ZyWALL 1050

Internet Security Gateway

CLI Reference Guide

Version 1.00
9/2006
Edition 3

ZyXEL

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

FCC Statement

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

1. This switch may not cause harmful interference.
2. This switch must accept any interference received, including interference that may cause undesired operations.

FCC Warning

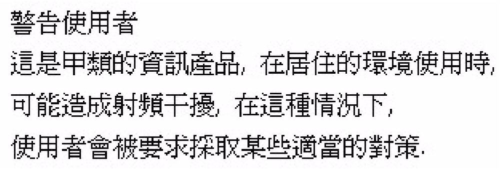
This equipment has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection)

A Warning:



警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Certifications

1 Go to www.zyxel.com.

2 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.

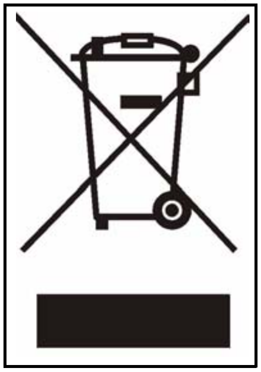
3 Select the certification you wish to view from this page.

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Connect the power cord to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.

This product is recyclable. Dispose of it properly.



ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Customer Support

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD	**SUPPORT E-MAIL**	**TELEPHONE**[A]	**WEB SITE**	**REGULAR MAIL**
LOCATION	**SALES E-MAIL**	**FAX**	**FTP SITE**	
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
COSTA RICA	soporte@zyxel.co.cr	+506-2017878	www.zyxel.co.cr	ZyXEL Costa Rica Plaza Roble Escazú Etapa El Patio, Tercer Piso San José, Costa Rica
	sales@zyxel.co.cr	+506-2015098	ftp.zyxel.co.cr	
CZECH REPUBLIC	info@cz.zyxel.com	+420-241-091-350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
	info@cz.zyxel.com	+420-241-091-359		
DENMARK	support@zyxel.dk	+45-39-55-07-00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 2860 Soeborg Denmark
	sales@zyxel.dk	+45-39-55-07-07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33-4-72-52-97-97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33-4-72-52-19-20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
HUNGARY	support@zyxel.hu	+36-1-3361649	www.zyxel.hu	ZyXEL Hungary 48, Zoldlomb Str. H-1025, Budapest Hungary
	info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN	http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave.,Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
	sales@zyxel.kz	+7-3272-590-689		
NORTH AMERICA	support@zyxel.com	1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	

METHOD	SUPPORT E-MAIL	TELEPHONE[A]	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
NORWAY	support@zyxel.no	+47-22-80-61-80	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47-22-80-61-81		
POLAND	info@pl.zyxel.com	+48 (22) 333 8250	www.pl.zyxel.com	ZyXEL Communications ul. Okrzei 1A 03-715 Warszawa Poland
		+48 (22) 333 8251		
RUSSIA	http://zyxel.ru/support	+7-095-542-89-29	www.zyxel.ru	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
	sales@zyxel.ru	+7-095-542-89-25		
SPAIN	support@zyxel.es	+34-902-195-420	www.zyxel.es	ZyXEL Communications Arte, 21 5ª planta 28033 Madrid Spain
	sales@zyxel.es	+34-913-005-345		
SWEDEN	support@zyxel.se	+46-31-744-7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46-31-744-7701		
UKRAINE	support@ua.zyxel.com	+380-44-247-69-78	www.ua.zyxel.com	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
	sales@ua.zyxel.com	+380-44-494-49-32		
UNITED KINGDOM	support@zyxel.co.uk	+44-1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44-1344 303034	ftp.zyxel.co.uk	

a. “+” is the (prefix) number you enter to make an international telephone call.

Table of Contents

Chapter 6

Chapter 7

Chapter 8

List of Figures

List of Tables

Preface

Congratulations on your purchase of the ZyWALL.

About This User's Guide

This manual is designed to guide you through the configuration of your ZyWALL for its various applications using the CLI (Command Line Interface). Generally, it is organized by feature as outlined in the web configurator.

Note: See the web configurator User’s Guide for related information on all features.

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.

- User’s Guide

  The User’s Guide explains how to use the web configurator to configure the ZyWALL.

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

- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.

- ZyXEL Web Site

  Please go to http://www.zyxel.com for product news, firmware, updated documents, and other support materials.

User Guide Feedback

Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you!

CHAPTER 1 Command Line Interface

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

1.1 Overview

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

1.1.1 The Configuration File

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

You can perform the following with a configuration file:

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

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

1.2 Accessing the CLI

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

Note: The ZyWALL might force you to log out of your session if reauthentication time, lease time, or idle timeout is reached. See Chapter 21 on page 163 for more information about these settings.

1.2.1 Console Port

See the User’s Guide for console port settings. When you turn on your ZyWALL, it performs several internal tests as well as line initialization. You can view the initialization information using the console port.

Figure 1 Console Port Power-on Display

```
Main Processor : Intel Pentium(R) 4 2.80GHz(133x21.0)
Memory Testing :  346432K OK









Press DEL to enter SETUP60, ESC to skip memory test
```

After the initialization, the login screen displays.

Figure 2 The Login Screen

```
Welcome to ZyWALL 1050

Username:
```

Enter the user name and password at the prompts.

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

1.2.2 Web Configurator Console

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

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

1 Log into the web configurator.

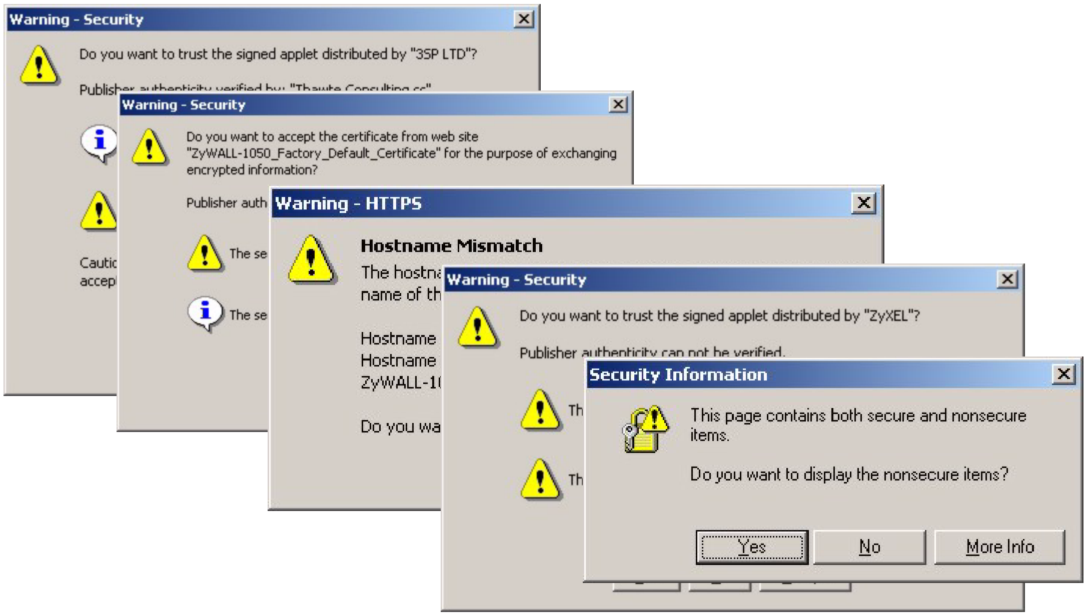
2 Click the **Console** icon 🖥 in the top-right corner of the web configurator screen.

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

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

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

Figure 3 Web Console: Security Warnings



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

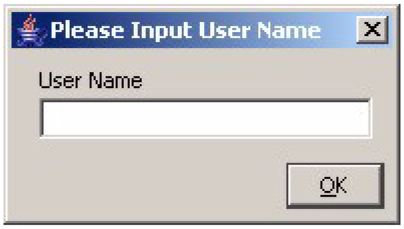
Security Information

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



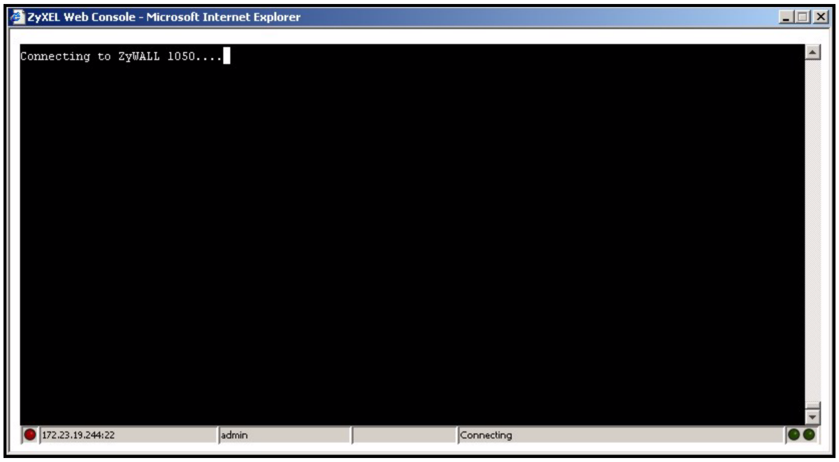
Please Input User Name

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.

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

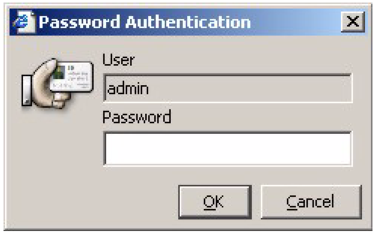
Figure 5   Web Console: Connecting



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

Then, the **Password** screen appears.

Figure 6   Web Console: Password



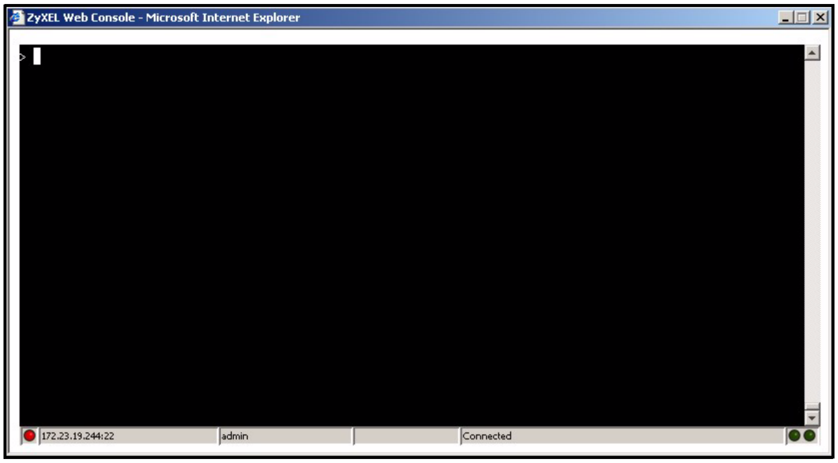
User

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



```
>
```

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

1.2.3 Telnet

Use the following steps to Telnet into your ZyWALL.

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

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

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

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

1.2.4 SSH (Secure SHell)

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

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

Figure 8 SSH Login Example

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

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

1.3 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 *italicized*.
- 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.

1.3.1 Changing the Password

It is highly recommended that you change the password for accessing the ZyWALL. See Section 21.2 on page 164 for the appropriate commands.

1.4 CLI Modes

You run CLI commands in one of several modes.

Table 1 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

Table 1 CLI Modes (continued)

	USER	PRIVILEGE	CONFIGURATION	SUB-COMMAND
What **Admin** users can do	• Look at system information (like **Status** screen) • Run basic diagnostics	• Look at system information (like **Status** screen) • Run basic diagnostics	• Configure simple features (such as an address object) • Create or remove complex parts (such as an interface)	• Configure complex parts (such as an interface) in the ZyWALL
How you enter it	Log in to the ZyWALL	Type **enable** in **User** mode	Type **configure terminal** in **User** or **Privilege** mode	Type the command used to create the specific part in **Configuration** mode

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

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

See Chapter 21 on page 163 for more information about the user types. **User** users can only log in, look at (but not run) the available commands in **User** mode, and log out. **Limited-Admin** users can look at the configuration in the web configurator and CLI, and they can run basic diagnostics in the CLI. **Admin** users can configure the ZyWALL in the web configurator or CLI.

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

1.5 Shortcuts and Help

1.5.1 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> ?
apply
clear
configure
copy
delete
 ------------------[Snip]--------------------
run
setenv
show
traceroute
write
Router>
```

Figure 10 Help: Available Command Example 2

```
Router> show ?
aaa
account
address-object
alg
 ------------------[Snip]--------------------
username
users
version
vrrp
zone
Router> show
```

1.5.2 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>
access-group
port
|
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
```

1.5.3 Entering Partial Commands

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

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

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

Figure 13 Non-Unique Partial Command Example

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

1.5.4 Command History

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

1.5.5 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.

