-timezone` and/or `clock auto-sync-daylight-saving` were issued. For example, if `clock auto-sync-timezone` was not issued, then ZyWALL / USG will not automatically update the time-zone.

Table 217 Command Summary: Date/Time (continued)

COMMAND	DESCRIPTION
`show myzyxel-service get-cloud-timezone`	Displays the time-zone, daylight savings time start-date, daylight savings time end-date and daylight savings time offset from the cloud server.
`show clock date`	Displays the current date of your ZyWALL / USG.
`show clock status`	Displays your time zone and daylight saving settings.
`show clock time`	Displays the current time of your ZyWALL / USG.
`show ntp server`	Displays time server settings.

55.5 Console Port Speed

This section shows you how to set the console port speed when you connect to the ZyWALL / USG via the console port using a terminal emulation program. The following table describes the console port commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 218 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.

55.6 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.

55.6.1 Domain Zone Forwarder

A domain zone forwarder contains a DNS server’s IP address. The ZyWALL / USG can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

A name query begins at a client computer and is passed to a resolver, a DNS client service, for resolution. The ZyWALL / USG can be a DNS client service. The ZyWALL / USG can resolve a DNS query locally using cached Resource Records (RR) obtained from a previous query (and kept for a period of time). If the ZyWALL / USG does not have the requested information, it can forward the request to DNS servers. This is known as recursion.

The ZyWALL / USG can ask a DNS server to use recursion to resolve its DNS client requests. If recursion on the ZyWALL / USG or a DNS server is disabled, they cannot forward DNS requests for resolution.

A Domain Name Server (DNS) amplification attack is a kind of Distributed Denial of Service (DDoS) attack that uses publicly accessible open DNS servers to flood a victim with DNS response traffic. An open DNS server is a DNS server which is willing to resolve recursive DNS queries from anyone on the Internet.

In a DNS amplification attack, an attacker sends a DNS name lookup request to an open DNS server with the source address spoofed as the victim's address. When the DNS server sends the DNS record response, it is sent to the victim. Attackers can request as much information as possible to maximize the amplification effect.

55.6.2 DNS Commands

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

Table 219 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 some ZyWALL / USG models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model. For other ZyWALL / USG models, use a name such as wan1, wan2, opt, lan1, 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 / USG 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 / USG model supports.

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

Table 220 Command Summary: DNS

COMMAND	DESCRIPTION
`[no] ip dns server a-record` *fqdn w.x.y.z*	Sets an A record that specifies the mapping of a fully qualified domain name (FQDN) to an IP address. The `no` command deletes an A record.
`ip dns server cache-flush`	Clears the DNS.
`[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.

Table 220 Command Summary: DNS (continued)

COMMAND	DESCRIPTION
`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 / USG 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 { ip_type }`*` [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 / USG connects to the DNS server through a VPN tunnel. Otherwise, use the `interface` command to set the interface through which the ZyWALL / USG sends DNS queries to a DNS server. The `auto` means any interface that the ZyWALL / USG uses to send DNS queries to a DNS server according to the routing rule.
`ip dns server zone-forwarder move <1..32> to <1..32>`	Changes the index number of a zone forwarder record.
`no ip dns server rule <1..32>`	Deletes a service control rule.
`show ip dns server`	Displays all DNS entries.
`show ip dns server database`	Displays all configured records.
`show ip dns server status`	Displays whether this service is enabled or not.
`show ip dns security-options all`	Displays security options configured for the customized and default rules.
`ip dns server aaaa-record {FQDN_DNS | FQDN_WILDCARD_DNS} IPv6`	An address record contains the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. Type a Fully-Qualified Domain Name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
`ip dns server cname-record {FQDN_DNS | FQDN_WILDCARD_DNS} {FQDN_DNS}`	A Canonical Name Record or CNAME record is a type of resource record in the Domain Name System (DNS) that specifies that the domain name is an alias of another, canonical domain name. Type a Fully-Qualified Domain Name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).

Table 220 Command Summary: DNS (continued)

COMMAND	DESCRIPTION
`ip dns security-options {default | 1}]`	Selects to use the default security option or profile ‘1’. The default allows any address to use `additional-from-cache` and `recursion`.
`name DNS_OPTIONS_NAME`	Names the DNS security options profile.
`no address-object-group {any | PROFILE}`	Sets the address object to be any or a previously created one. no removes the address object from this DNS security options profile.
`no additional-from-cache activate`	Activated allows the ZyWALL / USG to reply to queries with previously cached DNS requests. Deactivated (no) does not.
`no recursion activate`	Activated recursion allows the ZyWALL / USG to forward queries it can’t find in its DNS database. Deactivated (no) does not.

55.6.3 DNS Command Examples

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
```

This command displays security options configured for the customized and default rules.

```
Router# configure terminal
Router(config)# show ip dns security-options all
security option rule: 1
   Name: Customize
   Address Object: RFC1918_1, RFC1918_2, RFC1918_3
   Additional Info from Cache: allow
   Recursion Query: deny
security option rule: default
   Name: Default
   Address Object: any
   Additional Info from Cache: allow
   Recursion Query: allow
Router(config)#
```

55.7 Authentication Server Overview

The ZyWALL / USG can also work as a RADIUS server to exchange messages with other APs for user authentication and authorization.

55.7.1 Authentication Server Commands

The following table lists the authentication server commands you use to configure the ZyWALL / USG's built-in authentication server settings.

Table 221 Command Summary: Authentication Server

COMMAND	DESCRIPTION
`[no] auth-server activate`	Sets the ZyWALL / USG to act as an authentication server for other RADIUS clients, such as APs. The `no` command sets the ZyWALL / USG to not act as an authentication server for other APs.
`auth-server authentication` *`auth_method`*	Specifies an authentication method used by the authentication server.
`no auth-server authentication`	Resets the authentication method used by the authentication server to the factory default (`default`).
`[no] auth-server cert` *`certificate_name`*	Specifies a certificate used by the authentication server (ZyWALL / USG). The `no` command resets the certificate used by the authentication server to the factory default (`default`). *`certificate_name`*: The name of the certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
`[no] auth-server trusted-client` *`profile_name`*	Creates a trusted RADIUS client profile. The `no` command deletes the specified profile. *`profile-name`*: You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`[no] activate`	Enables the client profile. The `no` command disables the profile.
`[no] ip address` *`ip subnet_mask`*	Sets the client's IP address and subnet mask. The `no` command clears this setting.
`[no] secret` *`secret`*	Sets a password as the key to be shared between the ZyWALL / USG and the client. The `no` command clears this setting.
`[no] description` *`description`*	Sets the description for the profile. The `no` command clears this setting. *`description`*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
`show auth-server status`	Displays the ZyWALL / USG's authentication server settings.
`show auth-server trusted-client`	Displays all RADIUS client profile settings.
`show auth-server trusted-client` *`profile_name`*	Displays the specified RADIUS client profile settings.

55.7.2 Authentication Server Command Examples

The following example shows you how to enable the authentication server feature on the ZyWALL / USG and sets a trusted RADIUS client profile. This example also shows you the authentication server and client profile settings.

```
Router# configure terminal
Router(config)# auth-server activate
Router(config)# auth-server trusted-client AP-1
Router(config-trusted-client-AP-1)# activate
Router(config-trusted-client-AP-1)# ip address 10.10.1.2 255.255.255.0
Router(config-trusted-client-AP-1)# secret 12345678
Router(config-trusted-client-AP-1)# exit
Router(config)# show auth-server status
activation: yes
authentication method: default
certificate: default
Router(config)# show auth-server trusted-client AP-1
Client: AP-1
  Activation: yes
  Description:
  IP: 10.10.1.2
  Netmask: 255.255.255.0
  Secret: VQEq907jWB8=
Router(config)#
```

55.8 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 222 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.

55.9 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 223 Command Summary: IPv6

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

55.10 ZON Overview

The ZyXEL One Network (ZON) utility uses the ZyXEL Discovery Protocol (ZDP) for discovering and configuring ZDP-aware ZyXEL devices in the same broadcast domain as the computer on which ZON is installed.

The ZON Utility issues requests via ZDP and in response to the query, the ZyXEL device responds with basic information including IP address, firmware version, location, system and model name. The information is then displayed in the ZON Utility screen and you can perform tasks like basic configuration of the devices and batch firmware upgrade in it. You can download the ZON Utility at www.zyxel.com and install it on a computer.

55.10.1 LLDP

LLDP is a layer-2 protocol that allows a network device to advertise its identity and capabilities on the local network. It also allows the device to maintain and store information from adjacent devices which are directly connected to the network device. This helps you discover network changes and perform necessary network reconfiguration and management.

55.10.2 ZON Commands

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

Table 224 Command Summary: ZON

COMMAND	DESCRIPTION
`zon lldp server`	Activates LLDP discovery on the ZyWALL / USG. This allows you to use Link Layer Discovery Protocol (LLDP) for discovering and configuring LLDP-aware devices in the same broadcast domain as the ZyWALL / USG that you are logged into using the web configurator.
`zon lldp server tx-hold <1..10>`	Sets the multiplier used to calculate the TTL (Time To Live) value for the transmitted LLDP packets. The TTL value determines how long the device information can be saved on the neighbors. LLDP TTL = the multi pl er * the LLDP transmission interval

Table 224 Command Summary: ZON (continued)

COMMAND	DESCRIPTION
`zon lldp server tx-interval <1..600>`	Sets the interval (in seconds) at which the ZyWALL / USG sends a LLDP packet to the neighbor.
`zon zdp server`	Activates ZDP discovery on the ZyWALL / USG.
`show zon lldp neighbors`	Displays the ZyWALL / USG’s neighboring devices via LLDP.
`show zon lldp server config`	Displays the LLDP settings.
`show zon lldp server statistics`	Displays the LLDP traffic statistics.
`show zon lldp server status`	Displays whether LLDP discovery is enabled.
`show zon zdp server status`	Displays whether ZDP discovery is enabled.

55.10.3 ZON Examples

This example enables LLDP discovery and displays whether LLDP discovery is enabled on the ZyWALL / USG.

```
Router(config)# zon lldp server
Router(config)# zon lldp server status
status: active
Router(config)#
```

System Remote Management

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

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

56.1 Remote Management Overview

You may manage your ZyWALL / USG from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (LAN&WAN&DMZ)
- DMZ only

To disable remote management of a service, deselect **Enable** in the corresponding service screen.

56.1.1 Remote Management Limitations

Remote management will not work when:

1. You have disabled that service in the corresponding screen.
2. The accepted IP address in the **Service Control** table does not match the client IP address. If it does not match, the ZyWALL / USG will disconnect the session immediately.
3. There is a firewall rule that blocks it.

56.1.2 System Timeout

There is a lease timeout for administrators. The ZyWALL / USG automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the ZyWALL / USG for authentication again when the reauthentication time expires.

56.2 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 225 Input Values for General System Commands

LABEL	DESCRIPTION
address_object	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
rule_number	The number of a service control rule. 1 - *X* where *X* is the highest number of rules the ZyWALL / USG model supports.
zone_object	The name of the zone. For some ZyWALL / USG models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other ZyWALL / USG models, use pre-defined zone names like DMZ, LAN1, SSL VPN, IPSec VPN, OPT, and WAN.

56.3 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 226 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 / USG web configurator. The `no` command disables HTTPS access to the ZyWALL / USG web configurator.
`[no] ip http secure-server auth-client`	Sets the client to authenticate itself to the HTTPS server. The `no` command sets the client not to authenticate itself to the HTTPS server.

Table 226 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.
`[no] ip http secure-server sslv3`	Turns on SSLv3 support in the HTTP server. The `no` command turns SSLv3 support off.
ip http secure-server table {admin|user} rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny}	Sets a service control rule for HTTPS service.
ip http secure-server table {admin|user} rule move *rule_number* to *rule_number*	Changes the index number of a HTTPS service control rule.
ip http secure-server cipher-suite {*cipher_algorithm*} [*cipher_algorithm*] [*cipher_algorithm*] [*cipher_algorithm*]	Sets the encryption algorithms (up to four) that the ZyWALL / USG uses for the SSL in HTTPS connections and the sequence in which it uses them. The *cipher_algorithm* can be any of the following. `rc4`: RC4 (RC4 may impact the ZyWALL / USG's CPU performance since the ZyWALL / USG'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 / USG not use the specified encryption algorithm for the SSL in HTTPS connections.
`[no] ip http server`	Allows HTTP access to the ZyWALL / USG web configurator. The `no` command disables HTTP access to the ZyWALL / USG web configurator.
ip http server table {admin|user} rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny}	Sets a service control rule for HTTP service.
ip http server table {admin|user} rule move *rule_number* to *rule_number*	Changes the number of a HTTP service control rule.
no ip http secure-server table {admin|user} rule *rule_number*	Deletes a service control rule for HTTPS service.
no ip http server table {admin|user} rule *rule_number*	Deletes a service control rule for HTTP service.
`show ip http server status`	Displays HTTP settings.
`show ip http server secure status`	Displays HTTPS settings.
`ip http skip-csrf-check`	Omits cross-site request forgery (CSRF) checking. CSRF exploits the trust that a site has in a user's browser to transmit unauthorized commands as if they are from a user that the website trusts.
`no ip http skip-csrf-check`	Performs cross-site request forgery (CSRF) checking.
`show ip http skip-csrf-check`	Shows whether cross-site request forgery (CSRF) checking is done or not.

56.3.1 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 *Example* 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
```

56.4 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.

56.4.1 SSH Implementation on the ZyWALL / USG

Your ZyWALL / USG supports SSH versions 1 and 2 using RSA authentication and four encryption methods (AES, 3DES, Archfour, and Blowfish). The SSH server is implemented on the ZyWALL / USG for remote management on port 22 (by default).

56.4.2 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ZyWALL / USG over SSH.

56.4.3 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 227 Command Summary: SSH

COMMAND	DESCRIPTION
`[no] ip ssh server`	Allows SSH access to the ZyWALL / USG CLI. The no command disables SSH access to the ZyWALL / USG CLI.
[no] ip ssh server cert *certificate_name*	Sets a certificate whose corresponding private key is to be used to identify the ZyWALL / USG for SSH connections. The no command resets the certificate used by the SSH server to the factory default (`default`). *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 some ZyWALL / USG models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other ZyWALL / USG models, use pre-defined zone names like DMZ, LAN1, SSL VPN, IPSec VPN, OPT, and WAN.
ip ssh server rule move *rule_number* to *rule_number*	Changes the index number of a SSH service control rule.
[no] ip ssh server v1	Enables remote management using SSH v1. The no command stops the ZyWALL / USG from using SSH v1.
no ip ssh server rule *rule_number*	Deletes a service control rule for SSH service.
show ip ssh server status	Displays SSH settings.

56.4.4 SSH Command Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using SSH service.

```
Router# configure terminal
Router(config)# ip ssh server rule 2 access-group Marketing zone WAN action accept
```

This command sets a certificate (Default) to be used to identify the ZyWALL / USG.

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

56.5 Telnet

You can configure your ZyWALL / USG for remote Telnet access.

56.6 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 228 Command Summary: Telnet

COMMAND	DESCRIPTION
[no] ip telnet server	Allows Telnet access to the ZyWALL / USG CLI. The `no` command disables Telnet access to the ZyWALL / USG CLI.
[no] ip telnet server port <1..65535>	Sets the Telnet service port number. The `no` command resets the Telnet service port number back to the factory default (23).
ip telnet server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny}	Sets a service control rule for Telnet service. *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 some ZyWALL / USG models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other ZyWALL / USG models, use pre-defined zone names like DMZ, LAN1, SSL VPN, 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.

56.6.1 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)#
```

56.7 Configuring FTP

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

56.7.1 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 229 Command Summary: FTP

COMMAND	DESCRIPTION
[no] ip ftp server	Allows FTP access to the ZyWALL / USG. The no command disables FTP access to the ZyWALL / USG.
[no] ip ftp server cert *certificate_name*	Sets a certificate to be used to identify the ZyWALL / USG. The no command resets the certificate used by the FTP server to the factory default.
[no] ip ftp server port <1..65535>	Sets the FTP service port number. The no command resets the FTP service port number to the factory default (21).
[no] ip ftp server tls-required	Allows FTP access over TLS. The no command disables FTP access over TLS.
ip ftp server rule {*rule_number*|append|insert *rule_number*} access-group {ALL|*address_object*} zone {ALL|*zone_object*} action {accept|deny}	Sets a service control rule for FTP service. *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 some ZyWALL / USG models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other ZyWALL / USG models, use pre-defined zone names like DMZ, LAN1, SSL VPN, 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.

56.7.2 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
========================================================================
```

56.8 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your ZyWALL / USG supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL / USG through the network. The ZyWALL / USG supports SNMP version one (SNMPv1) version two (SNMPv2c) and version 3 (SNMPv3).

SNMP v3 enhances security for SNMP management using authentication and encryption. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

56.8.1 Supported MIBs

The ZyWALL / USG supports MIB II that is defined in RFC-1213 and RFC-1215. The ZyWALL / USG also supports private MIBs (zywall.mib and zyxel-zywall-ZLD-Common.mib) to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the ZyWALL / USG’s MIBs from www.zyxel.com.

56.8.2 SNMP Traps

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

Table 230 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the ZyWALL / USG is turned on or an agent restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
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.

Table 230 SNMP Traps (continued)

OBJECT LABEL	OBJECT ID	DESCRIPTION
vpnTunnelDisconnected	1.3.6.1.4.1.890.1.6.22.2.3	This trap is sent when an IPSec VPN tunnel is disconnected.
vpnTunnelName	1.3.6.1.4.1.890.1.6.22.2.2.1.1	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the disconnected tunnel's IPSec SA name.
vpnIKEName	1.3.6.1.4.1.890.1.6.22.2.2.1.2	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the disconnected tunnel's IKE SA name.
vpnTunnelSPI	1.3.6.1.4.1.890.1.6.22.2.2.1.3	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the security parameter index (SPI) of the disconnected VPN tunnel.

56.8.3 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 231 Command Summary: SNMP

COMMAND	DESCRIPTION
`[no] snmp-server`	Allows SNMP access to the ZyWALL / USG. The `no` command disables SNMP access to the ZyWALL / USG.
`[no] snmp-server community` *`community_string`* `{ro|rw}`	Enters up to 64 characters to set the password for read-only (ro) or read-write (rw) access. The `no` command resets the password for read-only (`ro`) or read-write (`rw`) access to the default.
`[no] snmp-server contact` *`description`*	Sets the contact information (of up to 60 characters) for the person in charge of the ZyWALL / USG. The `no` command removes the contact information for the person in charge of the ZyWALL / USG.
`[no] snmp-server enable {informs|traps}`	Enables all SNMP notifications (informs or traps). The `no` command disables all SNMP notifications (informs or traps).
`[no] snmp-server host {`*`w.x.y.z|fqdn|ipv6 address`*`} [`*`community_string`*`]`	Sets the IPv4 or IPv6 address of the host that receives the SNMP notifications. The `no` command removes the host that receives the SNMP notifications.
`[no] snmp-server location` *`description`*	Sets the geographic location (of up to 60 characters) for the ZyWALL / USG. The `no` command removes the geographic location for the ZyWALL / USG.
`[no] snmp-server port <1..65535>`	Sets the SNMP service port number. The `no` command resets the SNMP service port number to the factory default (`161`).
`snmp-server rule {`*`rule_number`*`|append|insert` *`rule_number`*`} access-group {ALL|`*`address_object`*`} zone {ALL|`*`zone_object`*`} action {accept|deny}`	Sets a service control rule for SNMP service. *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 some ZyWALL / USG models, use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other ZyWALL / USG models, use pre-defined zone names like DMZ, LAN1, SSL VPN, 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.

Table 231 Command Summary: SNMP (continued)

COMMAND	DESCRIPTION
`snmp-server v3user username` *`description`* `authentication {md5 | sha} privacy {none | des | aes} privilege {ro | rw}`	Sets the authentication, privacy and privilege for an SNMPv3 user.
`snmp-server version {v2c | v3}`	Sets the SNMP version for the ZyWALL / USG. The SNMP version on the ZyWALL / USG must match the version on the SNMP manager.
`show snmp status`	Displays SNMP Settings.
`show snmp-server v3user status`	Displays authentication, privacy and privilege for configured SNMPv3 users.

56.8.4 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
```

The following commands create an SNMPv3 rule and then displays the configured settings.

```
Router# configure terminal
Router(config)# snmp-server v3user username john authentication md5 privacy none
privilege rw
Router(config)# show snmp-server v3user status
SNMPv3 user profile: 1
  username: john
  authentication: md5
  privacy: none
  privilege: rw
Router(config)#
```

56.9 ICMP Filter

The `ip icmp-filter` commands are obsolete. See Chapter 27 on page 185 to configure secure policy rules for ICMP traffic going to the ZyWALL / USG to discard or reject ICMP packets destined for the ZyWALL / USG.

Configure the ICMP filter to help keep the ZyWALL / USG hidden from probing attempts. You can specify whether or not the ZyWALL / USG is to respond to probing for unused ports.

You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 232 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.

56.10 CloudCNM Screen

CloudCNM is a cloud-based network management system that allows management and monitoring of ZyWALL/USG/UAG security gateways with firmware that supports the TR-069 protocol.

CloudCNM features include:

- Batch import of managed devices at one time using one CSV file
- See an overview of all managed devices and system information in one place
- Monitor and manage devices
- Install firmware to multiple devices of the same model at one time
- Backup and restore device configuration
- View the location of managed devices on a map
- Receive notification for events and alarms, such as when a device goes down
- Graphically monitor individual devices and see related statistics
- Directly access a device for remote configuration
- Create four types of administrators with different privileges
- Perform Site-to-Site, Hub & Spoke, Fully-meshed and Remote Access VPN provisioning.

To allow CloudCNM management of your ZyWALL / USG:

- You must have a CloudCNM license with CNM ID number or a CloudCNM URL identifying the server.
- The ZyWALL / USG must be able to communicate with the CloudCNM server.

Table 233 Command Summary: CloudCNM

COMMAND	DESCRIPTION
`[no] cnm-agent activate`	Allows management of the ZyWALL / USG by CloudCNM. The no command disallows management of the ZyWALL / USG by CloudCNM.
`[no] cnm-agent auto-get-acs activate`	Automatically lets the ZyWALL / USG get the CloudCNM URL from MyZyXEL.com. CloudCNM server must be able to access MyZyXEL.com and you must have a CNM ID from the CloudCNM license. The no command disallows the ZyWALL / USG getting the CloudCNM URL from MyZyXEL.com, so you must manually configure it.
`cnm-agent cnm-id <ID>`	Enter the CNM ID exactly as on the CloudCNM license.
`[no] cnm-agent manager <https_url|http_url>`	Sets the URL (HTTP or HTTPs) for the CloudCNM server. The no command removes the URL (HTTP or HTTPs) for the CloudCNM server. Type the IPv4 IP address of the CloudCNM server followed by the TR-069 port number (default 7547) in CNM URL. For example, if you installed CloudCNM on a server with IP address 1.1.1.1, then enter http://1.1.1.1:7547 as the CNM URL. If the default TR-069 port on the CloudCNM server is changed, then replace 7547 with the new port number.
`[no] cnm-agent periodic-inform activate`	Has the ZyWALL / USG inform the CloudCNM server of its presence at regular intervals.
`cnm-agent periodic-inform interval <10…86400>`	Sets how often the ZyWALL / USG should inform CloudCNM server of its presence.
`show cnm-agent configuration`	Displays current CloudCNM configuration on the ZyWALL / USG.

57

File Manager

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

57.1 File Directories

The ZyWALL / USG stores files in the following directories.

Table 234 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.

57.2 Configuration Files and Shell Scripts Overview

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

When you apply a configuration file, the ZyWALL / USG uses the factory default settings for any features that the configuration file does not include. Shell scripts are files of commands that you can store on the ZyWALL / USG and run when you need them. When you run a shell script, the ZyWALL / USG only applies the commands that it contains. Other settings do not change.

You can edit configuration files or shell scripts in a text editor and upload them to the ZyWALL / USG. Configuration files use a .conf extension and shell scripts use a .zysh extension.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

Figure 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
secure-policy insert 4
from WAN
to ZyWALL
sourceip TW_TEAM
service TELNET
action allow
exit
write
```

While configuration files and shell scripts have the same syntax, the ZyWALL / USG applies configuration files differently than it runs shell scripts. This is explained below.