1.5.6 Erase Current Command

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

1.6 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>
```

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

Table 2 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>
<tr><td><connection_id></td><td>1+</td><td>alphanumeric or -_:</td></tr>
<tr><td><contact></td><td>1-61</td><td>alphanumeric, spaces, or '()+,/:=?;!*#@$_%-.</td></tr>
<tr><td><country code></td><td>0 or 2</td><td>alphanumeric</td></tr>
<tr><td><custom signature file name></td><td>0-30</td><td>alphanumeric or _-.
first character: letter</td></tr>
<tr><td rowspan="4"><description></td><td colspan="2">Used in keyword criteria for log entries</td></tr>
<tr><td>1-64</td><td>alphanumeric, spaces, or '()+,/:=?;!*#@$_%-.</td></tr>
<tr><td colspan="2">Used in other commands</td></tr>
<tr><td>1-61</td><td>alphanumeric, spaces, or '()+,/:=?;!*#@$_%-</td></tr>
<tr><td><distinguished name></td><td>1-511</td><td>alphanumeric, spaces, or .@=,_-</td></tr>
<tr><td rowspan="6">domain name</td><td colspan="2">Used in content filtering</td></tr>
<tr><td>0+</td><td>lower-case letters, numbers, or .-</td></tr>
<tr><td colspan="2">Used in ip dns server</td></tr>
<tr><td>0-247</td><td>alphanumeric or .-
first character: alphanumeric or -</td></tr>
<tr><td colspan="2">Used in domainname, ip dhcp pool, and ip domain</td></tr>
<tr><td>0-254</td><td>alphanumeric or ._-
first character: alphanumeric or -</td></tr>
<tr><td><email></td><td>1-63</td><td>alphanumeric or .@_-</td></tr>
<tr><td><e-mail></td><td>1-64</td><td>alphanumeric or .@_-</td></tr>
<tr><td><encryption key></td><td>16-64
8-32</td><td>“0x” or “0X” + 16-64 hexadecimal values
alphanumeric or ;\|`~!@#$%^&*()_+\\{}':,./<>=-</td></tr>
<tr><td><file name></td><td>0-31</td><td>alphanumeric or _-</td></tr>
<tr><td><filter extension></td><td>1-256</td><td>alphanumeric, spaces, or '()+,/:=?;!*#@$_%.-</td></tr>
</table>

Table 2 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
<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
<inital string>	1-64	alphanumeric, spaces, or '()+,/:=!*#@$_%-.&
<isp account password>	0-63	alphanumeric or `~!@#$%^&*()_\-+={}|\;:'<,>./
<isp account username>	0-30	alphanumeric or -_@$./
<key length>	--	512, 768, 1024, 1536, 2048
license key	25	"S-" + 6 upper-case letters or numbers + "-" + 16 upper-case letters or numbers
<mac address>	--	aa:bb:cc:dd:ee:ff (hexadecimal)
<mail server fqdn>		lower-case letters, numbers, or -.
<name>	1-31	alphanumeric or _-
<notification message>	1-81	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-
<password: less than 15 chars>	1-15	alphanumeric or `~!@#$%^&*()_\-+={}|\;:'<,>./
<password: less than 8 chars>	1-8	alphanumeric or ;/?:@&=+$\.-_!~*'()%,#$
<password>	Used in user and ip ddns	
	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<,>./
	Used in e-mail log profile SMTP authentication	
	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<>./
	Used in device HA synchronization	
	1-63	alphanumeric or ~#%^*_-={}:,.
	Used in registration	
	6-20	alphanumeric or .@_-
<phone number>	1-20	numbers or ,+

Table 2 Input-Value Formats for Strings in CLI Commands (continued)

<table>
<tr><th>TAG</th><th># VALUES</th><th>LEGAL VALUES</th></tr>
<tr><td><preshared key></td><td>16-64</td><td>“0x” or “0X” + 16-64 hexadecimal values
alphanumeric or ;|`~!@#$%^&*()_+\{}':,./<>=-</td></tr>
<tr><td><profile name></td><td>0-30</td><td>alphanumeric or _-
first character: letters or _-</td></tr>
<tr><td><proto name></td><td>1-16</td><td>lower-case letters, numbers, or -</td></tr>
<tr><td><protocol name></td><td>0-30</td><td>alphanumeric or _-
first character: letters or _-</td></tr>
<tr><td><quoted string less than 127 chars></td><td>1-255</td><td>alphanumeric, spaces, or ;/?:@&=+$\.-_!~*'()%,</td></tr>
<tr><td><quoted string less than 63 chars></td><td>1-63</td><td>alphanumeric, spaces, or ;/?:@&=+$\.-_!~*'()%</td></tr>
<tr><td><quoted string></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>
<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>
</table>

Table 2 Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
user@domainname	1-80	alphanumeric or .@_-
<vrrp group name: less than 15 chars>	1-15	alphanumeric or _-
<week-day sequence, i.e. 1=first,2=second>	1	1-4
<xauth method>	1-31	alphanumeric or _-
<xauth password>	1-31	alphanumeric or ;|`~!@#$%^&*()_+\{}':,./<>=-
<ZyNOS style mac address>	0-12 (even number)	hexadecimal for example: aa aabbcc aabbccddeeff

1.7 Saving Configuration Changes

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

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

1.8 Logging Out

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

CHAPTER 2 User and Privilege Modes

This chapter describes how to use these two modes.

2.1 User And Privilege Modes

This is the mode you are in when you first log into the CLI. (Do not confuse 'user mode' with types of user accounts the ZyWALL uses. See Chapter 21 on page 163 for more information about the user types. 'User' type accounts can only run 'exit' in this mode. However, they may need to log into the device in order to be authenticated for 'user-aware' policies, for example a firewall rule that a particular user is exempt from or a VPN tunnel that only certain people may use.)

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

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

Table 3 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.
diag	P	Performs diagnostic commands.
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.
htm	U/P	Goes to htm (hardware test module) mode.

Table 3 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 of 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.
psm	U/P	Goes to psm (product support module) mode.
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 cached data to disk and stops the system processes. It does not turn off the power.
traceroute	P	Traces the route to the specified host name or IP address.
write	P	Saves the current configuration to the ZyWALL. All unsaved changes are lost after the ZyWALL restarts.

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

2.1.1 Debug Commands

Debug commands marked with an asterisk (*) are not available when the debug flag is on and are for service personnel use only. The debug commands follow a syntax that is Linux-based, so the Linux equivalent is displayed in this chapter for your reference.

Table 4 Debug Commands

COMMAND SYNTAX	DESCRIPTION	LINUX COMMAND EQUIVALENT
debug interface ifconfig [interface]	Shows system interfaces detail	> ifconfig [interface]
debug system ps	Shows system process information	> ps aux
debug system ipcs	Shows system IPC information	> ipcs
debug system vmstat	Shows system memory statistics	> vmstat
debug system free	Shows free and used memory in the system	> free

Table 4 Debug Commands (continued)

COMMAND SYNTAX	DESCRIPTION	LINUX COMMAND EQUIVALENT
debug system dmesg	Shows kernel debug messages	> demsg
debug system lsmod (*)	Shows system kernel modules	> lsmod
debug system tcpdump interface	Dump traffic on a network	> tcpdump –i interface
debug system ip route show table {default|local|main|num}	Shows IP routing information	
debug system ip route get ip_addr	Shows IP routing to the specifiied IP address.	> ip route
debug system ip addr	Shows interface IP address information	> ip addr
debug system iptables list table {nat|filter|mangle|vpn|zymark|vpnid|cfilter}	Shows system netfilter information.	
debug system iptables list chain {forward|prerouting|postrouting|input|output|pre_id}	Shows netfilter information	> iptables –L –t {nat|filter|mangle|vpn|zymark|vpnid|cfilter}
debug system ip rule	Shows IP routing tables	> ip rule
debug system tc {class|filter|qdisc} list	Shows system traffic control information	> tc {class|filter|qdisc} list
debug system show conntrack	Shows system sessions list	> cat /proc/net/ip_conntrack
debug system show slabinfo	Shows kernel cache information	> cat /proc/slabinfo
debug system show ksyms (*)	Shows kernel symbols	> cat /proc/ksyms
debug app show l7protocol (*)	Shows app patrol protocol list	> cat /etc/l7_protocols/protocol.list
debug gui show cgidump (*)	Shows gui cgi command buffer	> cat /tmp/zysh-cgi.dump
debug zyinetpkt {set|show} {desitnation|hooknum|protocol|enable|priority|source}	ZLD internal packet trace debug command	NA
debug app	Application patol debug command	NA
debug idp	IDP debug command	NA
debug policy-route (*)	Policy route debug command	NA
debug update server (*)	Update server debug command	NA
debug cmdexec {on|off}	ZyShell debug commands	NA
debug service-register	Service registration debug command	NA
debug gui (*)	GUI cgi related debug commands	NA
debug myzyxel server (*)	Myzyxel.com debug commands	NA
debug show myzyxel server status	Myzyxel.com debug commands	NA
debug hardware (*)	Hardware debug commandss	NA

2.1.2 htm Commands

Hardware Test Module (HTM) commands are for testing hardware components.

Table 5 htm commands

COMMAND	DESCRIPTION
clear-log	Clears htm hardware failure logs.
complete	Performs internal and external (to an external device in your network) loop-back tests on all hardware components.
exit	Leaves htm sub-command mode
external	Performs external loop-back tests on all hardware components.
help	Shows related htm commands and valid parameters.
internal	Performs internal loop-back tests on all hardware components.
phase	Lists, adds or deletes phase test items
show-log	Shows all htm hardware failure logs.

2.1.3 psm Commands

Product Support Module (PSM) commands are for setting product parameters.

Table 6 psm Commands

COMMAND	DESCRIPTION	ZYNOS EQUIVALENT
psm athe	Displays all available PSM commands.	ATHE
psm help	Displays all available PSM commands	ATHE
psm atwe MAC COUNTRY_CODE ENGDBGFLAG FEATURE_BIT HARDWARE_VERSION SERIES_NUMBER	Writes MAC addr, country code,EngDbgFlag,Main Feature Bit, Hardware Version, Serial Number to flash ROM	ATWE a(,b,c,d,e,f)
psm atcu COUNTRY_CODE	Writes country code to flash ROM	ATCUx
psm atcb	Copies from flash ROM to working buffer	ATCB
psm atcl	Clears working buffer	ATCL
psm atsb	Saves working buffer to flash ROM	ATSB
psm atbu	Shows manufacturer related data in working buffer	ATBU
psm atsh	Shows manufacturer related data in flash ROM	ATSH
psm atwm MAC	Sets MAC address in working buffer. If there are n physical ports, the MAC address will be assigned to each physical port by adding 1 to MAC incrementally.	ATWMx
psm atco COUNTRY_CODE	Sets country code in working buffer	ATCOx

Table 6 psm Commands

COMMAND	DESCRIPTION	ZYNOS EQUIVALENT
psm atfl ENGDBGFLAG	Sets EngDebugFlag in working buffer	ATFLx
psm atst ROMRAS_ADDRESS	Sets ROMRAS address in working buffer	ATSTx
psm atsy SYSTEM_TYPE	Sets system type (in hex value) in working buffer	ATSYx
diag psm atvd VENDOR_NAME	Sets vendor name in working buffer	ATVDx
psm atpn PRODUCT_NAME	Sets product name in working buffer	ATPNx
psm atfe <0..29> FEATURE_BITS	Sets feature bits in working buffer	ATFEx,y,...
psm atse	Shows the password seed for EngDbgFlag to get more privilege to commands	ATSE
psm athv HARDWARE_VERSION	Sets hardware version	ATHV
psm atsn SERIES_NUMBER	Sets series number	ATSN
psm atba BAUD_RATE	Changes baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k 5:115.2k	ATBA
psm aten ENGDBGFLAG AUTH_PHRASE	Login by debug account to set EngDebugFlag	ATEN
psm atbt BOOTBLOCK_FLAG	block0 write enable (1=enable, other=disable	ATBT

CHAPTER 3 Registration

This chapter introduces myzyxel.com and shows you how to register the ZyWALL for IDP and Content Filtering service using commands.

3.1 myZyXEL.com overview

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

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

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

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

3.1.1 Subscription Services Available on the ZyWALL

At the time of writing, the ZyWALL can use content filtering and IDP (Intrusion Detection and Prevention) subscription services.

Content filtering allows or blocks access to web sites. Subscribe to category-based content filtering to block access to categories of web sites based on content. Your ZyWALL accesses an external database that has millions of web sites categorized based on content. You can have the ZyWALL block, block and/or log access to web sites based on these categories.

The IDP feature uses the signature files on the ZyWALL to detect malicious or suspicious packets and respond immediately. After the service is activated, the ZyWALL can download the up-to-date signature files from the update server (http://myupdate.zywall.zyxel.com).

You will get automatic e-mail notification of new signature releases from mySecurityZone after you activate the IDP service. You can also check for new signatures at http://mysecurity.zyxel.com.

See the chapters about content filtering and IDP for more information.

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

3.2 Registration Commands

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

Table 7 Input Values for General Registration Commands

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

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

Table 8 Command Summary: Registration

COMMAND	DESCRIPTION
`device-register checkuser` *user_name*	Checks if the user name exists in the myZyXEL.com database.
`device-register username` *user_name* `password` *password* `[e-mail` *user@domainname* `country-code` *country_code*`]`	Registers the device with an existing account or creates a new account and registers the device at one time. *country_code*: see Table 9 on page 51
`service-register checkexpire`	Gets information of all service subscriptions from myZyXEL.com and updates the status table.
`service-register service-type standard license-key` *keyvalue*	Activates a standard service subscription with the license key.
`service-register service-type trial service {all|content-filter|idp}`	Activates the trial service subscription(s).
`show device-register status`	Displays whether the device is registered and account information.
`show service-register status {all|content-filter|idp}`	Displays service license information.

3.2.1 Command Examples

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

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

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