Table 235 Configuration Files and Shell Scripts in the ZyWALL / USG

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 390 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.)

57.2.1 Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use “#” or “!” as the first character of a command line to have the ZyWALL / USG treat the line as a comment.

Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the ZyWALL / USG exit sub command mode.

Note: “exit” or “!'” must follow sub commands if it is to make the ZyWALL / USG exit sub command mode.

Line 3 in the following example exits sub command mode.

```
interface ge1
ip address dhcp
!
```

Lines 1 and 3 in the following example are comments and line 4 exits sub command mode.

```
!
interface ge1
# this interface is a DHCP client
!
```

Lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2006/06/05
interface ge1
ip address dhcp
!
```

57.2.2 Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the ZyWALL / USG processes the file line-by-line. The ZyWALL / USG checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the ZyWALL / USG finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The ZyWALL / USG ignores any errors in the configuration file or shell script and applies all of the valid commands. The ZyWALL / USG still generates a log for any errors.

57.2.3 ZyWALL / USG Configuration File Details

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

- When you first receive the ZyWALL / USG, it uses the **system-default.conf** configuration file of default settings.
- When you change the configuration, the ZyWALL / USG creates a **startup-config.conf** file of the current configuration.
- The ZyWALL / USG checks the **startup-config.conf** file for errors when it restarts. If there is an error in the **startup-config.conf** file, the ZyWALL / USG copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file.

- When the ZyWALL / USG reboots, if the **startup-config.conf** file passes the error check, the ZyWALL / USG keeps a copy of the **startup-config.conf** file as the **lastgood.conf** configuration file for you as a back up file. If you upload and apply a configuration file with an error, you can apply **lastgood.conf** to return to a valid configuration.

57.2.4 Configuration File Flow at Restart

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

If there is a **startup-config.conf**, the ZyWALL / USG checks it for errors and applies it. If there are no errors, the ZyWALL / USG uses it and copies it to the **lastgood.conf** configuration file. If there is an error, the ZyWALL / USG generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the ZyWALL / USG applies the **system-default.conf** configuration file.

You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The ZyWALL / USG ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The ZyWALL / USG still generates a log for any errors.

57.3 File Manager Commands Input Values

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

Table 236 File Manager Command Input Values

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

57.4 File Manager Commands Summary

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

Table 237 File Manager Commands Summary

COMMAND	DESCRIPTION
`apply /conf/`*`file_name.conf`* `[ignore-error] [rollback]`	Has the ZyWALL / USG use a specific configuration file. You must still use the `write` command to save your configuration changes to the flash (“non-volatile” or “long term”) memory. 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 / USG 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 / USG with a fully valid configuration file. Use `rollback` without `ignore-error`: this gets the ZyWALL / USG 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 / USG to go back to its system defaults.
`copy {/conf | /idp | /packet_trace | /script | /tmp}`*`file_name-a.conf`* `{/conf | /idp | /packet_trace | /script | /tmp}/`*`file_name-b.conf`*	Saves a duplicate of a file on the ZyWALL / USG from the source file name to the target file name. Specify the directory and file name of the file that you want to copy and the directory and file name to use for the duplicate. Always copy the file into the same directory.
`copy running-config startup-config`	Saves your configuration changes to the flash (“non-volatile” or “long term”) memory. The ZyWALL / USG immediately uses configuration changes made via commands, but if you do not use this command or the write command, the changes will be lost when the ZyWALL / USG restarts.
`copy running-config /conf/`*`file_name.conf`*	Saves a duplicate of the configuration file that the ZyWALL / USG is currently using. You specify the file name to which to copy.
`delete {/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 {/conf | /idp | /packet_trace | /script | /tmp}`	Displays the list of files saved in the specified directory.
`rename {/conf | /idp | /packet_trace | /script | /tmp}/`*`old-file_name`* `{/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 / USG execute a specific shell script file. You must still use the `write` command to save your configuration changes to the flash (“non-volatile” or “long term”) memory.
`schedule-run 1` *`file_name.zysh`* `{daily | monthly | weekly} time {`*`date`* `| sun | mon | tue | wed | thu | fri | sat}`	Has the ZyWALL / USG execute the specified specific shell script file at the the specified time. You must still use the `write` command to save your configuration changes to the flash (“non-volatile” or “long term”) memory.

Table 237 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 / USG ignore any errors in the startup-config.conf file and apply all of the valid commands.
`show setenv-startup`	Displays whether or not the ZyWALL / USG is set to ignore any errors in the startup-config.conf file and apply all of the valid commands.
`write`	Saves your configuration changes to the flash ("non-volatile" or "long term") memory. The ZyWALL / USG immediately uses configuration changes made via commands, but if you do not use the `write` command, the changes will be lost when the ZyWALL / USG restarts.

57.5 File Manager Dual Firmware Commands

The following table lists the commands that you can use for managing dual firmware. Firmware uploaded using FTP goes to the Running partition. Use the web configurator to upload firmware to the Standby partition. The ZyWALL / USG reboots automatically when you upload firmware to the Running partition.

Table 238 File Manager Dual Firmware Commands

COMMAND	DESCRIPTION
`set firmware boot option <0..1>`	Sets the behavior of the ZyWALL / USG when firmware is uploaded to the Standby partition. (This command does not upload firmware.) Use 0 to have the ZyWALL / USG reboot immediately after firmware is uploaded to the Standby partition and become the Running firmware. Use 1 to not have the ZyWALL / USG reboot immediately after a firmware is uploaded to the Standby partition.
`show firmware image boot option`	Shows the behavior of the ZyWALL / USG when firmware is uploaded to the Standby partition.
`set firmware boot number <1..2>`	Reboots the ZyWALL / USG immediately with firmware in partition 1 or 2. If 2 is the Standby partition, then it becomes the Running partition after reboot. Use `show version` to see which partition is Standby and which is Running.

57.6 File Manager Command Examples

These are examples of the dual firmware commands .

```
Router(config)# set firmware boot option 0
Router(config)#
Router(config)# show firmware image boot option
boot option: 0
Router(config)#
Router(config)# set firmware boot number 2

Welcome to USG110

Username:
Terminate All Processes: OK
kill_process_and_umountfs() returns -7
Restarting system.

<snipped>

Welcome to USG110
Username: admin
Password:
Router> configure terminal
Router(config)# show version
ZyXEL Communications Corp.
image number model                     firmware version
build date           boot status
===============================================================================
1         USG110                     V4.11(AAPH.0)b3s1
2015-01-11 21:53:44  Standby
2         USG110                      V4.11(AAPH.0)
2015-03-13 03:47:52  Running
```

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)#
```

57.7 FTP File Transfer

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

57.7.1 Command Line FTP File Upload

1 Connect to the ZyWALL / USG.

2 Enter “bin” to set the transfer mode to binary.

3 You can upload the firmware after you log in through FTP. To upload other files, use “cd” to change to the corresponding directory.

4 Use “put” to transfer files from the computer to the ZyWALL / USG.[1] For example:

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

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

The firmware update can take up to five minutes. Do not turn off or reset the ZyWALL / USG while the firmware update is in progress! If you lose power during the firmware upload, you may need to refer to Section 57.10 on page 400 to recover the firmware.

57.7.2 Command Line FTP Configuration File Upload Example

The following example transfers a configuration file named tomorrow.conf from the computer and saves it on the ZyWALL / USG as next.conf.

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

Figure 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.
```

57.7.3 Command Line FTP File Download

1 Connect to the ZyWALL / USG.

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

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.

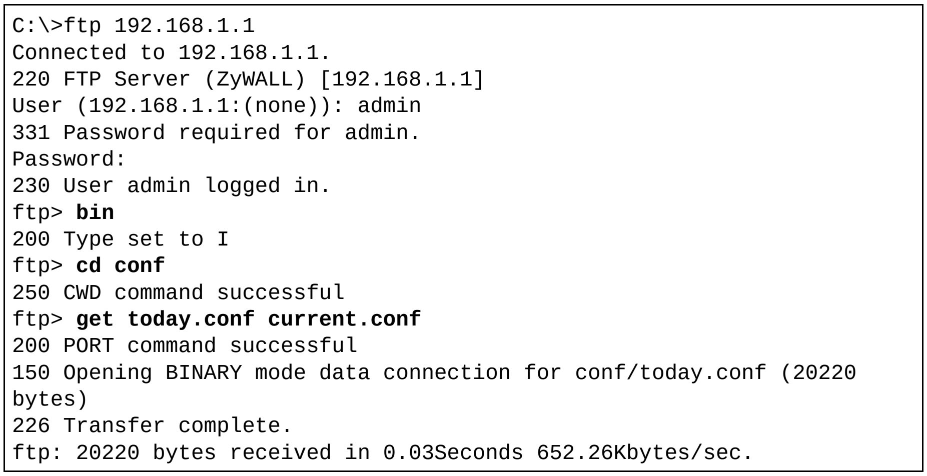
5. Use "get” to download files. For example:

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

57.7.4 Command Line FTP Configuration File Download Example

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

Figure 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.
```

57.8 Cloud Helper Commands

Cloud Helper lets you know if there is a later firmware available on the Cloud Helper server and lets you download it if you did. You must register your ZyWALL / USG at myZyXEL.com first.

Table 239 Cloud Helper Commands

COMMAND	DESCRIPTION
`cloud-helper check all`	Sends a query to the Cloud Helper Server to get the latest firmware, Geo IP, IDP signature and SSL CA certificate information.
`cloud-helper check firmware`	Sends a query to the Cloud Helper Server to get the latest firmware information.
`cloud-helper check geoip`	Sends a query to the Cloud Helper Server to get the latest Geo IP information.
`cloud-helper check idp`	Sends a query to the Cloud Helper Server to get the latest IDP signature information.
`cloud-helper check sslca`	Sends a query to the Cloud Helper Server to get the latest SSL CA certificate information.

Table 239 Cloud Helper Commands (continued)

COMMAND	DESCRIPTION
`cloud-helper get firmware <1..2>`	Downloads the latest firmware on the Cloud Helper server to the specified system space on the ZyWALL / USG.
`cloud-helper get idp`	Downloads the latest IDP signature on the Cloud Helper server to the ZyWALL / USG.
`cloud-helper get sslca`	Downloads the latest SSL certificate on the Cloud Helper server to the ZyWALL / USG.
`cloud-helper set {[retry_times <1..10>]} {[retry_period <2..60>]} {[retry_fail_period <180..720>]}`	Specifies criteria for how the ZyWALL / USG should download firmware, IDP signatures or SSL certificates from the Cloud Helper server. `retry_times`: Up to 10 attempts are allowed to download items. `retry_period`: The retry interval must be between 2 and 60 seconds. `retry_fail_period`: The retry interval after retry attempts have expired must be between 180 and 720 seconds.
`cloud-helper clean-download firmware`	Stops and removes a firmware being downloaded to the ZyWALL / USG.
`cloud-helper pause-download firmware <1..2>`	Temporarily stops a firmware being downloaded to the specified system space on the ZyWALL / USG.
`cloud-helper update firmware <1..2>`	Resumes a firmware being downloaded to the specified system space on the ZyWALL / USG.
`show cloud-helper firmware`	Displays latest firmware information received from the Cloud Helper server.

57.8.1 File Manager Command Examples

These are examples of Cloud Helper commands.

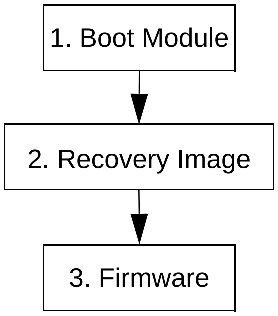
```
Router(config)#
Router(config)# cloud-helper check firmware
===============================================================================
Cloud status      : NORMAL
firmware version  : 4.20(AAPL.0)b5
firmware release  : 2016-07-15T02:29:11Z
firmware md5      : 752ed3f2d8296e669ea2146c29523bda
firmware news file: YES
firmware note file: YES
firmware message file: NO
boot status      : Running
===============================================================================
Cloud status      : NORMAL
firmware version  : 4.20(AAPL.0)b5
firmware release  : 2016-07-15T02:29:11Z
firmware md5      : 752ed3f2d8296e669ea2146c29523bda
firmware news file: YES
firmware note file: YES
firmware message file: NO
boot status      : Standby
Router(config)#
```

```
Router# show cloud-helper firmware
===============================================================================
Cloud status      : NORMAL
firmware version  : 4.20(AAPL.0)b5
firmware release  : 2016-07-15T02:29:11Z
firmware md5      : 752ed3f2d8296e669ea2146c29523bda
firmware news file: YES
firmware note file: YES
firmware message file: NO
boot status      : Running
===============================================================================
Cloud status      : NORMAL
firmware version  : 4.20(AAPL.0)b5
firmware release  : 2016-07-15T02:29:11Z
firmware md5      : 752ed3f2d8296e669ea2146c29523bda
firmware news file: YES
firmware note file: YES
firmware message file: NO
boot status      : Standby
Router#
Router#
```

57.9 ZyWALL / USG File Usage at Startup

The ZyWALL / USG uses the following files at system startup.

Figure 30 ZyWALL / USG File Usage at Startup



1 The boot module performs a basic hardware test. You cannot restore the boot module if it is damaged. The boot module also checks and loads the recovery image. The ZyWALL / USG notifies you if the recovery image is damaged.

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

57.10 Notification of a Damaged Recovery Image or Firmware

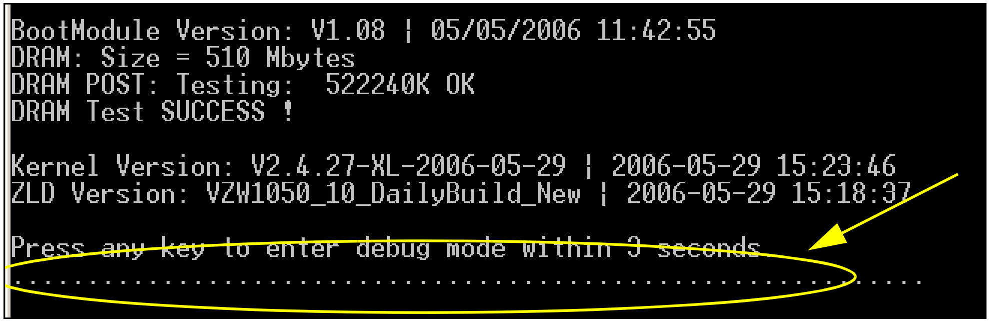
The ZyWALL / USG's recovery image and/or firmware could be damaged, for example by the power going off during a firmware upgrade. This section describes how the ZyWALL / USG notifies you of a damaged recovery image or firmware file. Use this section if your device has stopped responding for an extended period of time and you cannot access or ping it. Note that the ZyWALL / USG does not respond while starting up. It takes less than five minutes to start up with the default configuration, but the start up time increases with the complexity of your configuration.

1 Use a console cable and connect to the ZyWALL / USG via a terminal emulation program (such as HyperTerminal). Your console session displays the ZyWALL / USG's startup messages. If you cannot see any messages, check the terminal emulation program's settings (see Section 1.2.1 on page 24) and restart the ZyWALL / USG.

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

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

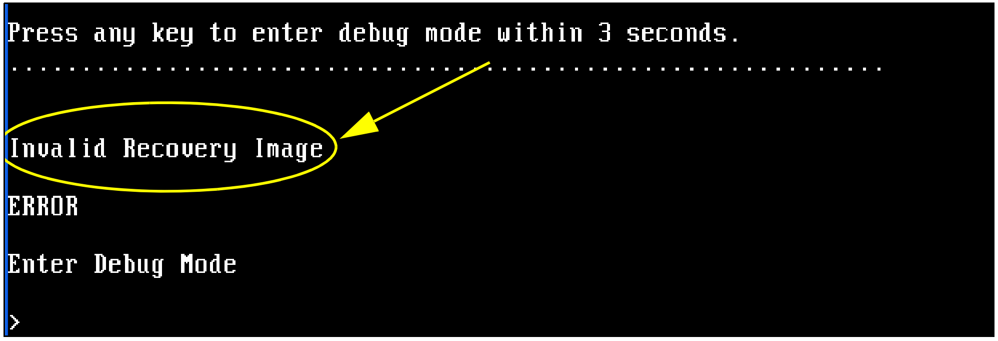
Figure 31 System Startup Stopped



```
BootModule Version: V1.08 | 05/05/2006 11:42:55
DRAM: Size = 510 Mbytes
DRAM POST: Testing:  522240K OK
DRAM Test SUCCESS !

Kernel Version: V2.4.27-XL-2006-05-29 | 2006-05-29 15:23:46
ZLD Version: VZW1050_10_DailyBuild_New | 2006-05-29 15:18:37

Press any key to enter debug mode within 3 seconds
..............................................................
```

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 57.11 on page 401 to restore the recovery image.

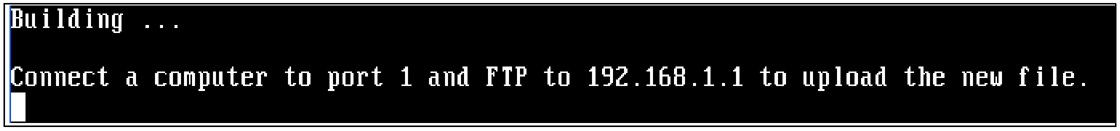
Figure 32 Recovery Image Damaged



```
Press any key to enter debug mode within 3 seconds.
............................................................

Invalid Recovery Image

ERROR

Enter Debug Mode

>
```

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 57.12 on page 403 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.
```

57.11 Restoring the Recovery Image

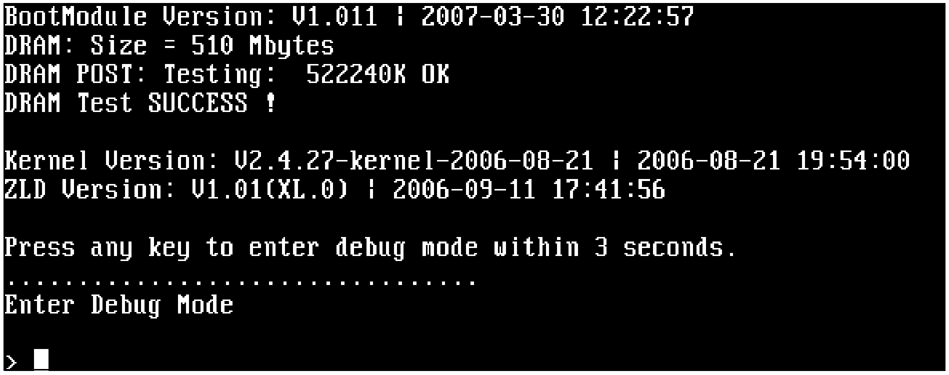
This procedure requires the ZyWALL / USG's recovery image. Download the firmware package from www.zyxel.com and unzip it. The recovery image uses a .ri extension, for example, "1.01(XL.0)C0.ri". Do the following after you have obtained the recovery image file.

Note: You only need to use this section if you need to restore the recovery image.

1 Restart the ZyWALL / USG.

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

Figure 34 Enter Debug Mode

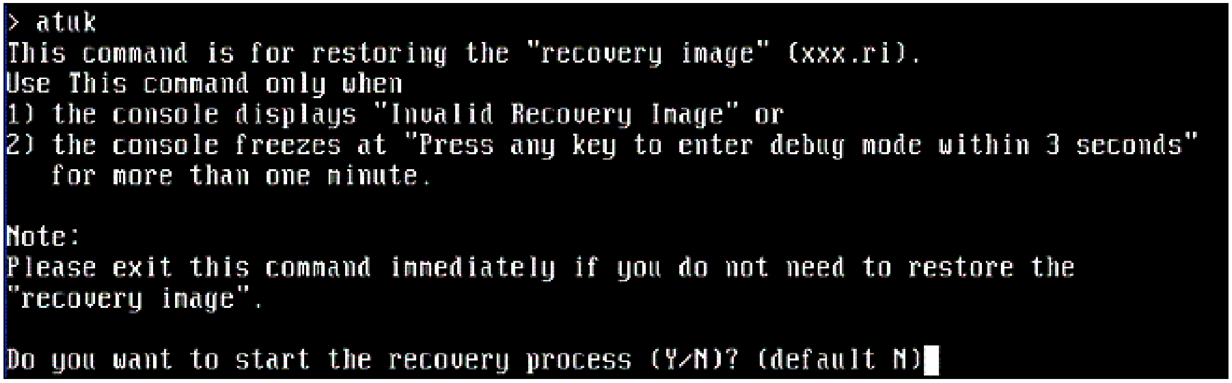


```
BootModule Version: V1.011 | 2007-03-30 12:22:57
DRAM: Size = 510 Mbytes
DRAM POST: Testing:  522240K OK
DRAM Test SUCCESS !

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.

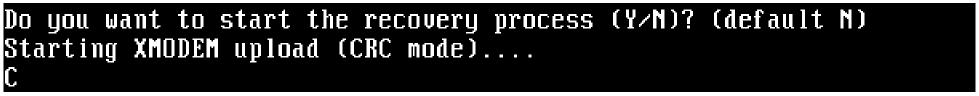
Figure 35 atuk Command for Restoring the Recovery Image



```
> 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.

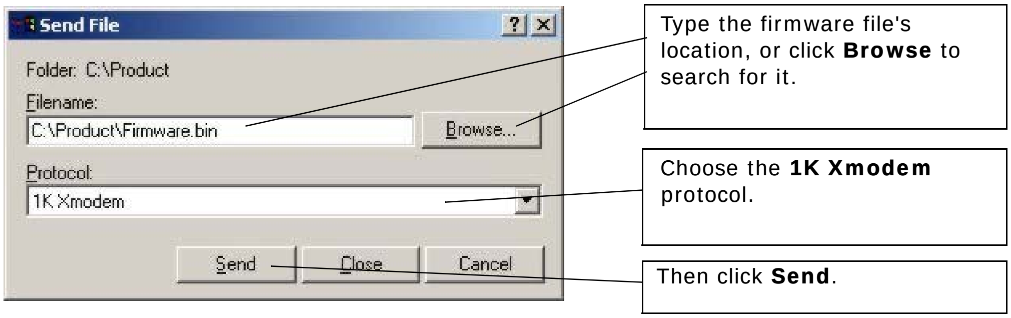
Figure 36 Starting Xmodem Upload



```
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



Folder: C:\Product

Filename: C:\Product\Firmware.bin

Protocol: 1K Xmodem

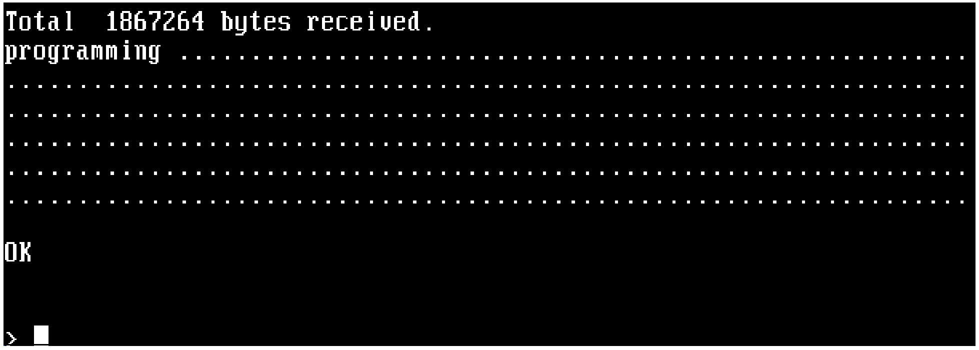
Type the firmware file's location, or click **Browse** to search for it.