```
Router# configure terminal
Router(config)# show device-register status
username               : alexctsui
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     Expiration
========================================================================
IDP Signature Update Licensed     Standard 370
Content-Filter       Expired      Trial    0
```

3.3 Country Code

The following table displays the number for each country.

Table 9 Country Code

COUNTRY CODE	COUNTRY NAME	COUNTRY CODE	COUNTRY NAME
001	Afghanistan	002	Albania
003	Algeria	004	American Samoa
005	Andorra	006	Angola
007	Anguilla	008	Antarctica
009	Antigua & Barbuda	010	Argentina
011	Armenia	012	Aruba
013	Ascension Island	014	Australia

Table 9 Country Code (continued)

COUNTRY CODE	COUNTRY NAME	COUNTRY CODE	COUNTRY NAME
015	Austria	016	Azerbaijan
017	Bahamas	018	Bahrain
019	Bangladesh	020	Barbados
021	Belarus	022	Belgium
023	Belize	024	Benin
025	Bermuda	026	Bhutan
027	Bolivia	028	Bosnia and Herzegovina
029	Botswana	030	Bouvet Island
031	Brazil	032	British Indian Ocean Territory
033	Brunei Darussalam	034	Bulgaria
035	Burkina Faso	036	Burundi
037	Cambodia	038	Cameroon
039	Canada	040	Cape Verde
041	Cayman Islands	042	Central African Republic
043	Chad	044	Chile
045	China	046	Christmas Island
047	Cocos (Keeling) Islands	048	Colombia
049	Comoros	050	Congo, Democratic Republic of the
051	Congo, Republic of	052	Cook Islands
053	Costa Rica	054	Cote d'Ivoire
055	Croatia/Hrvatska	056	Cyprus
057	Czech Republic	058	Denmark
059	Djibouti	060	Dominica
061	Dominican Republic	062	East Timor
063	Ecuador	064	Egypt
065	El Salvador	066	Equatorial Guinea
067	Eritrea	068	Estonia
069	Ethiopia	070	Falkland Islands (Malvina)
071	Faroe Islands	072	Fiji
073	Finland	074	France
075	France (Metropolitan)	076	French Guiana
077	French Polynesia	078	French Southern Territories
079	Gabon	080	Gambia
081	Georgia	082	Germany
083	Ghana	084	Gibraltar
085	Great Britain	086	Greece
087	Greenland	088	Grenada
089	Guadeloupe	090	Guam

Table 9 Country Code (continued)

COUNTRY CODE	COUNTRY NAME	COUNTRY CODE	COUNTRY NAME
091	Guatemala	092	Guernsey
093	Guinea	094	Guinea-Bissau
095	Guyana	096	Haiti
097	Heard and McDonald Islands	098	Holy See (City Vatican State)
099	Honduras	100	Hong Kong
101	Hungary	102	Iceland
103	India	104	Indonesia
105	Ireland	106	Isle of Man
107	Italy	108	Jamaica
109	Japan	110	Jersey
111	Jordan	112	Kazakhstan
113	Kenya	114	Kiribati
115	Korea, Republic of	116	Kuwait
117	Kyrgyzstan	118	Lao People’s Democratic Republic
119	Latvia	120	Lebanon
121	Lesotho	122	Liberia
123	Liechtenstein	124	Lithuania
125	Luxembourg	126	Macau
127	Macedonia, Former Yugoslav Republic	128	Madagascar
129	Malawi	130	Malaysia
131	Maldives	132	Mali
133	Malta	134	Marshall Islands
135	Martinique	136	Mauritania
137	Mauritius	138	Mayotte
139	Mexico	140	Micronesia, Federal State of
141	Moldova, Republic of	142	Monaco
143	Mongolia	144	Montserrat
145	Morocco	146	Mozambique
147	Namibia	148	Nauru
149	Nepal	150	Netherlands
151	Netherlands Antilles	152	New Caledonia
153	New Zealand	154	Nicaragua
155	Niger	156	Nigeria
157	Niue	158	Norfolk Island
159	Northern Mariana Islands	160	Norway
161	Not Determined	162	Oman
163	Pakistan	164	Palau

Table 9 Country Code (continued)

COUNTRY CODE	COUNTRY NAME	COUNTRY CODE	COUNTRY NAME
165	Panama	166	Papua New Guinea
167	Paraguay	168	Peru
169	Philippines	170	Pitcairn Island
171	Poland	172	Portugal
173	Puerto Rico	174	Qatar
175	Reunion Island	176	Romania
177	Russian Federation	178	Rwanda
179	Saint Kitts and Nevis	180	Saint Lucia
181	Saint Vincent and the Grenadines	182	San Marino
183	Sao Tome and Principe	184	Saudi Arabia
185	Senegal	186	Seychelles
187	Sierra Leone	188	Singapore
189	Slovak Republic	190	Slovenia
191	Solomon Islands	192	Somalia
193	South Africa	194	South Georgia and the South Sandwich Islands
185	Spain	196	Sri Lanka
197	St Pierre and Miquelon	198	St. Helena
199	Suriname	200	Svalbard and Jan Mayen Islands
201	Swaziland	202	Sweden
203	Switzerland	204	Taiwan
205	Tajikistan	206	Tanzania
207	Thailand	208	Togo
209	Tokelau	210	Tonga
211	Trinidad and Tobago	212	Tunisia
213	Turkey	214	Turkmenistan
215	Turks and Caicos Islands	216	Tuvalu
217	US Minor Outlying Islands	218	Uganda
219	Ukraine	220	United Arab Emirates
221	United Kingdom	222	United States
223	Uruguay	224	Uzbekistan
225	Vanuatu	226	Venezuela
227	Vietnam	228	Virgin Islands (British)
229	Virgin Islands (USA)	230	Wallis And Futuna Islands
231	Western Sahara	232	Western Samoa
233	Yemen	234	Yugoslavia
235	Zambia	236	Zimbabwe

CHAPTER 4
File Manager

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

4.1 File Directories

The ZyWALL stores files in the following directories.

Table 10 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.

4.2 Configuration Files and Shell Scripts Overview

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

When you apply a configuration file, the ZyWALL uses the factory default settings for any features that the configuration file does not include. Shell scripts are files of commands that you can store on the ZyWALL and run when you need them. When you run a shell script, the ZyWALL only applies the commands that it contains. Other settings do not change.

You can edit configuration files or shell scripts in a text editor and upload them to the ZyWALL. Configuration files use a .conf extension and shell scripts use a .zysh extension.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

Figure 14 Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
# configure ge3
interface ge3
ip address 172.23.37.240 255.255.255.0
ip gateway 172.23.37.254 metric 1
exit
# create address objects for remote management / to-ZyWALL firewall rules
# use the address group in case we want to open up remote management later
address-object TW_SUBNET 172.23.37.0/24
object-group address TW_TEAM
address-object TW_SUBNET
exit
# enable Telnet access (not enabled by default, unlike other services)
ip telnet server
# open WAN-to-ZyWALL firewall for TW_TEAM for remote management
firewall WAN ZyWALL insert 4
sourceip TW_TEAM
service TELNET
action allow
exit
write
```

While configuration files and shell scripts have the same syntax, the ZyWALL applies configuration files differently than it runs shell scripts. This is explained below.

Table 11 Configuration Files and Shell Scripts in the ZyWALL

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

You have to run the example in Table 14 on page 56 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 1.4 on page 34 for more information about CLI modes.)

4.2.1 Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use “#” or “!” as the first character of a command line to have the ZyWALL treat the line as a comment.

Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the ZyWALL exit sub command mode.

Note: “exit” or “!'” must follow sub commands if it is to make the ZyWALL exit sub command mode.

Line 3 in the following example exits sub command mode.

```
interface ge1
ip address dhcp
!
```

Lines 1 and 3 in the following example are comments and line 4 exits sub command mode.

```
!
interface ge1
# this interface is a DHCP client
!
```

Lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2006/06/05
interface ge1
ip address dhcp
!
```

4.2.2 Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the ZyWALL processes the file line-by-line. The ZyWALL checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the ZyWALL finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The ZyWALL ignores any errors in the configuration file or shell script and applies all of the valid commands. The ZyWALL still generates a log for any errors.

4.2.3 ZyWALL Configuration File Details

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

- When you first receive the ZyWALL, it uses the **system-default.conf** configuration file of default settings.
- When you change the configuration, the ZyWALL creates a **startup-config.conf** file of the current configuration.
- The ZyWALL checks the **startup-config.conf** file for errors when it restarts. If there is an error in the **startup-config.conf** file, the ZyWALL copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file.
- When the ZyWALL reboots, if the **startup-config.conf** file passes the error check, the ZyWALL keeps a copy of the **startup-config.conf** file as the **lastgood.conf** configuration file for you as a back up file. If you upload and apply a configuration file with an error, you can apply **lastgood.conf** to return to a valid configuration.

4.2.4 Configuration File Flow at Restart

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

If there is a **startup-config.conf**, the ZyWALL checks it for errors and applies it. If there are no errors, the ZyWALL uses it and copies it to the **lastgood.conf** configuration file. If there is an error, the ZyWALL generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the ZyWALL applies the **system-default.conf** configuration file.

You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The ZyWALL ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The ZyWALL still generates a log for any errors.

4.3 File Manager Commands Input Values

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

Table 12 File Manager Command Input Values

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

4.4 File Manager Commands Summary

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

Table 13 File Manager Commands Summary

COMMAND	DESCRIPTION
apply /conf/*file_name.conf*	Has the ZyWALL use a specific configuration file. You must still use the write command to save your configuration changes to the flash ("non-volatile" or "long term") memory.
copy {/cert | /conf | /idp | /packet_trace | /script | /tmp}*file_name-a.conf* {/cert | /conf | /idp | /packet_trace | /script | /tmp}/*file_name-b.conf*	Saves a duplicate of a file on the ZyWALL from the source file name to the target file name. Specify the directory and file name of the file that you want to copy and the directory and file name to use for the duplicate. Always copy the file into the same directory.
copy running-config startup-config	Saves your configuration changes to the flash ("non-volatile" or "long term") memory. The ZyWALL immediately uses configuration changes made via commands, but if you do not use this command or the write command, the changes will be lost when the ZyWALL restarts.
copy running-config /conf/*file_name.conf*	Saves a duplicate of the configuration file that the ZyWALL is currently using. You specify the file name to which to copy.
delete {/cert | /conf | /idp | /packet_trace | /script | /tmp}/*file_name*	Removes a file. Specify the directory and file name of the file that you want to delete.
dir {/cert | /conf | /idp | /packet_trace | /script | /tmp}	Displays the list of files saved in the specified directory.
rename {/cert | /conf | /idp | /packet_trace | /script | /tmp}/*old-file_name* {/cert | /conf | /idp | /packet_trace | /script | /tmp}/*new-file_name*	Changes the name of a file. Specify the directory and file name of the file that you want to rename. Then specify the directory again followed by the new file name.
rename /script/*old-file_name* /script/*new-file_name*	Changes the name of a shell script.
run /script/*file_name.zysh*	Has the ZyWALL execute a specific shell script file. You must still use the write command to save your configuration changes to the flash ("non-volatile" or "long term") memory.
show running-config	Displays the settings of the configuration file that the system is using.
write	Saves your configuration changes to the flash ("non-volatile" or "long term") memory. The ZyWALL immediately uses configuration changes made via commands, but if you do not use the write command, the changes will be lost when the ZyWALL restarts.

4.5 File Manager Command Example

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
```

4.6 FTP File Transfer

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

4.6.1 Command Line FTP File Upload

1. Connect to the ZyWALL.
2. Enter “bin” to set the transfer mode to binary.
3. You can upload the firmware after you log in through FTP. To upload other files, use “cd” to change to the corresponding directory.
4. Use “put” to transfer files from the computer to the ZyWALL.[1] For example:

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

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

Note: Do not turn off the ZyWALL while firmware upload is in progress!