Choose the **1K Xmodem** protocol.

Then click **Send**.

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

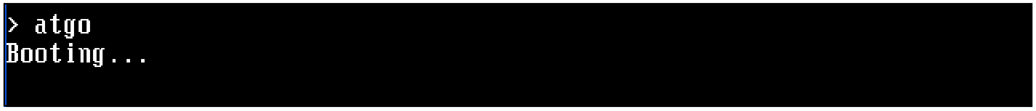
Figure 38 Recovery Image Upload Complete



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

OK


>
```

7 Enter atgo. The ZyWALL / USG starts up. If “Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file” displays on the screen, the firmware file is damaged and you need to use the procedure in Section 57.12 on page 403 to recover the firmware.

Figure 39 atgo Debug Command



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

57.12 Restoring the Firmware

This procedure requires the ZyWALL / USG’s firmware. Download the firmware package from www.zyxel.com and unzip it. The firmware file uses a .bin extension, for example, "1.01(XL.0)C0.bin". Do the following after you have obtained the firmware file.

Note: This section is not for normal firmware uploads. You only need to use this section if you need to recover the firmware.

1 Connect your computer to the ZyWALL / USG’s port **1** (only port **1** can be used).

2 The ZyWALL / USG’s FTP server IP address for firmware recovery is 192.168.1.1, so set your computer to use a static IP address from 192.168.1.2 ~192.168.1.254.

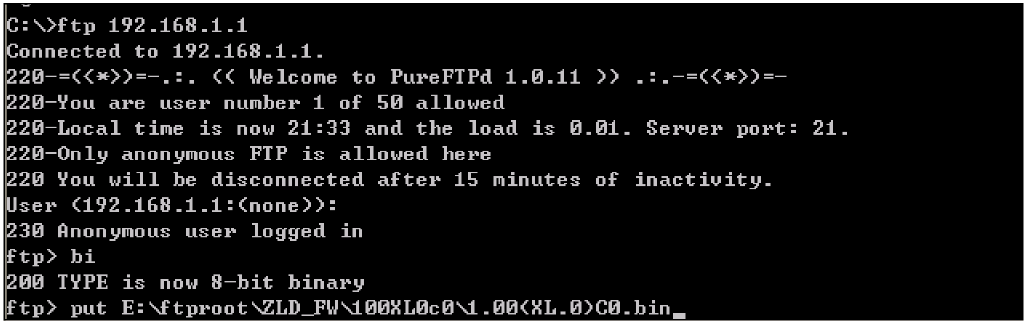
3 Use an FTP client on your computer to connect to the ZyWALL / USG. For example, in the Windows command prompt, type ftp 192.168.1.1. Keep the console session connected in order to see when the firmware recovery finishes.

4 Hit enter to log in anonymously.

5 Set the transfer mode to binary (type bin).

6 Transfer the firmware file from your computer to the ZyWALL / USG. Type put followed by the path and name of the firmware file. This examples uses put e:\ftproot\ZLD FW \1.01(XL.0)C0.bin.

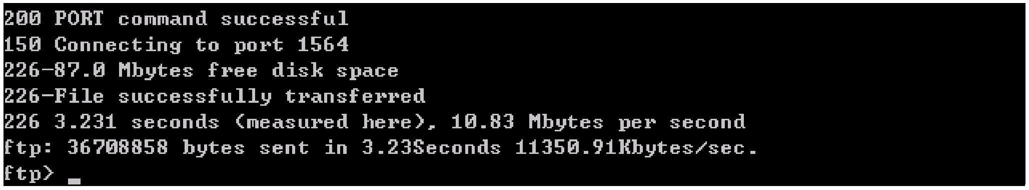
Figure 40 FTP Firmware Transfer Command



```
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.

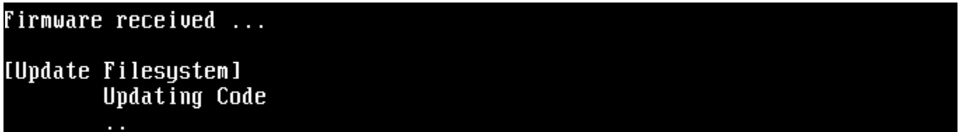
Figure 41 FTP Firmware Transfer Complete



```
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 / USG recovers the firmware.

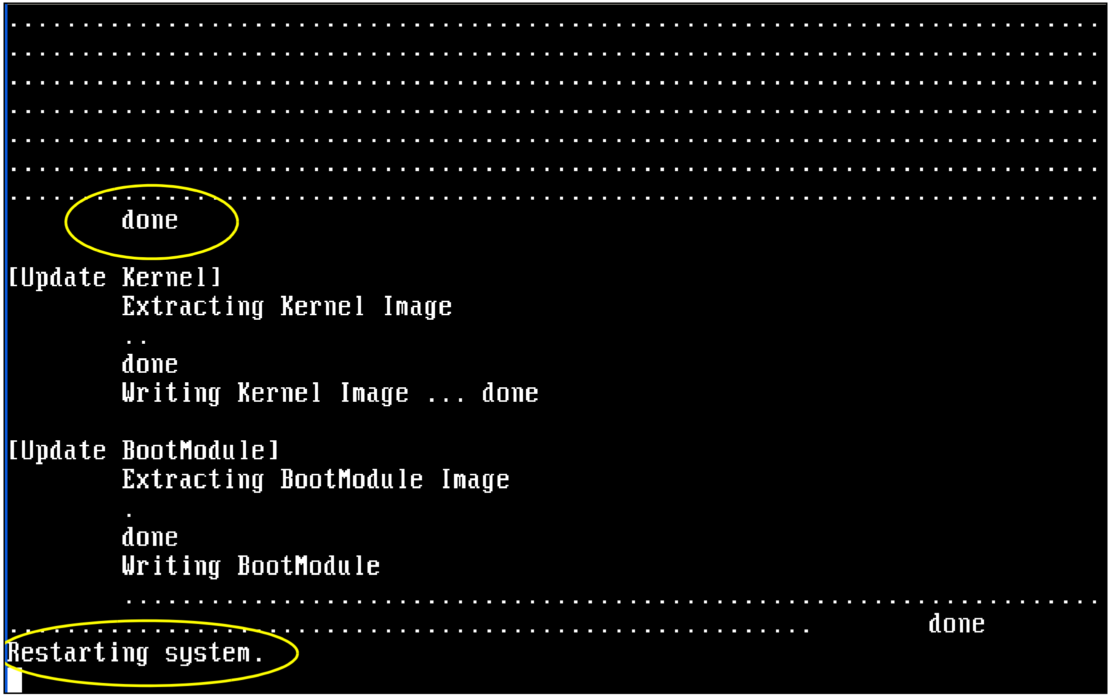
Figure 42 Firmware Received and Recovery Started



```
Firmware received ...

[Update Filesystem]
        Updating Code
        ..
```

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

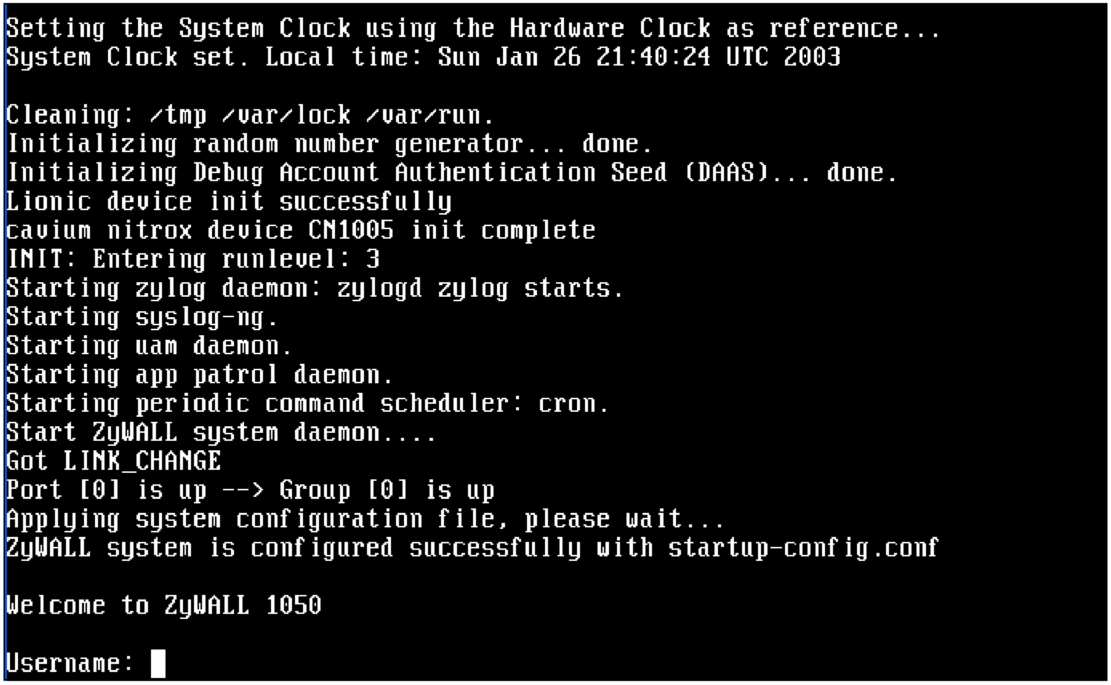
Figure 43 Firmware Recovery Complete and Restart



```
...........................................................................
...........................................................................
...........................................................................
...........................................................................
...........................................................................
...........................................................................
...........................................................................
         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 / USG starts up successfully. The firmware recovery process is now complete and the ZyWALL / USG is ready to use.

Figure 44 Restart Complete



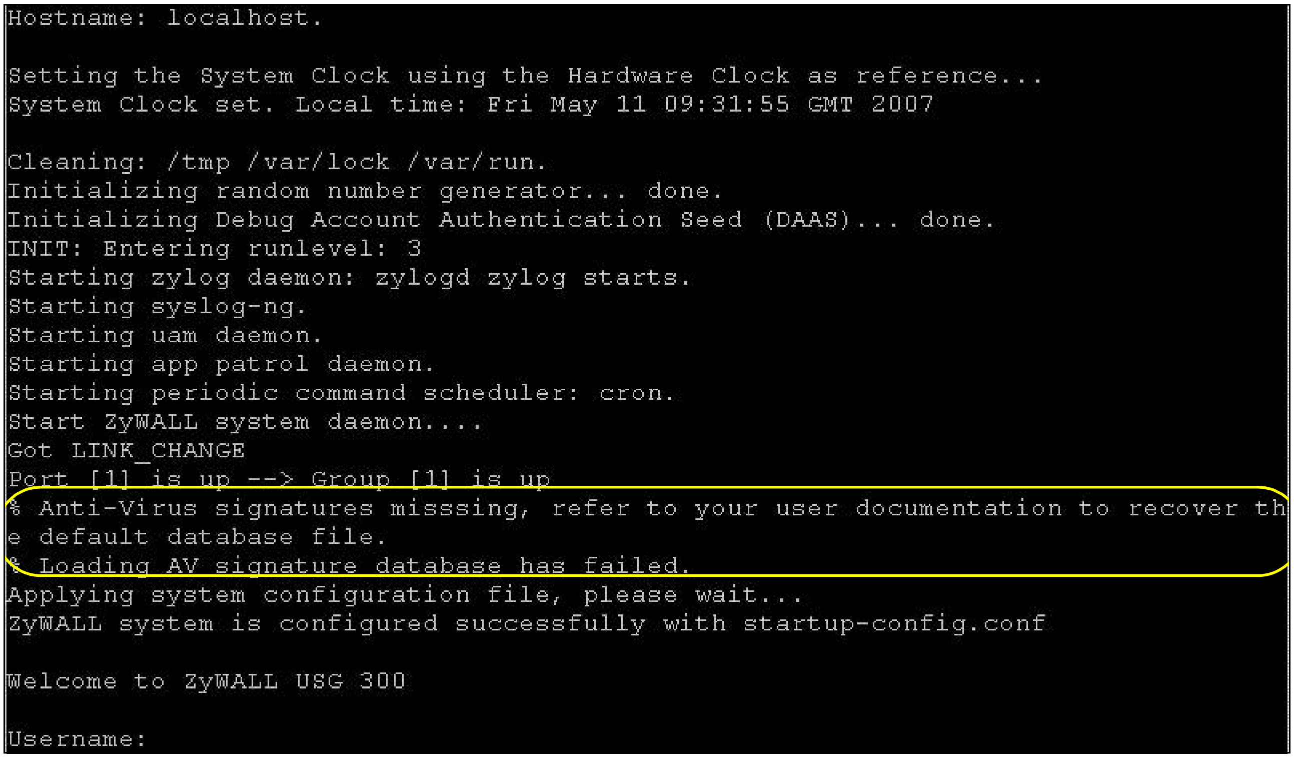
```
Setting the System Clock using the Hardware Clock as reference...
System Clock set. Local time: Sun Jan 26 21:40:24 UTC 2003

Cleaning: /tmp /var/lock /var/run.
Initializing random number generator... done.
Initializing Debug Account Authentication Seed (DAAS)... done.
Lionic device init successfully
cavium nitrox device CN1005 init complete
INIT: Entering runlevel: 3
Starting zylog daemon: zylogd zylog starts.
Starting syslog-ng.
Starting uam daemon.
Starting app patrol daemon.
Starting periodic command scheduler: cron.
Start ZyWALL system daemon....
Got LINK_CHANGE
Port [0] is up --> Group [0] is up
Applying system configuration file, please wait...
ZyWALL system is configured successfully with startup-config.conf

Welcome to ZyWALL 1050

Username: █
```

57.13 Restoring the Default System Database

The default system database stores information such as the default anti-virus or IDP signatures. The ZyWALL / USG can still operate if the default system database is damaged or missing, but related features (like anti-virus or IDP) may not function properly.