If you lose power during the firmware upload, you may need to refer to Section 4.7 on page 62 to recover the firmware.

4.6.2 Command Line FTP Configuration File Upload Example

The following example transfers a configuration file named tomorrow.conf from the computer and saves it on the ZyWALL as next.conf.

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

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

Figure 15 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.
```

4.6.3 Command Line FTP File Download

1 Connect to the ZyWALL.

2 Enter “bin” to set the transfer mode to binary.

3 Use “cd” to change to the directory that contains the files you want to download.

4 Use “dir” or “ls” if you need to display a list of the files in the directory.

5 Use "get” to download files. For example:

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

4.6.4 Command Line FTP Configuration File Download Example

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

Figure 16 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.
```

4.7 Firmware Recovery

This section describes how to recover the ZyWALL’s firmware if it has been damaged. Firmware damage could be caused for example by the power going off during a firmware upgrade. Use the following procedure if your device has stopped responding for an extended period of time and you cannot access or ping it. [1]

1 Use a console cable and connect to the ZyWALL via a terminal emulation program (such as HyperTerminal). Make sure that you use the correct settings in the terminal emulation program. See Section 1.2.1 on page 30 for the default console port settings.

2 If you cannot see any messages, restart the ZyWALL.

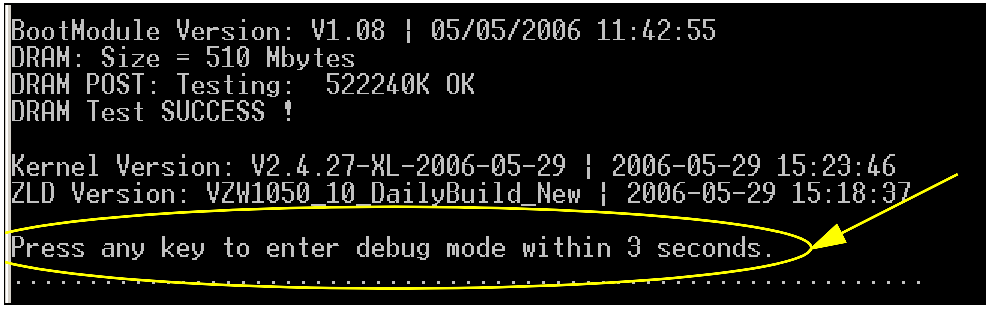
3 Your console session displays the ZyWALL’s startup messages. If not, you may want to try other console port speeds in case it has changed. [2]

4 The system startup messages display followed by “Press any key to enter debug mode within 3 seconds.” (see Figure 17 on page 63). If the console session displays nothing else for more than one minute, contact your local customer support.

[1] The ZyWALL does not respond while starting up. It takes less than five minutes to start up with the default configuration, but the start up time increases with the complexity of your configuration.

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

Figure 17 System Startup Stopped



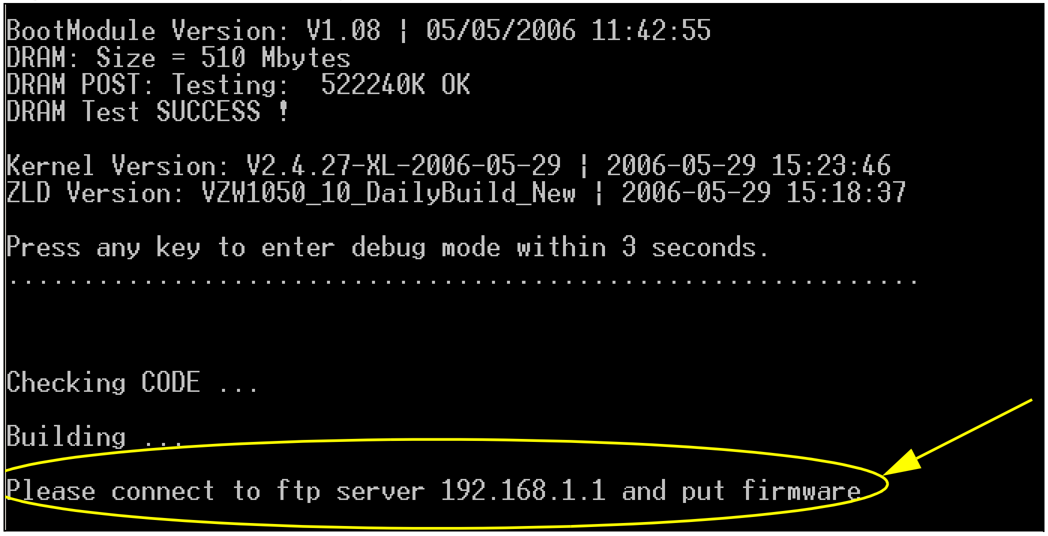
```
BootModule Version: V1.08 | 05/05/2006 11:42:55
DRAM: Size = 510 Mbytes
DRAM POST: Testing:  522240K OK
DRAM Test SUCCESS !

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.
.............................................................
```

5 If "Please connect to ftp server 192.168.1.1 and put firmware" displays on the screen, the firmware file is damaged and you need to use the procedure in Section 4.7.1 on page 63 to recover the firmware. If the message does not display, the firmware is OK and you do not need to use the firmware recovery procedure.

Figure 18 Firmware Damaged



```
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.
.............................................................



Checking CODE ...

Building ...

Please connect to ftp server 192.168.1.1 and put firmware
```

4.7.1 Firmware Recovery Procedure

This procedure requires the ZyWALL's firmware, which you can download from www.zyxel.com. The firmware file uses a .bin extension, for example, "1.00(XL.0).bin". Do the following after you have obtained the firmware file.

4.7.1.1 Connect to the ZyWALL

1 You will use FTP to upload the firmware. Keep the console session open in order to see when the firmware recovery finishes.

2 Set your computer to use a static IP address from 192.168.1.2 ~192.168.1.254. No matter how you have configured the ZyWALL's IP addresses, your computer must use a static IP address in this range to recover the firmware.

3 Connect your computer to the ZyWALL's port **1** (this is the only port that you can use for recovering the firmware).

4.7.1.2 Transfer the Firmware via FTP

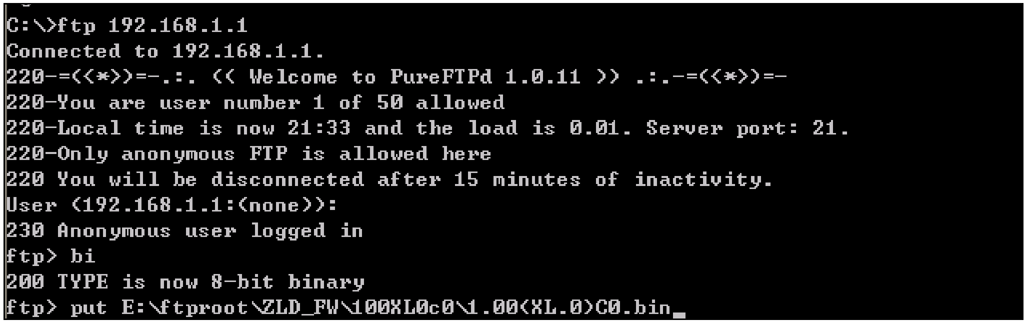
1 Use an FTP client on your computer to connect to the ZyWALL. This example uses the ftp command in the Windows command prompt. The ZyWALL's FTP server IP address for firmware recovery is 192.168.1.1.

2 Log in anonymously.

3 Set the transfer mode to binary. Use "bin" (or just "bi") in the Windows command prompt.

4 Transfer the firmware file from your computer to the ZyWALL (the command is "put 1.00(XL.0).bin" in the Windows command prompt).

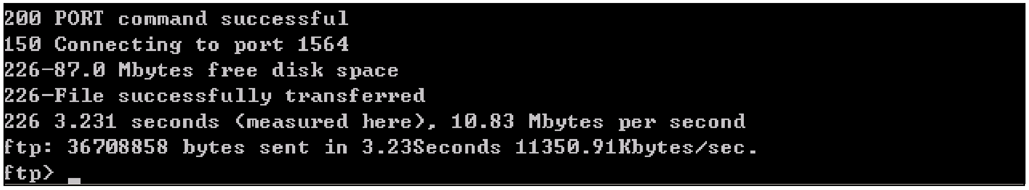
Figure 19 FTP Firmware Transfer Command



```
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_
```

5 Wait for the file transfer to complete.

Figure 20 FTP Firmware Transfer Complete

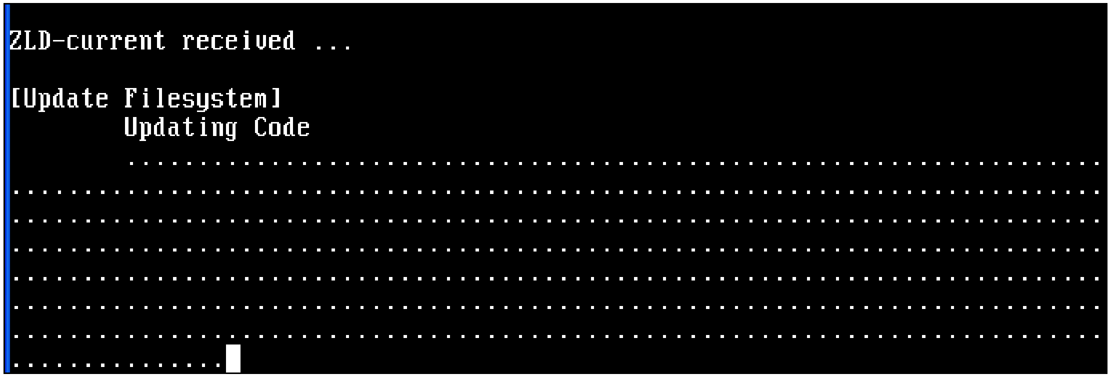


```
200 PORT command successful
150 Connecting to port 1564
226-87.0 Mbytes free disk space
226-File successfully transferred
226 3.231 seconds (measured here), 10.83 Mbytes per second
ftp: 36708858 bytes sent in 3.23Seconds 11350.91Kbytes/sec.
ftp> _
```

4.7.1.3 Monitor the Status in the Console Session

1 The console session displays "ZLD-current received" after the FTP file transfer is complete. Then you need to wait while the ZyWALL recovers the firmware (this may take up to four minutes).

Figure 21 Firmware Received and Recovery Started

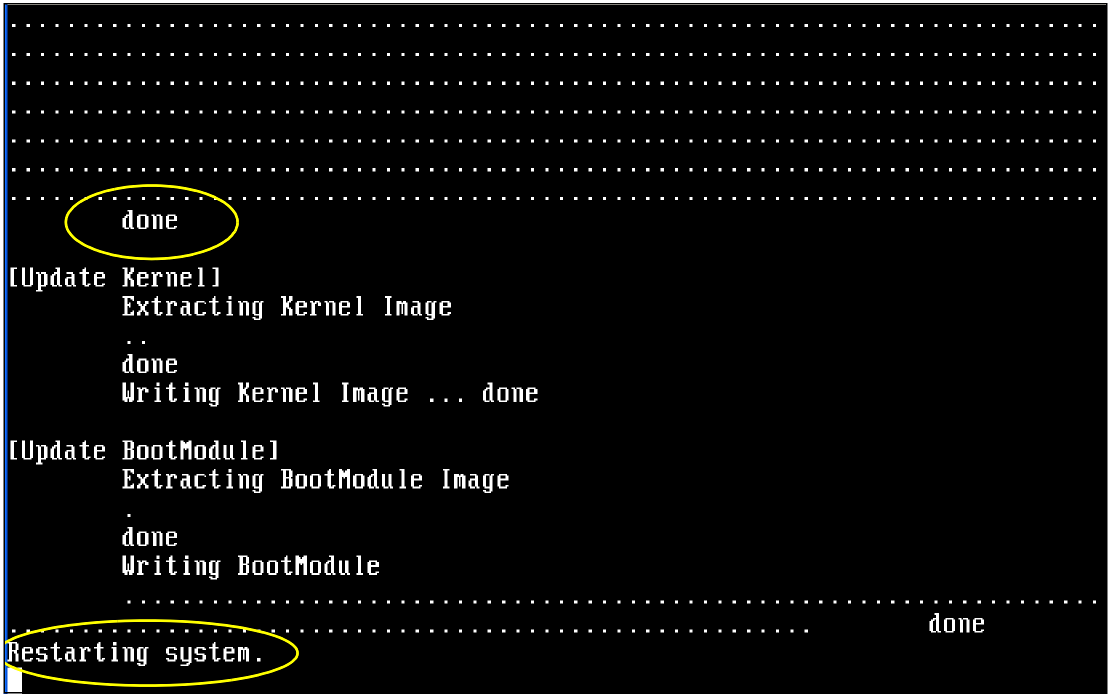


```
ZLD-current received ...

[Update Filesystem]
        Updating Code
        .............................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
..............
```

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

Figure 22 Firmware Recovery Complete and Restart



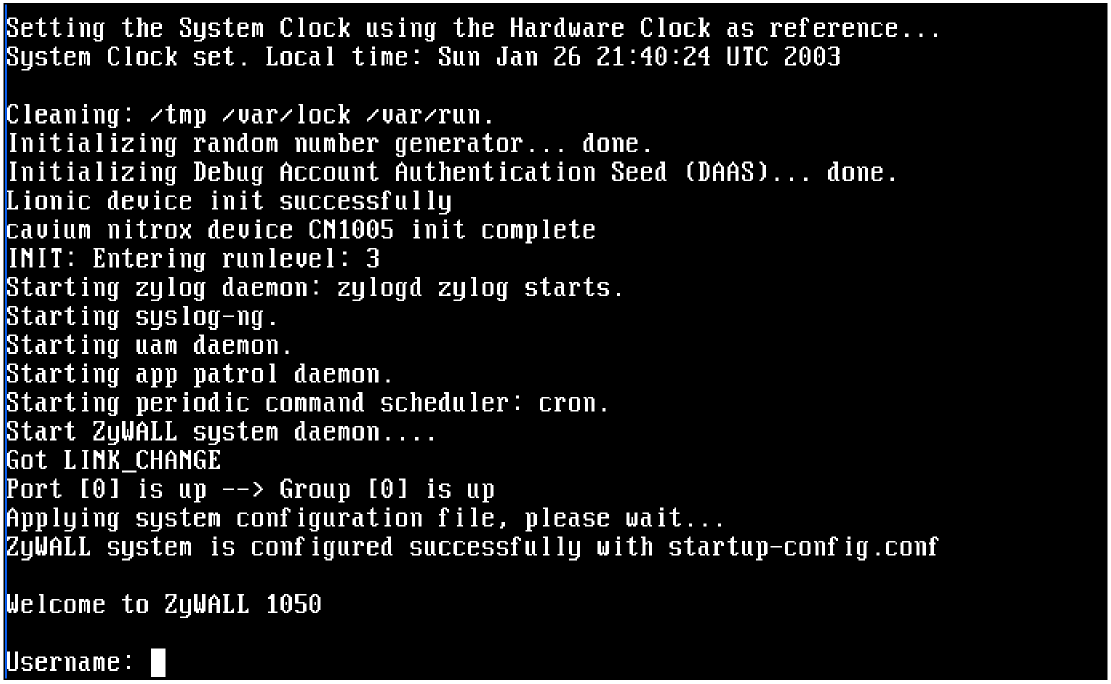
```
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
        done

[Update Kernel]
        Extracting Kernel Image
        ..
        done
        Writing Kernel Image ... done

[Update BootModule]
        Extracting BootModule Image
        .
        done
        Writing BootModule
        ....................................................................
...................................................              done
Restarting system.
```

3 The username prompt displays after the ZyWALL starts up successfully. The firmware recovery process is now complete and the ZyWALL is ready to use.

Figure 23 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:
```

CHAPTER 5 Interfaces

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

5.1 Interface Overview

In general, an interface has the following characteristics.

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

Some characteristics do not apply to some types of interfaces.

5.1.1 Types of Interfaces

You can create several types of interfaces in the ZyWALL.

- **Port groups** create a hardware connection between physical ports at the layer-2 (data link, MAC address) level.
- **Ethernet interfaces** are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- **VLAN interfaces** receive and send tagged frames. The ZyWALL automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- **Bridge interfaces** create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Unlike port groups, bridge interfaces can take advantage of some security features in the ZyWALL. You can also assign an IP address and subnet mask to the bridge.
- **PPPoE/PPTP interfaces** support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE/PPTP interfaces.
- **Virtual interfaces** provide additional routing information in the ZyWALL. There are three types: **virtual Ethernet interfaces**, **virtual VLAN interfaces**, and **virtual bridge interfaces**.
- The **auxiliary interface**, along with an external modem, provides an interface the ZyWALL can use to dial out. This interface can be used as a backup WAN interface, for example. The auxiliary interface controls the **DIAL BACKUP** port.

- **Trunks** manage load balancing between interfaces.

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

Table 14 Characteristics of Ethernet, VLAN, Bridge, PPPoE/PPTP, and Virtual Interfaces

CHARACTERISTICS	ETHERNET	VLAN	BRIDGE	PPPOE/PPTP	VIRTUAL
Name*	ge*x*	vlan*x*	br*x*	ppp*x*	**
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
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

5.1.2 Relationships Between Interfaces

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

Table 15 Relationships Between Different Types of Interfaces

INTERFACE	REQUIRED PORT / INTERFACE
auxiliary interface	auxiliary port
port group	physical port
Ethernet interface	physical port port group

Table 15 Relationships Between Different Types of Interfaces (continued)

INTERFACE	REQUIRED PORT / INTERFACE
VLAN interface	Ethernet interface
bridge interface	Ethernet interface* VLAN interface*
PPPoE/PPTP interface	Ethernet interface* VLAN interface* bridge interface
virtual interface **(virtual Ethernet interface)** **(virtual VLAN interface)** **(virtual bridge interface)**	Ethernet interface* VLAN interface* bridge interface
trunk	Ethernet interface VLAN interface bridge interface PPPoE/PPTP interface auxiliary interface

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

5.2 Interface Commands Summary

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

Table 16 Input Values for General Interface Commands

LABEL	DESCRIPTION
`interface_name`	The name of the interface. Ethernet interface: ge*x*, *x* = 1 - 5 virtual interface on top of Ethernet interface: ge*x*:*y*, *x* = 1 - 5, *y* = 1 - 4 VLAN interface: vlan*x*, *x* = 0 - 31 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 31, *y* = 1 - 4 bridge interface: br*x*, *x* = 0 - 11 virtual interface on top of bridge interface: br*x*:*y*, *x* = 0 - 11, *y* = 1 - 4 PPPoE/PPTP interface: ppp*x*, *x* = 0 - 11
`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 initial sections introduce commands that are supported by several types of interfaces. The remaining sections then introduce the unique commands for each type of interface.

5.2.1 Basic Interface Properties and IP Address Commands

This table lists basic properties and IP address commands.

Table 17 interface Commands: Basic Properties and IP Address Assignment

COMMAND	DESCRIPTION
show interface {*interface_name* | ethernet | vlan | bridge | ppp | virtual ethernet | virtual vlan | virtual bridge | auxiliary | all}	Displays information about the specified interface, specified type of interfaces, or all interfaces.
[no] interface *interface_name*	Creates the specified interface if necessary and enters sub-command mode. The no command deletes the specified interface.
[no] shutdown	Deactivates the specified interface. The no command activates it.
[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] 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.

5.2.1.1 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
```

5.2.2 Interface Parameter Commands

This table lists the commands for Section on page 68.

Table 18 interface Commands: Interface Parameters

COMMAND	DESCRIPTION
`interface` *`interface_name`*	Enters sub-command mode.
`    [no] upstream <0..1048576>`	Specifies the upstream bandwidth for the specified interface. The `no` command sets the upstream bandwidth to 1048576.
`    [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.
`    [no] mtu <576..1500>`	Specifies the Maximum Transmission Unit, which is the maximum number of bytes in each packet moving through this interface. The ZyWALL divides larger packets into smaller fragments. The `no` command resets the MTU to 1500.

5.2.3 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 19 interface Commands: DHCP Settings

COMMAND	DESCRIPTION
`show ip dhcp pool [`*`profile_name`*`]`	Shows information about the specified DHCP pool or about all DHCP pools.
`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. • If you use the `host` command, the ZyWALL treats this DHCP pool as a static DHCP entry. • If you do not use the `host` command and use the `network` command, the ZyWALL treats this DHCP pool as a pool of IP addresses. • If you do not use the `host` command or the `network` command, the DHCP pool is not properly configured and cannot be bound to any interface. The `no` command removes the specified DHCP pool.

Table 19 interface Commands: DHCP Settings (continued)

COMMAND	DESCRIPTION
`show`	Shows information about the specified DHCP pool.
	Use the following commands if you want 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 should assign. Use this command, along with `hardware-address`, to create a static DHCP entry. **Note:** The IP address must be in the same subnet as the interface to which you plan to bind the DHCP pool. When this command is used, the ZyWALL treats this DHCP pool like a static entry, regardless of the `network` setting. The `no` command clears this field.
`[no] hardware-address` *`mac_address`*	Reserves the DHCP pool for the specified MAC address. Use this command, along with `host`, to create a static DHCP entry. The `no` command clears this field.
`[no] client-identifier` *`mac_address`*	Specifies the MAC address that appears in the DHCP client list. The `no` command clears this field.
`[no] client-name` *`host_name`*	Specifies the host name that appears in the DHCP client list. The `no` command clears this field. *host_name*: You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
	Use the following commands if you want to create a pool of IP addresses. These commands have no effect if you use the `host` command. You can still set them, however.

`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] domain-name` *`domain_name`*	Specifies the domain name assigned to DHCP clients. The `no` command clears this field.

Table 19 interface Commands: DHCP Settings (continued)

COMMAND	DESCRIPTION
[no] starting-address *ip* pool-size <1..65535>	Sets the IP start address and maximum pool size of the specified DHCP pool. The final pool size is limited by the subnet mask. **Note:** You must specify the `network number` first, and the start address must be in the same subnet. The `no` command clears the IP start address and maximum pool size.
[no] first-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns}	Sets the first DNS server to the specified IP address or the specified interface's first, second, or third DNS server. The `no` command resets the first DNS server setting to its default value.
[no] second-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns}	Sets the second DNS server to the specified IP address or the specified interface's first, second, or third DNS server. The `no` command resets the second DNS server setting to its default value.
[no] third-dns-server {*ip* | *interface_name* {1st-dns | 2nd-dns | 3rd-dns}	Sets the third DNS server to the specified IP address or the specified interface's first, second, or third DNS server. The `no` command resets the third DNS server setting to its default value.
[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.
renew dhcp *interface-name*	Renews the TCP/IP configuration of the specified interface. The interface must be a DHCP client.
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.

5.2.3.1 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.tw
Router(config-ip-dhcp-pool)#  first-dns-server 172.23.5.1
Router(config-ip-dhcp-pool)#  second-dns-server ge1 1st-dns
Router(config-ip-dhcp-pool)#  third-dns-server 172.23.5.2
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:C6:88
Router(config-ip-dhcp-pool)#  client-identifier 00:0F:20:74:C6:88
Router(config-ip-dhcp-pool)#  client-name TW12210
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
```

5.2.4 Ping Check Commands

This table lists ping check commands

Table 20 interface Commands: Ping Check

COMMAND	DESCRIPTION
show ping-check [*interface_name*]	Displays information about ping check settings for the specified interface or for all interfaces.
interface *interface_name*	Enters sub-command mode.
[no] ping-check activate	Enables ping check for the specified interface. The no command disables ping check for the specified interface.
ping-check {*domain_name* | *ip* | default-gateway}	Specifies what the ZyWALL pings for the ping check; you can specify a fully-qualified domain name, IP address, or the default gateway for the interface.
ping-check {*domain_name* | *ip* | default-gateway} period <5..30>	Specifies what the ZyWALL pings for the ping check and sets the number of seconds between each ping check.
ping-check {*domain_name* | *ip* | default-gateway} timeout <1..10>	Specifies what the ZyWALL pings for the ping check and sets the number of seconds the ZyWALL waits for a response.
ping-check {*domain_name* | *ip* | default-gateway} fail-tolerance <1..10>	Specifies what the ZyWALL pings for the ping check and sets the number of times the ZyWALL times out before it stops routing through the specified interface.

5.2.5 Ethernet Interface Commands

This section identifies commands that support Ethernet interfaces.

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 Ethernet Interface Commands

LABEL	DESCRIPTION
`interface_name`	The name of the interface. ge*x*, *x* = 1 - 5

5.2.5.1 RIP Commands

This table lists the commands for RIP settings.

Table 22 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 Section 8.2 on page 97.
`    [no] ip rip v2-broadcast`	Enables RIP-2 packets using subnet broadcasting. The `no` command uses multi-casting.

5.2.5.2 OSPF Commands

This table lists the commands for OSPF settings.

Table 23 interface Commands: OSPF Settings

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

Table 23 interface Commands: OSPF Settings (continued)

COMMAND	DESCRIPTION
`[no] passive-interface` *`interface_name`*	Sets the OSPF direction of the specified interface to in-only. The `no` command makes OSPF bi-directional in the specified interface.
`interface` *`interface_name`*	Enters sub-command mode.
`[no] ip ospf priority <0..255>`	Sets the priority of the specified interface to the specified value. The `no` command sets the priority to 1.
`[no] ip ospf cost <1..65535>`	Sets the cost of the specified interface to the specified value. 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`	Makes OSPF authentication in the specified interface follow the settings in the corresponding area.
`[no] ip ospf authentication-key` *`password`*	Sets the simple text password for OSPF text authentication in the specified interface. The `no` command clears the text password. *password*: 1-8 alphanumeric characters or underscores
`ip ospf message-digest-key <1..255> md5` *`password`*	Sets the ID and password for OSPF MD5 authentication in the specified interface. *password*: 1-16 alphanumeric characters or underscores
`no ip ospf message-digest-key`	Clears the ID and password for OSPF MD5 authentication in the specified interface.
`[no] ip ospf hello-interval <1..65535>`	Sets the number of seconds between “hello” messages to peer routers. These messages let peer routers know the ZyWALL is available. The `no` command sets the number of seconds to 10. See `ip ospf dead-interval` for more information.
`[no] ip ospf dead-interval <1..65535>`	Sets the number of seconds the ZyWALL waits for “hello” messages from peer routers before it assumes the peer router is not available and deletes associated routing information. The `no` command sets the number of seconds to 40. See `ip ospf hello-interval` for more information.
`[no] ip ospf retransmit-interval <1..65535>`	Sets the number of seconds the ZyWALL waits for an acknowledgment to a link state announcement before it re-sends the link state announcement.

5.2.6 Port Grouping Commands

This section identifies commands that support port grouping.

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

Table 24 port-grouping Commands

COMMAND	DESCRIPTION
`show port-grouping`	Displays which physical ports are assigned to each representative interface.
`port-grouping ge<1..5> port <1..5>`	Adds the specified physical port to the specified representative interface.
`no port <1..5>`	Removes the specified physical port from its current representative interface and adds it to its default representative interface (port *x* --> ge*x*).

5.2.6.1 Port Grouping Command Examples

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