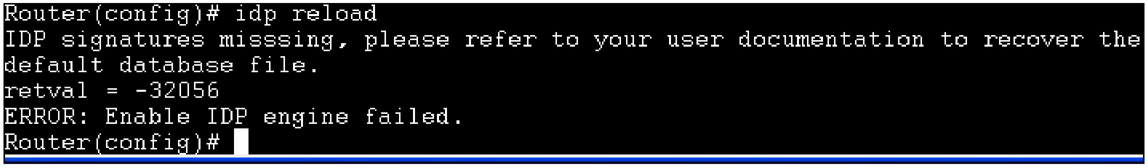
If the default system database file is not valid, the ZyWALL / USG displays a warning message in your console session at startup or when reloading the anti-virus or IDP signatures. It also generates a log. Here are some examples. Use this section to restore the ZyWALL / USG's default system database.

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



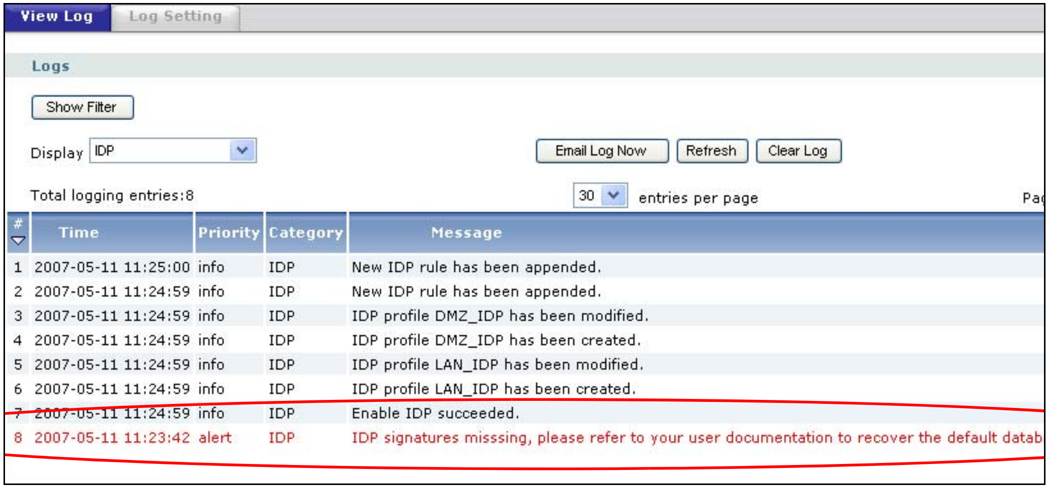
```
Hostname: localhost.

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 missing, 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



Display IDP

Total logging entries:8

30 entries per page

#	Time	Priority	Category	Message
1	2007-05-11 11:25:00	info	IDP	New IDP rule has been appended.
2	2007-05-11 11:24:59	info	IDP	New IDP rule has been appended.
3	2007-05-11 11:24:59	info	IDP	IDP profile DMZ_IDP has been modified.
4	2007-05-11 11:24:59	info	IDP	IDP profile DMZ_IDP has been created.
5	2007-05-11 11:24:59	info	IDP	IDP profile LAN_IDP has been modified.
6	2007-05-11 11:24:59	info	IDP	IDP profile LAN_IDP has been created.
7	2007-05-11 11:24:59	info	IDP	Enable IDP succeeded.
8	2007-05-11 11:23:42	alert	IDP	IDP signatures misssing, please refer to your user documentation to recover the default datab

This procedure requires the ZyWALL / USG's default system database file. Download the firmware package from www.zyxel.com and unzip it. The default system database file uses a .db extension, for example, "1.01(XL.0)C0.db". Do the following after you have obtained the default system database file.

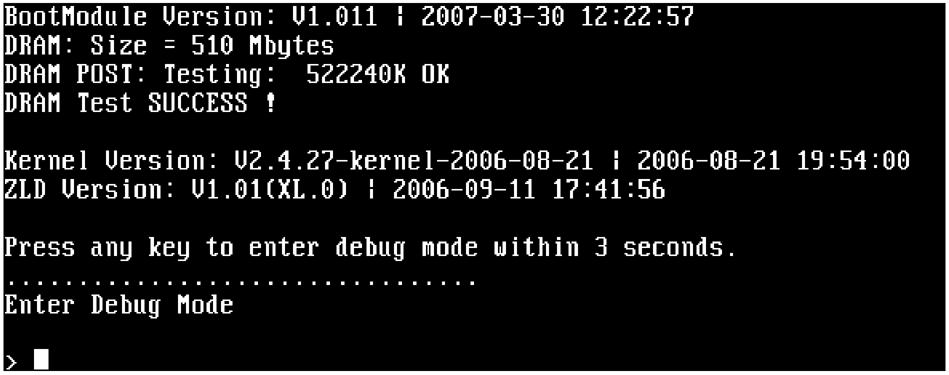
57.13.1 Using the atkz -u Debug Command

Note: You only need to use the `atkz -u` command if the default system database is damaged.

1 Restart the ZyWALL / USG.

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

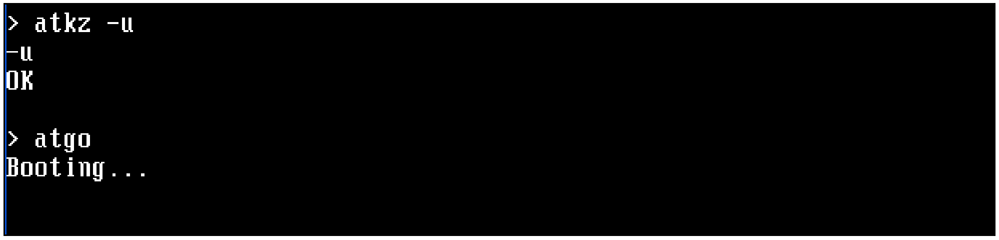
Figure 48 Enter Debug Mode



```
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.

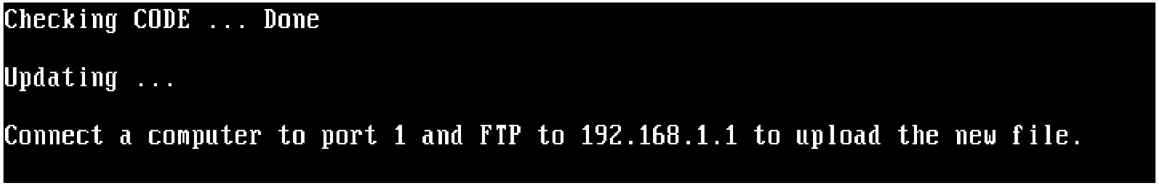
Figure 49 atkz -u Command for Restoring the Default System Database



```
> 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 / USG’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 / USG’s FTP server IP address for firmware recovery is 192.168.1.1, so set your computer to use a static IP address from 192.168.1.2 ~192.168.1.254.

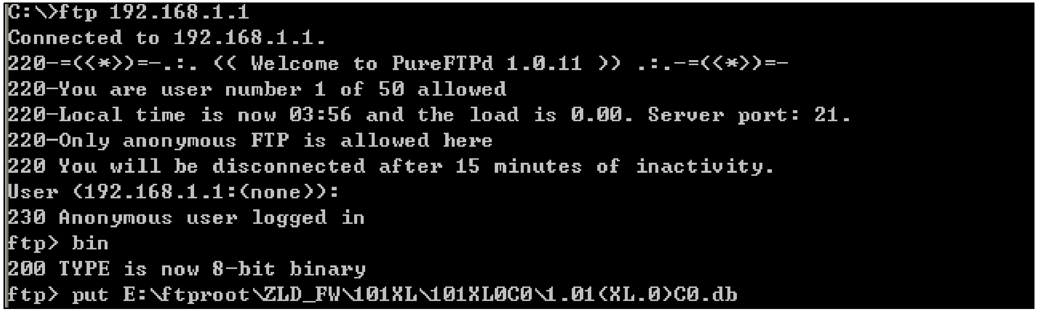
6 Use an FTP client on your computer to connect to the ZyWALL / USG. For example, in the Windows command prompt, type `ftp 192.168.1.1`. Keep the console session connected in order to see when the default system database recovery finishes.

7 Hit enter to log in anonymously.

8 Set the transfer mode to binary (type `bin`).

9 Transfer the firmware file from your computer to the ZyWALL / USG. Type `put` followed by the path and name of the firmware file. This examples uses `put e:\ftproot\ZLD FW \1.01(XL.0)C0.db`.

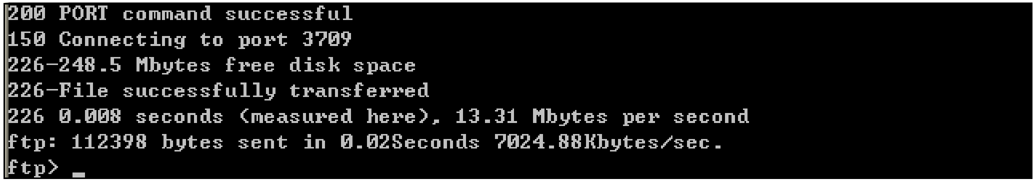
Figure 51 FTP Default System Database Transfer Command



```
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.