```
Router# configure terminal
Router(config)# show port-grouping
No. Representative Name  Port1 Port2 Port3 Port4 Port5
=========================================================
1   ge1                  yes   no    no    no    no
2   ge2                  no    yes   no    no    no
3   ge3                  no    no    yes   no    no
4   ge4                  no    no    no    yes   no
5   ge5                  no    no    no    no    yes
Router(config)# port-grouping ge1
Router(config-port-grouping)# port 5
Router(config-port-grouping)# exit
Router(config)# show port-grouping
No. Representative Name  Port1 Port2 Port3 Port4 Port5
=========================================================
1   ge1                  yes   no    no    no    yes
2   ge2                  no    yes   no    no    no
3   ge3                  no    no    yes   no    no
4   ge4                  no    no    no    yes   no
5   ge5                  no    no    no    no    no
```

5.2.7 VLAN Interface Commands

This section identifies commands that support VLAN interfaces. VLAN interfaces also use many of the general interface commands discussed at the beginning of Section 5.2 on page 69.

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 VLAN Interface Commands

LABEL	DESCRIPTION
interface_name	VLAN interface: vlan*x*, *x* = 0 - 31 Ethernet interface: ge*x*, *x* = 1 - 5

This table lists the VLAN interface commands.

Table 26 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. *interface_name*: Ethernet interface
`[no] vlan-id <1..4094>`	Specifies the VLAN ID used to identify the VLAN. The `no` command clears the VLAN ID.

5.2.7.1 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
```

5.2.8 Bridge Commands

This section identifies commands that support bridge interfaces. Bridge interfaces also use many of the general interface commands discussed at the beginning of Section 5.2 on page 69.

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 Bridge Interface Commands

LABEL	DESCRIPTION
interface_name	The name of the interface. Ethernet interface: ge*x*, *x* = 1 - 5 VLAN interface: vlan*x*, *x* = 0 - 31 bridge interface: br*x*, *x* = 0 - 11

This table lists the bridge interface commands.

Table 28 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.

5.2.8.1 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
```

5.2.9 PPPoE/PPTP Commands

This section identifies commands that support PPPoE/PPTP interfaces. PPPoE/PPTP interfaces also use many of the general interface commands discussed at the beginning of Section 5.2 on page 69.

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

Table 29 Input Values for PPPoE/PPTP Interface Commands

LABEL	DESCRIPTION
interface_name	The name of the interface. PPPoE/PPTP interface: ppp*x*, *x* = 0 - 11
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 30 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] 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] 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] local-address` *ip*	Specifies a static IP address for the specified PPPoE/PPTP interface. The `no` command makes the PPPoE/PPTP interface a DHCP client; the other computer assigns the IP address.
`[no] remote-address` *ip*	Specifies the IP address of the PPPoE/PPTP server. If the PPPoE/PPTP server is not available at this IP address, no connection is made. The `no` command lets the ZyWALL get the IP address of the PPPoE/PPTP server automatically when it establishes the connection.

5.2.9.1 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
```

5.2.10 Auxiliary Interface Commands

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

Table 31 interface Commands: Auxiliary Interface

COMMAND	DESCRIPTION

`interface dial aux`
`interface disconnect aux`
	Dials or disconnects the auxiliary interface.

`interface aux`	Enters sub-command mode.
`[no] phone-number` *`phone`*	Specifies the phone number of the auxiliary interface. You can use 1-20 numbers, commas (,), or plus signs (+). Use a comma to pause during dialing. Use a plus sign to tell the external modem to make an international call. The `no` command clears the phone number.
`[no] dialing-type {tone | pulse}`	Specifies the dial type of the auxiliary interface. The `no` command sets the dial type to tone.
`[no] port-speed {9600 | 19200 | 38400 | 57600 | 115200}`	Specifies the baud rate of the auxiliary interface. The `no` command sets the baud rate to 115200.

Table 31 interface Commands: Auxiliary Interface (continued)

COMMAND	DESCRIPTION
`[no] initial-string` *`initial_string`*	Specifies the initial string of the auxiliary interface. The `no` command sets the initial string to “ATZ”. *initial_string*: You can use up to 64 characters. Semicolons (;) and backslashes (\) are not allowed.
`[no] dial-timeout <30..120>`	Specifies the number of seconds the auxiliary interface waits for an answer each time it tries to connect. The `no` command disables the timeout.
`[no] idle <0..360>`	Specifies the number of seconds the auxiliary interface waits for activity before it automatically disconnects. The `no` command disables the idle timeout.
`[no] username` *`username`*	Specifies the username of the auxiliary interface. The `no` command clears the username. *username*: You can use alphanumeric, underscores (_), dashes (-), and `/@$` characters, and it can be up to 30 characters long.
`[no] password` *`password`*	Specifies the password of the auxiliary interface. The `no` command clears the password. *password*: You can use up to 63 printable ASCII characters. Spaces are not allowed.
`[no] authentication {chap-pap | chap | pap | mschap | mschap-v2}`	Specifies the authentication type of the auxiliary interface. The `no` command sets the authentication to chap-pap.
`[no] description` *`description`*	Specifies the description for the auxiliary interface. The `no` command clears the description. *description*: You can use alphanumeric and `()+/ :=?!*#@$_%-` characters, and it can be up to 60 characters long.
`[no] shutdown`	Activates the auxiliary interface. The `no` command deactivates it.

5.2.10.1 Auxiliary Interface Command Examples

The following commands show you how to set up the auxiliary interface aux with the following parameters: phone-number 0340508888, tone dialing, port speed 115200, initial-string ATZ, timeout 10 seconds, retry count 2, retry interval 100 seconds, username **kk**, password kk@u2online, chap-pap authentication, and description “I am aux interface”.

```
Router# configure terminal
Router(config)# interface aux
Router(config-if-aux)# phone-number 0340508888
Router(config-if-aux)# dialing-type tone
Router(config-if-aux)# port-speed 115200
Router(config-if-aux)# initial-string ATZ
Router(config-if-aux)# timeout 10
Router(config-if-aux)# retry-count 2
Router(config-if-aux)# retry-interval 100
Router(config-if-aux)# username kk
Router(config-if-aux)# password kk@u2online
Router(config-if-aux)# authentication chap-pap
Router(config-if-aux)# description I am aux interface
Router(config-if-aux)# exit
```

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

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

5.2.11 Virtual Interface Commands

Virtual interfaces use many of the general interface commands discussed at the beginning of Section 5.2 on page 69. There are no additional commands for virtual interfaces.

5.2.11.1 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
```

CHAPTER 6
Trunks

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

6.1 Trunks Overview

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

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

6.2 Trunk Scenario Examples

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

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

6.3 Trunk Commands Input Values

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

Table 32 interface-group Command Input Values

LABEL	DESCRIPTION
group_name	A descriptive name for the trunk. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.
interface	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: gex, *x* = 1 - 5 ppp interface: pppx, x = 0-11 VLAN interface: vlan*x*, *x* = 0 - 31 bridge interface: br*x*, *x* = 0 - 11
<cr>	Carriage Return (the “enter” key).

6.4 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 32 on page 86 for details about the values you can input with these commands.

Table 33 interface-group Commands Summary

COMMAND	DESCRIPTION
`show interface-group {`*group_name*`}`	Displays a 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.
`[no] interface {`*num*` | append | insert `*num*`} `*interface*` {<cr> | weight <1..10> | limit <1..1048576> | 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. The `no` command removes an interface from a trunk.
`mode {normal | trunk}`	Sets the mode for a trunk. Do this first in the trunk’s sub-command mode.
`algorithm {wrr | llf | spill-over}`	Sets the trunk’s load balancing algorithm.
`move <1..8> to <1..8>`	Changes a the interface order in a trunk.
`flush`	Deletes a trunk’s interface settings.

6.5 Trunk Command Examples

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

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

The following example creates a least load first trunk for Ethernet interface ge3 and VLAN 5. The ZyWALL sends new session traffic through the least utilized of these interfaces.

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

The following example creates a spill-over trunk for Ethernet interfaces ge1 and ge3. The ZyWALL sends traffic through ge1 until it hits the limit of 1000 kbps. The ZyWALL sends anything over 1000 kbps through ge3.

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

CHAPTER 7
IPSec VPN

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

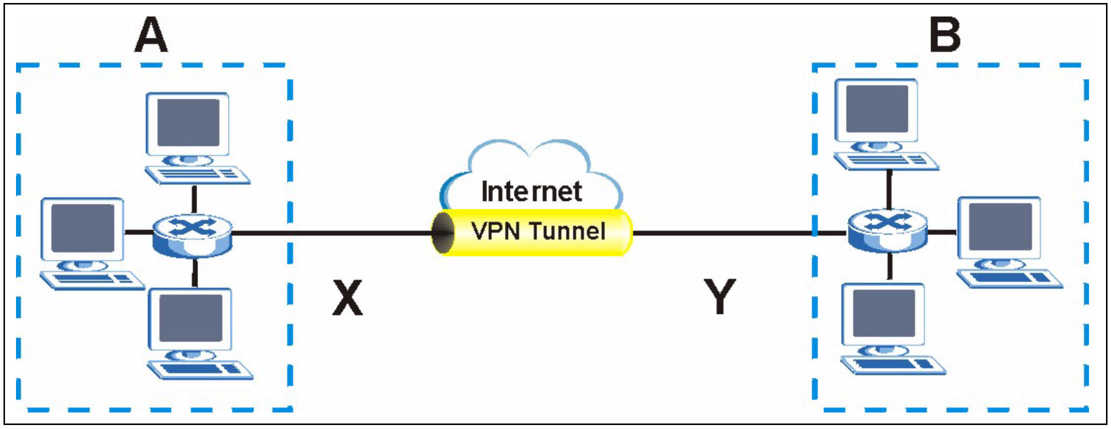
7.1 IPSec VPN Overview

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.

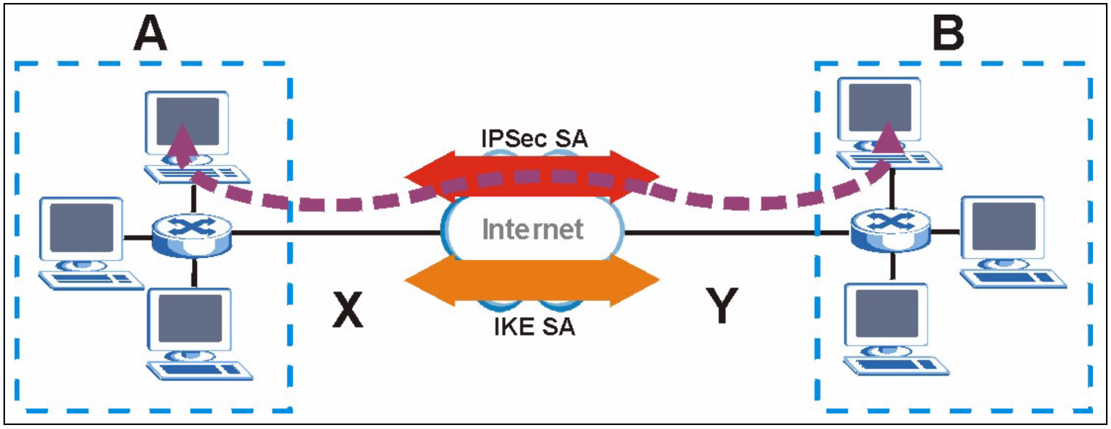
Figure 24 VPN: Example



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

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the ZyWALL and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the ZyWALL and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the ZyWALL and remote IPSec router can send data between computers on the local network and remote network. This is illustrated in the following figure.

Figure 25 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.

7.2 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 34 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 up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.

The following sections list the IPSec VPN commands.

7.2.1 IKE SA Commands

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

Table 35 isakmp Commands: IKE SAs

COMMAND	DESCRIPTION
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.
isakmp policy rename *policy_name policy_name*	Renames the specified IKE SA (first *policy_name*) to the specified name (second *policy_name*).
isakmp policy *policy_name*	
activate deactivate	Activates or deactivates the specified IKE SA.
mode {main | aggressive}	Sets the negotiating mode.
transform-set *isakmp-algo* [*isakmp_algo* [*isakmp_algo*]]	Sets the encryption and authentication algorithms for each proposal. *isakmp_algo*: {des-md5 | des-sha | 3des-md5 | 3des-sha | aes128-md5 | aes128-sha | aes192-md5 | aes192-sha | aes256-md5 | aes256-sha}
lifetime <180..3000000>	Sets the IKE SA life time to the specified value.
group1 group2 group5	Sets the DH*x* group to the specified group.
[no] natt	Enables NAT traversal. The no command disables NAT traversal.
[no] dpd	Enables Dead Peer Detection (DPD). The no command disables DPD.
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).
authentication {pre-share | rsa-sig}	Specifies whether to use a pre-shared key or a certificate for authentication.
keystring *pre_shared_key*	Sets the pre-shared key that can be used for authentication. *pre_shared_key*: You can use 8-31 alphanumeric or 16-62 hexadecimal characters. Hexadecimal keys should be preceded by “0x”. The pre-shared key is case-sensitive.
certificate *certificate-name*	Sets the certificate that can be used for authentication.

Table 35 isakmp Commands: IKE SAs (continued)

COMMAND	DESCRIPTION
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. *e_mail*: You can use up to 63 alphanumeric characters, underscores (_), dashes (-), or @ characters. *distinguished_name*: You can use up to 511 alphanumeric, characters, spaces, or .@=,_- characters.
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. *e_mail*: You can use up to 63 alphanumeric characters, underscores (_), dashes (-), or @ characters. *distinguished_name*: You can use up to 511 alphanumeric, characters, spaces, or .@=,_- characters.
[no] xauth type {server *xauth_method* | client name *username* password *password*}	Enables extended authentication and specifies whether the ZyWALL is the server or client. If the ZyWALL is the server, it also specifies the extended authentication method (aaa authentication *profile_name*); if the ZyWALL is the client, it also specifies the username and password to provide to the remote IPSec router. The no command disables extended authentication. *username*: You can use alphanumeric characters, underscores (_), and dashes (-), and it can be up to 31 characters long. *password*: You can use most printable ASCII characters. You cannot use square brackets [ ], double quotation marks ("), question marks (?), tabs or spaces. It can be up to 31 characters long.

7.2.2 IPSec SA Commands (except Manual Keys)

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

Table 36 crypto map Commands: IPSec SAs

COMMAND	DESCRIPTION
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*).

Table 36 crypto map Commands: IPSec SAs (continued)

COMMAND	DESCRIPTION
`crypto map` *map_name*	
`activate` `deactivate`	Activates or deactivates the specified IPSec SA.
`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` *esp_crypto_algo* [*esp_crypto_algo* [*esp_crypto_algo*]]	Sets the active protocol to ESP and sets the encryption and authentication algorithms for each proposal. *esp_crypto_algo*: {esp-3des-md5 | esp-3des-sha | esp-aes128-md5 | esp-aes128-sha | esp-aes192-md5 | esp-aes192-sha | esp-aes256-md5 | esp-aes256-sha | esp-des-md5 | esp-des-sha | esp-null-md5 | esp-null-sha}
`transform-set {ah-md5 | ah-sha} [{ah-md5 | ah-sha} [{ah-md5 | ah-sha}]]`	Sets the active protocol to AH and sets the encryption and authentication algorithms for each proposal.
`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.

Table 36 crypto map Commands: IPSec SAs (continued)

COMMAND	DESCRIPTION
`[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-num*) to the specified location (second *rule-num*) for in-bound traffic DNAT.
`in-dnat append protocol {all | tcp | udp} original-ip` *`address_name`* `<0..65535> <0..65535> mapped-ip` *`address_name`* `<0..65535> <0..65535>`	Maps the specified IP address and port range (original-ip) to the specified IP address and port range (mapped-ip) and appends this rule to the end of the rule list for in-bound traffic DNAT.
`in-dnat insert <1..10> protocol {all | tcp | udp} original-ip` *`address_name`* `<0..65535> <0..65535> mapped-ip` *`address_name`* `<0..65535> <0..65535>`	Maps the specified IP address and port range (original-ip) to the specified IP address and port range (mapped-ip) and inserts this rule before the specified rule.
`in-dnat <1..10> protocol {all | tcp | udp} original-ip` *`address_name`* `<0..65535> <0..65535> mapped-ip` *`address_name`* `<0..65535> <0..65535>`	Creates or revises the specified rule and maps the specified IP address and port range (original-ip) to the specified IP address and port range (mapped-ip).

7.2.3 IPSec SA Commands (for Manual Keys)

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

Table 37 crypto map Commands: IPSec SAs (Manual Keys)

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

7.2.4 VPN Concentrator Commands

This table lists the commands for the VPN concentrator.

Table 38 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.
`    [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*).

7.2.5 SA Monitor Commands

This table lists the commands for the SA monitor.

Table 39 sa Commands: SA Monitor

COMMAND	DESCRIPTION
`show sa monitor`	Displays current IPSec SA and the status of each one.
`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.

CHAPTER 8
Routing Protocol

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

8.1 Routing Protocol Overview

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

The ZyWALL supports two standards, RIP and OSPF, for routing protocols. RIP and OSPF are compared in Table 40 on page 97, and they are discussed further in the next two sections.

Table 40 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

8.2 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 41 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.

8.2.1 RIP Commands

This table lists the commands for RIP.

Table 42 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”.

8.2.2 General OSPF Commands

This table lists the commands for general OSPF configuration.

Table 43 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.

Table 43 router Commands: General OSPF Configuration (continued)

COMMAND	DESCRIPTION
`    [no] passive-interface interface_name`	Sets the direction to "In-Only" for the specified interface. The `no` command sets the direction to "BiDir".
`    [no] router-id ip`	Sets the 32-bit ID (in IP address format) of the ZyWALL. The `no` command resets it to "default", or the highest available IP address.

8.2.3 OSPF Area Commands

This table lists the commands for OSPF areas.

Table 44 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.

8.2.4 Virtual Link Commands

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

Table 45 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.

Table 45 router Commands: Virtual Links in OSPF Areas (continued)

COMMAND	DESCRIPTION
`[no] area ip virtual-link ip authentication`	Enables text authentication in the specified virtual link. The `no` command disables authentication in the specified virtual link.
`[no] area ip virtual-link ip authentication message-digest`	Enables MD5 authentication in the specified virtual link. The `no` command disables authentication in the specified virtual link.
`[no] area ip virtual-link ip authentication authentication-key authkey`	Sets the password for text authentication in the specified virtual link. The `no` command clears the password in the specified virtual link.
`[no] area ip virtual-link ip authentication message-digest-key <1..255> md5 authkey`	Sets the MD5 ID and password for MD5 authentication in the specified virtual link. The `no` command clears the MD5 ID and password in the specified virtual link.
`[no] area ip virtual-link ip authentication same-as-area`	Sets the virtual link's authentication method to the area's default authentication.
`[no] area ip virtual-link ip authentication-key authkey`	Sets the password for text authentication in the specified virtual link. The `no` command clears the password.
`area ip virtual-link ip message-digest-key <1..255> md5 authkey`	Sets the MD5 ID and password for MD5 authentication in the specified virtual link.
`no area ip virtual-link ip message-digest-key <1..255>`	Clears the MD5 ID in the specified virtual link.

8.2.5 Learned Routing Information Commands

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

Table 46 ip route Commands: Learned Routing Information

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

CHAPTER 9
Zones

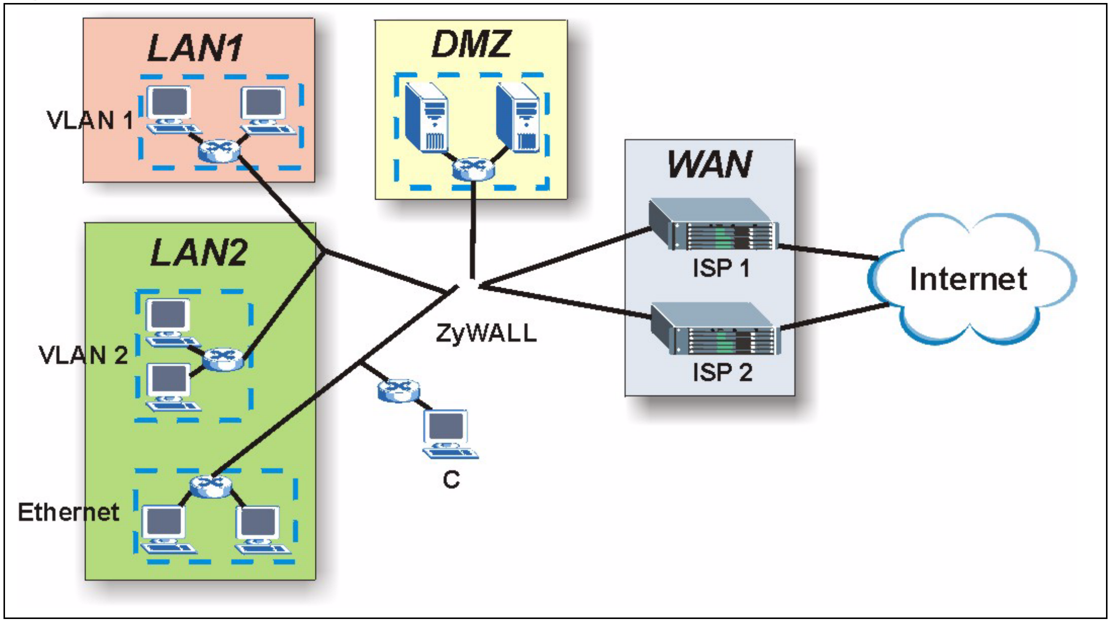
Set up zones to configure network security and network policies in the ZyWALL.

9.1 Zones Overview

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

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

Figure 26 Example: Zones



9.2 Zone Commands Summary

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

Table 47 Input Values for Zone Commands

LABEL	DESCRIPTION
profile_name	The name of the zone, or the name of the VPN tunnel. 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 zone commands.

Table 48 zone Commands

COMMAND	DESCRIPTION
`show zone [`*profile_name*`]`	Displays information about the specified zone or about all zones.
`[no] zone` *profile_name*	Creates the zone if necessary and enters sub-command mode. The `no` command deletes the zone.
`zone` *profile_name*	
`    [no] block`	Blocks intra-zone traffic. The `no` command allows intra-zone traffic.
`    [no] interface` *interface_name*	Adds the specified interface to the specified zone. The `no` command removes the specified interface from the specified zone. See Section 5.2 on page 69 for information about interface names.
`    [no] crypto` *profile_name*	Adds the specified VPN tunnel to the specified zone. The `no` command removes the specified VPN tunnel from the specified zone.

9.2.1 Zone Command Examples

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

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

CHAPTER 10
Device HA

Use device HA and Virtual Router Redundancy Protocol (VRRP) to increase network reliability.

10.1 Device HA Overview

This section provides an overview of VRRP, VRRP groups, and synchronization.

10.1.1 Virtual Router Redundancy Protocol (VRRP) Overview

Every computer on a network may send packets to a default gateway, which can become a single point of failure. Virtual Router Redundancy Protocol (VRRP), allows you to create redundant backup gateways to ensure that the default gateway is always available.

Note: The ZyWALL 1050 runs VRRP v2. You can only set up device HA with other ZyWALL 1050s running the same firmware version.

10.1.2 VRRP Group Overview

In the ZyWALL, you should create a VRRP group to add one of its interfaces to a virtual router. You can add any Ethernet interface, VLAN interface, or virtual interface (created on top of Ethernet interfaces or VLAN interfaces) with a static IP address. You can only enable one VRRP group for each interface, and you can only have one active VRRP group for each virtual router.

10.1.3 Synchronization Overview

In a virtual router, backup routers do not automatically get configuration updates from the master router. In this case, the master ZyWALL router can send backup ZyWALL routers these updates. This is called synchronization.

10.2 Device HA Commands Summary

The following table identify the values required for many `device-ha` commands. Other input values are discussed with the corresponding commands.

Table 49 Input Values for device-ha Commands

LABEL	DESCRIPTION
vrrp_group_name	The name of the VRRP group. The name can consist of alphanumeric characters, the underscore, and the dash and may be up to fifteen alphanumeric characters long.

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

10.2.1 VRRP Group Commands

The first table lists the commands for VRRP groups.

Table 50 device-ha Commands: VRRP Groups

COMMAND	DESCRIPTION
`show device-ha vrrp-group`	Displays information about all VRRP groups.
`show device-ha status`	Displays the status of active VRRP groups.
`[no] device-ha vrrp-group` *vrrp_group_name*	Creates the specified VRRP group if necessary and enters sub-command mode. The `no` command deletes the specified VRRP group.
`    [no] vrid <1..254>`	Sets the specified VRRP group's ID to the specified VR ID. The `no` command clears the VR ID.
`    [no] interface` *interface_name*	Specifies the interface that is part of the specified VRRP group. The `no` command removes the specified interface from the specified VRRP group.
`    [no] role {master | backup}`	Specifies the role of the specified VRRP group in the virtual router. The `no` command clears the role, which makes the configuration incomplete.
`    [no] priority <1..254>`	Sets the priority of the specified VRRP group in the virtual router. The `no` command resets the priority to 100.
`    [no] preempt`	Lets the ZyWALL preempt lower-priority routers in the virtual router. The `no` command prevents the ZyWALL from preempting lower-priority routers.
`    [no] manage-ip` *ip*	Specifies the IP address of the specified VRRP group when it is not the master. The `no` command clears the IP address.

Table 50 device-ha Commands: VRRP Groups (continued)

COMMAND	DESCRIPTION
`[no] authentication {string` *`password`* `| ah-md5` *`password`*`}`	Specifies the authentication method and password for the specified VRRP group. The `no` command means that the specified VRRP group does not use authentication. *password*: You may use alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ ()), and it can be up to eight characters long.
`[no] description` *`description`*	Specifies the description for the specified VRRP group. The `no` command clears the description. *description*: You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
`[no] activate`	Turns on the specified VRRP group. The `no` command turns off the VRRP group.

10.2.2 Synchronization Commands

This table lists the commands for synchronization. You can synchronize with other ZyWALL 1050 that are running the same firmware version.

Table 51 device-ha Commands: Synchronization

COMMAND	DESCRIPTION
`show device-ha sync`	Displays the current settings for synchronization.
`show device-ha sync status`	Displays the current status of synchronization.
`[no] device-ha sync from {`*`hostname`* `|` *`ip`*`}`	Specifies the fully-qualified domain name (FQDN) or IP address of the ZyWALL router. Usually, this is the IP address or FQDN of the virtual router. The `no` command clears this field. *hostname*: You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.
`[no] device-ha sync port <1..65535>`	Specifies the port number to use to synchronize with the specified ZyWALL router. The `no` command resets the port to 21.
`[no] device-ha sync authentication password` *`password`*	Specifies the password to use when synchronizing. Every router in the virtual router should use the same password. The `no` command resets the password to “1234”. *password*: You can use 4-63 alphanumeric characters, underscores (_), dashes (-), and `#%^*={}:,.~` characters.
`[no] device-ha sync auto`	Specifies whether or not to automatically synchronize at regular intervals.

Table 51 device-ha Commands: Synchronization (continued)

COMMAND	DESCRIPTION
`[no] device-ha sync interval <1..1440>`	Specifies the number of minutes between each synchronization if the ZyWALL automatically synchronizes with the specified ZyWALL router. The `no` command resets the interval to five minutes.
`[no] device-ha sync now`	Synchronize now.

10.2.3 Device HA Command Examples

The following commands show you how to set up VRRP group A1 with the following characteristics: VR ID 150, backup router, ge1 interface, priority 100, enable preempt, manage IP 192.168.1.0/24, simple authentication, password “abc123”, and description "vrrp-group A1". Then, the commands set up synchronization and synchronize immediately.