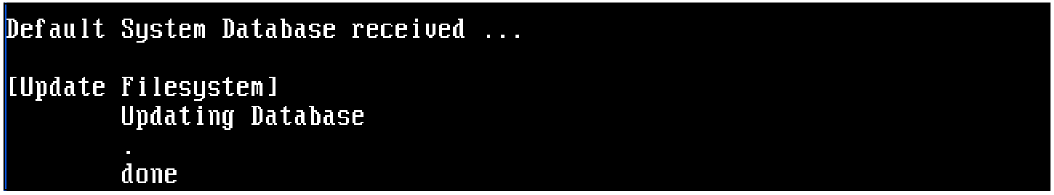
Figure 52 FTP Default System Database Transfer Complete



```
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.

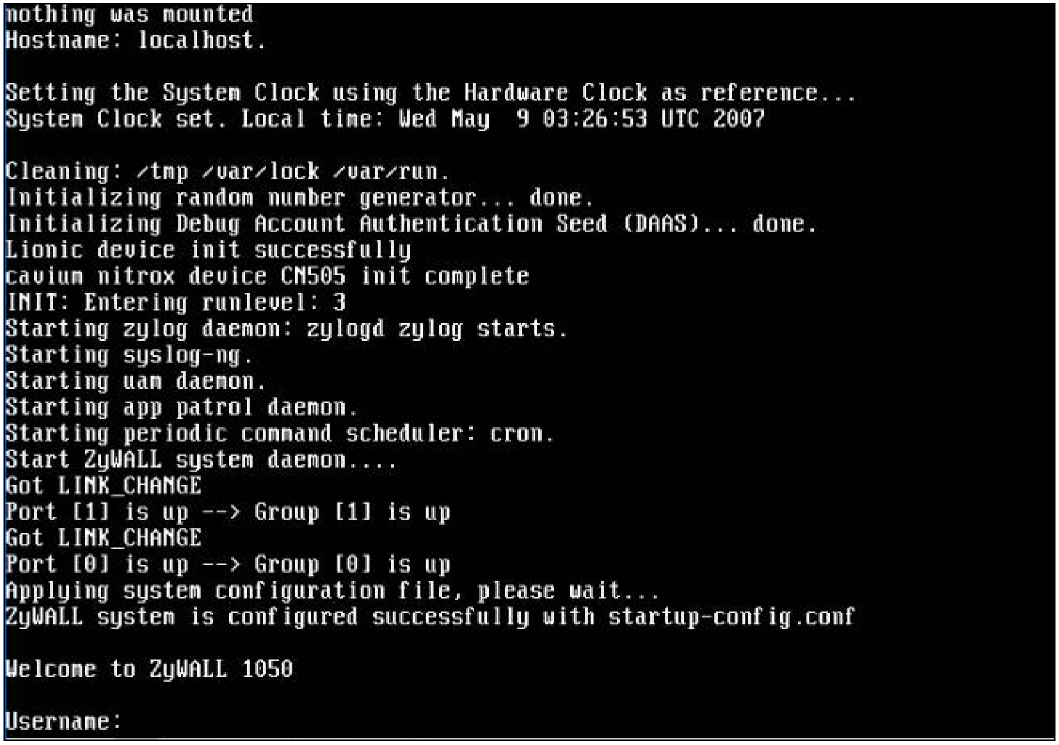
Figure 53 Default System Database Received and Recovery Complete



```
Default System Database received ...

[Update Filesystem]
        Updating Database
        .
        done
```

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

Figure 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:
```

Logs

This chapter provides information about the ZyWALL / USG's logs.

Note: When the system log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

See the User's Guide for the maximum number of system log messages in the ZyWALL / USG.

58.1 Log Commands Summary

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

Table 240 Input Values for Log Commands

LABEL	DESCRIPTION
interface_name	The name of the interface. Ethernet interface: For some ZyWALL / USG models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your ZyWALL / USG model. For othere ZyWALL / USG models, use a name such as wan1, wan2, opt, lan1, 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 / USG 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 / USG model supports.
module_name	The name of the category; kernel, syslog, ... The default category includes debugging messages generated by open source software. The all category includes all messages in all categories.
protocol	The name of a protocol such as TCP, UDP, ICMP.

The following sections list the logging commands.

58.1.1 Log Entries Commands

This table lists the commands to look at log entries.

Table 241 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

58.1.2 System Log Commands

This table lists the commands for the system log settings.

Table 242 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] logging cef-format include year	Includes the year in the cef (Common Event Format) syslog-compatible format.
[no] connectivity-check continuous-log activate	Has the ZyWALL / USG generate a log for each connectivity check. The no command has the ZyWALL / USG only log the first connectivity check.
show connectivity-check continuous-log status	Displays whether or not the ZyWALL / USG generates a log for each connectivity check.
clear logging system-log buffer	Clears the system log.

58.1.2.1 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    ,
```

58.1.3 Debug Log Commands

This table lists the commands for the debug log settings.

Table 243 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. For the purposes of this device's CLI, Access Points are referred to as WTPs.

Table 244 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 245 logging Commands: VRPT Settings

COMMAND	DESCRIPTION
vrpt send device information interval <15..3600>	Sets the interval (in seconds) for how often the ZyWALL / USG sends a device information log to the VRPT server.
vrpt send interface statistics interval <15..3600>	Sets the interval (in seconds) for how often the ZyWALL / USG sends an interface statistics log to the VRPT server.
vrpt send system status interval <15..3600>	Sets the interval (in seconds) for how often the ZyWALL / USG sends a system status log to the VRPT server.
show vrpt send device information interval	Displays the interval (in seconds) for how often the ZyWALL / USG sends a device information log to the VRPT server.
show vrpt send interface statistics interval	Displays the interval (in seconds) for how often the ZyWALL / USG sends an interface statistics log to the VRPT server.
show vrpt send system status interval	Displays the interval (in seconds) for how often the ZyWALL / USG sends a system status log to the VRPT server.
MODULE_NAME_WTP	{user| zysh| built-in-service| system| system-monitoring| routing-protocol| pki| interface| interface-statistics| account| force-auth| traffic-log| file-manage| wlan| daily-report| dhcp| default| capwap| wlan-station-info| all}
FACILITY	{local_1|local_2|local_3|local_4|local_5|local_6|local_7}
HOSTNAME	"(([a-z0-9\-])+\.)+([a-z]{2}\.[a-z]{2}|[a-z]{2,4})"
USER_NAME_	"([0-9]|[a-z]|[A-Z]|[-_]|\.|\@|[0-9]|[a-z]|[A-Z]|[-_])+"
ZYLOG_SUBJECT	"[a-zA-Z0-9 '()+,./:=?;!*#@$_%-]{1,61}""<subject>";

Table 245 logging Commands: VRPT Settings (continued)

COMMAND	DESCRIPTION
`MODULE_NAME_WTP_`	{user| zysh| built-in-service| system| routing-protocol| pki| interface| account| force-auth| file-manage| wlan| daily-report| dhcp| default| capwap| wlan-station-info| all}
`WEEKDAYS`	{sun|mon|tue|wed|thu|fri|sat}

58.1.4 E-mail Profile Commands

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

Table 246 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.
`[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> tls activate`	Select Transport Layer Security (TLS) if you want encrypted communications between the mail server and the ZyWALL / USG.
`[no ]logging mail <1..2> tls authenticate-server`	If you choose TLS Security, you may also select this to have the ZyWALL / USG authenticate the mail server in the TLS handshake.
`[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 / USG 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.

Table 246 logging Commands: E-mail Profile Settings (continued)

COMMAND	DESCRIPTION
[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
[no] logging mail <1..2> tls starttls-off	Turns off STARTTLS and uses the TLS protocol for SMTP mail encryption over TLS logging. The no command enables the default STARTTLS protocol.

58.1.4.1 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
```

58.1.5 Console Port Logging Commands

This table lists the commands for the console port settings.

Table 247 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.

Reports and Reboot

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

59.1 Report Commands Summary

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

59.1.1 Report Commands

This table lists the commands for reports.

Table 248 report Commands

COMMAND	DESCRIPTION
`[no] report`	Begins data collection. The `no` command stops data collection.
`show report status`	Displays whether or not the ZyWALL / USG is collecting data and how long it has collected data.
`clear report [`*`interface_name`*`]`	Clears the report for the specified interface or for all interfaces.
`show report [`*`interface_name`*` {ip | service | url}]`	Displays the traffic report for the specified interface and controls the format of the report. Formats are: `ip` - traffic by IP address and direction `service` - traffic by service and direction `url` - hits by URL

59.1.2 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
```

59.1.3 Session Commands

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

Table 249 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.

59.1.4 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 250 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 250 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.

59.2 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 251 Input Values for Email Daily Report Commands

LABEL	DESCRIPTION
e_mail	An e-mail address. You can use up to 80 alphanumeric characters, underscores (_), periods (.), or dashes (-), and you must use the @ character.

Use these commands to have the ZyWALL / USG e-mail you system statistics every day. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 252 Email Daily Report Commands

COMMAND	DESCRIPTION
`show daily-report status`	Displays the e-mail daily report settings.
`daily-report`	Enters the sub-command mode for configuring daily e-mail reports settings.
`[no] activate`	Turns daily e-mail reports on or off.
`draw-usage-graphics`	Has the report e-mail include usage graphs.
`smtp-address {ip | hostname}`	Sets the SMTP mail server IP address or domain name.
`[no] smtp-auth activate`	Enables or disables SMTP authentication.
`smtp-auth username username password password`	Sets the username and password for SMTP authentication.
`no smtp-address`	Resets the SMTP mail server configuration.
`no smtp-auth username`	Resets the authentication configuration.
`[no] smtp-port <1..65535>`	Sets the SMTP authentication port. The no command deletes the setting.
`mail-subject set subject`	Configures the subject of the report e-mails. Spaces are allowed.
`no mail-subject set`	Clears the configured subject for the report e-mails.
`[no] mail-subject append system-name`	Determines whether the system name will be appended to the subject of the report e-mails.
`[no] mail-subject append date-time`	Determines whether the sending date-time will be appended at subject of the report e-mails.
`[no] mail-from e_mail`	Sets the sender e-mail address of the report e-mails.
`[no] mail-to-1 e_mail`	Sets to whom the ZyWALL / USG sends the report e-mails (up to five recipients).
`[no] mail-to-2 e_mail`	See above.

Table 252 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.
`[no] smtp-tls starttls-off`	Turns off STARTTLS and uses the TLS protocol for SMTP mail encryption over TLS for the daily report. The no command enables the default STARTTLS protocol.
`exit`	Leaves the sub-command mode.

59.2.1 Email Daily Report Example

This example sets the following about sending a daily report e-mail:

- Disables the reporting.
- Specifies example-SMTP-mail-server.com as the address of the SMTP mail server.
- Sets the subject of the report e-mails to test.
- Stops the system name from being appended to the mail subject.
- Appends the date and time to the mail subject.
- Sets the sender as my-email@example.com.
- Sets example-administrator@example.com as the first account to which to send the mail.
- Has the ZyWALL / USG not use the second and third mail-to options.
- Sets my-email@example.com as the fourth mail-to option.

- Has the ZyWALL / USG not use the fifth mail-to option.
- Has the ZyWALL / USG provide username 12345 and password 12345 to the SMTP server for authentication.
- Sets the ZyWALL / USG to send the report at 1:57 PM.
- Has the ZyWALL / USG not reset the counters after sending the report.
- Has the report include CPU, memory, port, and session usage along with traffic statistics.
- Turns on the daily e-mail reporting.

```
Router(config)# daily-report
Router(config-daily-report)# no activate
Router(config-daily-report)# smtp-address example-SMTP-mail-server.com
Router(config-daily-report)# mail-subject set test
Router(config-daily-report)# no mail-subject append system-name
Router(config-daily-report)# mail-subject append date-time
Router(config-daily-report)# mail-from my-email@example.com
Router(config-daily-report)# mail-to-1 example-administrator@example.com
Router(config-daily-report)# no mail-to-2
Router(config-daily-report)# no mail-to-3
Router(config-daily-report)# mail-to-4 my-email@example.com
Router(config-daily-report)# no mail-to-5
Router(config-daily-report)# smtp-auth activate
Router(config-daily-report)# smtp-auth username 12345 password pass12345
Router(config-daily-report)# schedule hour 13 minutes 57
Router(config-daily-report)# no reset-counter
Router(config-daily-report)# item cpu-usage
Router(config-daily-report)# item mem-usage
Router(config-daily-report)# item port-usage
Router(config-daily-report)# item session-usage
Router(config-daily-report)# item traffic-report
Router(config-daily-report)# activate
Router(config-daily-report)# exit
Router(config)#
```

This displays the email daily report settings and has the ZyWALL / USG send the report.

```
Router(config)# show daily-report status
email daily report status
=========================
activate: yes
scheduled time: 13:57
reset counter: no
smtp address: example-SMTP-mail-server.com
smtp port: 25
smtp auth: yes
smtp username: 12345
smtp password: pass12345
mail subject:  test subject
append system name: no
append date time: yes
mail from: my-email@example.com
mail-to-1: example-administrator@example.com
mail-to-2:
mail-to-3:
mail-to-4: my-email@example.com
mail-to-5:
cpu-usage: yes
mem-usage: yes
session-usage: yes
port-usage: yes
traffic-report: yes

Router(config)# daily-report send-now
```

59.3 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.

60

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 253 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
```

61

Diagnostics

This chapter covers how to use the diagnostics feature.

61.1 Diagnostics

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

61.2 Diagnosis Commands

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

Table 254 diagnosis Commands

COMMAND	DESCRIPTION
`diag-info collect`	Has the ZyWALL / USG create a new diagnostic file.
`show diag-info`	Displays the name, size, and creation date (in yyyy-mm-dd hh:mm:ss format) of the diagnostic file.

61.3 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      : 2014-04-23 09:55:09
```

62

Packet Flow Explore

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

62.1 Packet Flow Explore

Use this to get a clear picture on how the ZyWALL / USG determines where to forward a packet and how to change the source IP address of the packet according to your current settings. This function provides you a summary of all your routing and SNAT settings and helps troubleshoot the related problems.

62.2 Packet Flow Explore Commands

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

Table 255 Packet Flow Explore Commands

COMMAND	DESCRIPTION
`show route order`	Displays the order of routing related functions the ZyWALL / USG checks for packets. Once a packet matches the criteria of a routing rule, the ZyWALL / USG takes the corresponding action and does not perform any further flow checking.
`show system snat order`	Displays the order of SNAT related functions the ZyWALL / USG checks for packets. Once a packet matches the criteria of an SNAT rule, the ZyWALL / USG uses the corresponding source IP address and does not perform any further flow checking.
`show system route policy-route`	Displays activated policy routes.
`show system route nat-1-1`	Displays activated 1-to-1 NAT rules.
`show system route site-to-site-vpn`	Displays activated site-to-site VPN rules.
`show system route dynamic-vpn`	Displays activated dynamic VPN rules.
`show system route default-wan-trunk`	Displays the default WAN trunk settings.
`show ip route static-dynamic`	Displays activated static-dynamic routes.
`show system snat policy-route`	Displays activated policy routes which use SNAT.
`show system snat nat-1-1`	Displays activated NAT rules which use SNAT.
`show system snat nat-loopback`	Displays activated activated NAT rules which use SNAT with NAT loopback enabled.
`show system snat default-snat`	Displays the default WAN trunk settings.

62.3 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>
```

63

Maintenance Tools

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

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

Table 256 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 / USG dumps the traffic to /packet_trace/packet_trace_interface. Use FTP to retrieve the files (see Section 57.7 on page 395). If you do not assign the duration, the ZyWALL / USG 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 / USG. Note: Use the packet-capture configure command to configure the packet-capture settings before using this command.
packet-capture configure	Enters the sub-command mode.
duration <0..300>	Sets a time limit in seconds for the capture. The ZyWALL / USG stops the capture and generates the capture file when either this period of time has passed or the file reaches the size specified using the files-size command below. 0 means there is no time limit.

Table 256 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 / USG stops the capture and generates the capture file when either the file reaches this size or the time period specified (using the `duration` command above) expires.
`host-ip {ip-address | profile_name | any>`	Sets a host IP address or a host IP address object for which to capture packets. any means to capture packets for all hosts.
`host-port <0..65535>`	If you set the IP Type to any, `tcp`, or udp using the `proto-type` command below, you can specify the port number of traffic to capture.
`iface {add | del} {interface_name | virtual_interface_name}`	Adds or deletes an interface or a virtual interface for which to capture packets to the capture interfaces list.
`ip-version {ip|ip6|any}`	Sets wether to capture IPv4 or IPv6 traffic. Any means to capture packets for all types of traffic.
`proto-type {icmp | icmp6 | igmp | igrp | pim | ah | esp | vrrp | udp | tcp | any}`	Sets the protocol of traffic for which to capture packets. any means to capture packets for all types of traffic.
`snaplen <68..1512>`	Specifies the maximum number of bytes to capture per packet. The ZyWALL / USG automatically truncates packets that exceed this size. As a result, when you view the packet capture files in a packet analyzer, the actual size of the packets may be larger than the size of captured packets.
`storage <internal|usbstorage>`	Sets to have the ZyWALL / USG only store packet capture entries on the ZyWALL / USG (internal) or on a USB storage connected to the ZyWALL / USG.
`ring-buffer <enable|disable>`	Enables or disables the ring buffer used as a temporary storage.
`split-size <1..2048>`	Specify a maximum size limit in megabytes for individual packet capture files. After a packet capture file reaches this size, the ZyWALL / USG starts another packet capture file.
`Ping {ipv4 | hostname} [source ipv4] [size <0..65507>] [forever| count <1..4096>]`	Sends an ICMP ECHO_REQUEST to test the reachability of a host on an IPv4 network and to measure the round-trip time for a message sent from the originating host to the destination computer. `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.

Table 256 Maintenance Tools Commands in Privilege Mode (continued)

COMMAND	DESCRIPTION
ping {ipv4_addr | *hostname*} [source *ipv4*] [size <0..65507>] [forever | count <1..4096>] [interface *interface_name*] [extension *filter-extension*]	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. Use the extension filter to extend the use of this command. source: Set source address to specified interface IPv4 address. 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. *interface_name*: specifies interface through which to send the ECHO_REQUEST packets. *filter_extension*: You can use 1-256 alphanumeric characters, spaces, or '()+,/:=?;!*#@$_%.- characters.
ping6{*ipv6* | *hostname*} [source *ipv6*] [size <0..65527>] [forever| count <1..4096>] [interface {*interface_name* | *virtual_interface_name*}][extension *filter_extension*]	Sends an ICMP ECHO_REQUEST to test the reachability of a host on an IPv6 network and to measure the round-trip time for a message sent from the originating host to the destination computer. Use the extension filter to extend the use of this command. source: Set source address to specified interface IPv6 address. When pinging IPv6 link-local address this option is required. size: specifies the number of data bytes to be sent count: Stop after sending this number of ECHO_REQUEST packets. forever: keep sending ECHO_REQUEST packets until you use Ctrl+c to stop. *interface_name*: specifies interface through which to send the ECHO_REQUEST packets. *filter_extension*: You can use 1-256 alphanumeric characters, spaces, or '()+,/:=?;!*#@$_%.- characters.
traceroute {*ipv4* | *hostname*} [source *ipv4*] [interface *interface_name*] [extension *filter-extension*]	Displays the route packets take to an IPv4 network host. Use the extension filter to extend the use of this command. source: Set source address to specified interface IPv4 address. *interface_name*: specifies a network interface to obtain the source IP address for outgoing probe packets. *filter_extension*: You can use 1-256 alphanumeric characters, spaces, or '()+,/:=?;!*#@$_%.- characters.
traceroute6 {*ipv6* | *hostname*} [source *ipv6*] [interface *interface_name*] [extension *filter-extension*]	Displays the route packets take to an IPv6 network host. Use the extension filter to extend the use of this command. source: Set source address to specified interface IPv6 address. *interface_name*: specifies a network interface to obtain the source IP address for outgoing probe packets. *filter_extension*: You can use 1-256 alphanumeric characters, spaces, or '()+,/:=?;!*#@$_%.- characters.
tracepath6 {*ipv6* | *hostname*}	Displays the path MTU for the target address.
show packet-capture status	Displays whether a packet capture is ongoing.

Table 256 Maintenance Tools Commands in Privilege Mode (continued)

COMMAND	DESCRIPTION
`show ipv6 neighbor-list`	Displays the ZyWALL / USG's IPv6 neighbors.
`show packet-capture config`	Displays current packet capture settings.

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

Table 257 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.

63.1 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 258 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
```

63.1.1 Packet Capture Command Example

The following examples show how to configure packet capture settings and perform a packet capture. First you have to check whether a packet capture is running. This example shows no other packet capture is running. Then you can also check the current packet capture settings.

```
Router(config)# show packet-capture status
capture status: off
Router(config)#
Router(config)# show packet-capture config
iface: None
ip-version: any
proto-type: any
host-port: 0
host-ip: any
file-suffix: -packet-capture
snaplen: 1500
duration: 0
file-size: 10
split-size: 2
ring-buffer: 0
storage: 0
```

Then configure the following settings to capture packets going through the ZyWALL / USG’s WAN1 interface only.

- IP address: any
- Host IP: any
- Host port: any (then you do not need to configure this setting)
- File suffix: Example
- File size: 10 megabytes
- Duration: 150 seconds
- Save the captured packets to: USB storage device
- Use the ring buffer: no
- The maximum size of a packet capture file: 100 megabytes

```
Router(config)# packet-capture configure
Router(packet-capture)# iface add wan1
Router(packet-capture)# ip-type any
Router(packet-capture)# host-ip any
Router(packet-capture)# file-suffix Example
Router(packet-capture)# files-size 10
Router(packet-capture)# duration 150
Router(packet-capture)# storage usbstorage
Router(packet-capture)# ring-buffer disable
Router(packet-capture)# split-size 100
Router(packet-capture)#
```

Exit the sub-command mode and have the ZyWALL / USG capture packets according to the settings you just configured.

```
Router(packet-capture)# exit
Router(config)# packet-capture activate
Router(config)#
```

Manually stop the running packet capturing.

```
Router(config)# no packet-capture activate
Router(config)#
```

Check current packet capture status and list all stored packet captures.

```
Router(config)# show packet-capture status
capture status: off
Router(config)# dir /packet_trace
File Name                                          Size     Modified Time
===========================================================================
wan1-Example.cap                                   575160   2009-11-24 09:06:59
Router(config)#
```

You can use FTP to download a capture file. Open and study it using a packet analyzer tool (for example, Ethereal or Wireshark).

Watchdog Timer

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

64.1 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 259 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.

64.2 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 260 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.

64.3 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 261 app-watchdog Commands

COMMAND	DESCRIPTION
`[no] app-watch-dog activate`	Turns the application watchdog timer on or off.
`[no] app-watch-dog auto-recover`	If app-watch-dog detects a dead process, app-watch-dog will try to auto recover. The no command turns off auto-recover
`[no] app-watch-dog console-print {always|once}`	Display debug messages on the console (every time they occur or once). The no command changes the setting back to the default.
`[no] app-watch-dog cpu-threshold min <1..100> max <1..100>`	Sets the percentage thresholds for sending a CPU usage alert. The ZyWALL / USG starts sending alerts when CPU usage exceeds the maximum (the second threshold you enter). The ZyWALL / USG stops sending alerts when the CPU usage drops back below the minimum threshold (the first threshold you enter). The no command changes the setting back to the default.
`[no] app-watch-dog interval <6..300>`	Sets how frequently (in seconds) the ZyWALL / USG checks the system processes. The no command changes the setting back to the default.
`[no] app-watch-dog retry-count <1..5>`	Set how many times the ZyWALL / USG is to re-check a process before considering it failed. The no command changes the setting back to the default.
`[no] app-watch-dog alert`	Has the ZyWALL / USG send an alert the user when the system is out of memory or disk space.
`[no] app-watch-dog disk-threshold min <1..100> max <1..100>`	Sets the percentage thresholds for sending a disk usage alert. The ZyWALL / USG starts sending alerts when disk usage exceeds the maximum (the second threshold you enter). The ZyWALL / USG stops sending alerts when the disk usage drops back below the minimum threshold (the first threshold you enter). The no command changes the setting back to the default.
`[no] app-watch-dog mem-threshold min <1..100> max <1..100>`	Sets the percentage thresholds for sending a memory usage alert. The ZyWALL / USG starts sending alerts when memory usage exceeds the maximum (the second threshold you enter). The ZyWALL / USG stops sending alerts when the memory usage drops back below the minimum threshold (the first threshold you enter). The no command changes the setting back to the default.
`app-watch-dog reboot-log flush`	Flushes the reboot log record.
`[no] app-watch-dog sys-reboot`	If auto recover fail reaches the maximum retry count, app-watch-dog reboots the device. The no command turns off system auto reboot.
`show app-watch-dog config`	Displays the application watchdog timer settings.
`show app-watch-dog monitor-list`	Display the list of applications that the application watchdog is monitoring.
`show app-watch-dog reboot-log`	Displays the application watchdog reboot log.

64.3.1 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.