```
Router# configure terminal
Router(config)# device-ha vrrp-group A1
Router(config-device-ha)# vrid 150
Router(config-device-ha)# interface ge1
Router(config-device-ha)# role backup
Router(config-device-ha)# priority 100
Router(config-device-ha)# preempt
Router(config-device-ha)# manage-ip 192.168.1.0/24
Router(config-device-ha)# authentication string abc123
Router(config-device-ha)# description "vrrp-group A1"
Router(config-device-ha)# exit
Router(config)# device-ha sync from 192.168.1.1
Router(config)# device-ha sync port 21
Router(config)# device-ha sync authentication password 1234
Router(config)# device-ha sync now
```

CHAPTER 11
ISP Accounts

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

11.1 ISP Accounts Overview

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

11.2 ISP Account Commands Summary

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

Table 52 Input Values for ISP Account Commands

LABEL	DESCRIPTION
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.

The following table lists the ISP account commands.

Table 53 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.
`[no] user` *`username`*	Sets the username for the specified ISP account. The `no` command clears the username. *username*: You can use alphanumeric, underscores (_), dashes (-), and `/@$` characters, and it can be up to 30 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.

Table 53 account Commands (continued)

COMMAND	DESCRIPTION
`[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 {on | off}`	Turns compression on or off for the specified ISP account. The `no` command turns off compression.
`[no] idle <0..360>`	Sets the idle timeout for the specified ISP account. The `no` command sets the idle timeout to zero.
`[no] service-name {`*`ip`*` | `*`hostname`*` | `*`service_name`*`}`	Sets the service name for the specified PPPoE ISP account. The `no` command clears the service name. *hostname*: You may up to 63 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period. *service_name*: You can use 1-253 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 (:).

CHAPTER 12 DDNS

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

12.1 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: If you have a private WAN IP address, then you cannot use Dynamic DNS.

Before you can use Dynamic DNS services with the ZyWALL, you first need to set up a dynamic DNS account with www.dyndns.org. (This is the only DNS service provider the ZyWALL supports at the time of writing.) DynDNS offers several DNS services. Please see www. dyndns.org for more information about each of them. When registration is complete, DynDNS gives you a password or key.

Note: You must go to DynDNS's Web site to set up a user account and a domain name before you can use the Dynamic DNS service with the ZyWALL.

After this, you configure the ZyWALL. Once the ZyWALL is configured, it automatically sends updated IP addresses to DynDNS, which helps redirect traffic accordingly.

12.2 DDNS Commands Summary

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

Table 54 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 55 ip ddns Commands

COMMAND	DESCRIPTION
`show ddns [profile_name]`	Displays information about the specified DDNS profile or about all DDNS profiles.
`[no] ip ddns profile profile_name`	Creates the specified DDNS profile if necessary and enters sub-command mode. The `no` command deletes it.
`[no] service-type {dyndns | dyndns_static | dyndns_custom}`	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] custom ip`	Sets the static IP address in the specified DDNS profile. The `no` command clears it.
`[no] mx {ip | domain_name}`	Enables the mail exchanger and sets the fully-qualified domain name of the mail server to which mail from this domain name is forwarded. The `no` command disables the mail exchanger. *domain_name*: You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character must be alphanumeric.
`[no] wan-iface interface_name`	Sets the WAN interface in the specified DDNS profile. The `no` command clears it.
`[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.

CHAPTER 13 Route

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

13.1 Policy Route

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

13.2 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 56 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.
interface_name	The name of the interface. Ethernet interface: gex, *x* = 1 - 5 virtual interface on top of Ethernet interface: gex:*y*, *x* = 1 - 5, *y* = 1 - 12 VLAN interface: vlanx, *x* = 0 - 15 virtual interface on top of VLAN interface: vlanx:*y*, *x* = 0 - 15, *y* = 1 - 12 bridge interface: brx, *x* = 0 - 11 virtual interface on top of bridge interface: brx:*y*, *x* = 0 - 11, *y* = 1 - 12 PPPoE/PPTP interface: pppx, *x* = 0 - 11
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.

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 57 Command Summary: Policy Route

COMMAND	DESCRIPTION
policy {<1..5000>|append<1..5000>|insert<1..5000>}	Enters the policy-route sub-command mode to configure, add or insert a policy.
[no] bandwidth <1..1048576> priority <1..1024>	Sets the maximum bandwidth and priority for the policy. The no command removes bandwidth settings from the rule.
[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] interface *interface_name*	Sets the interface on which the incoming packets are received. The no command resets the incoming interface to the default (any). any means all interfaces.
[no] next-hop {auto|gateway *address object* |interface *interface_name* |trunk *trunk_name*|tunnel *tunnel_name*}	Sets the next-hop to which the matched packets are routed. The no command resets next-hop settings to the default (auto).
[no] schedule *schedule_object*	Sets the schedule. The no command removes the schedule setting to the default (none). none means any time.
[no] service {*service_name*|any}	Sets the IP protocol. The no command resets service settings to the default (any). any means all services.
[no] snat {outgoing-interface|pool {*address_object*}}	Sets the source IP address of the matched packets that use SNAT. The no command removes source NAT settings from the rule.
[no] source {*address_object*|any}	Sets the source IP address that the matched packets must have. The no command resets the source IP address to the default (any). any means all IP addresses.
[no] trigger <1..8> incoming *service_name* trigger *service_name*	Sets a port triggering rule. The no command removes port trigger settings from the rule.
trigger append incoming *service_name* trigger *service_name*	Adds a new port triggering rule to the end of the list.
trigger delete <1..8>	Removes a port triggering rule.
trigger insert <1..8> incoming *service_name* trigger *service_name*	Adds a new port triggering rule before the specified number.
trigger move <1..8> to <1..8>	Moves a port triggering rule to the number that you specified.

Table 57 Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
`[no] tunnel` *`tunnel_name`*	Sets the incoming interface to a VPN tunnel. The `no` command removes the 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.
`policy default-route`	Enters the policy-route sub-command mode to set a route with the name "default-route".
`policy delete <1..5000>`	Removes a routing policy.
`policy flush`	Clears the policy routing table.
`policy move <1..5000> to <1..5000>`	Move a routing policy to the number that you specified.
`show policy-route [1..5000]`	Displays all or specified policy route settings.

13.2.1 Policy Route Command Example

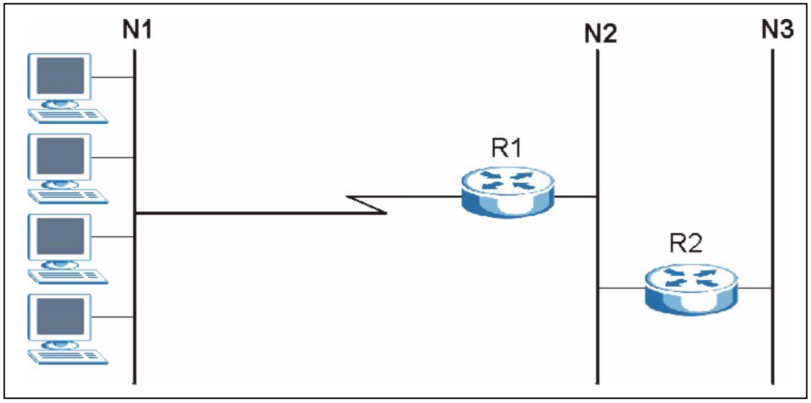
The following commands set a policy that routes the packets (with the source IP address TW_SUBNET and any destination IP address) through the interface ge1 to the next-hop router GW_1. This route uses the IP address of the outgoing interface as the matched packets' source IP address.

```
Router(config)# policy 1
Router(policy-route)# description example
Router(policy-route)# destination any
Router(policy-route)# interface ge1
Router(policy-route)# next-hop gateway GW_1
Router(policy-route)# snat outgoing-interface
Router(policy-route)# source TW_SUBNET
Router(policy-route)# exit
Router(config)# show policy-route 1
index: 1
  active: yes
  description: example
  user: any
  schedule: none
  interface: ge1
  tunnel: none
  source: TW_SUBNET
  destination: any
  service: any
  nexthop type: Gateway
  nexthop: GW_1
  bandwidth: 0
  bandwidth priority: 0
  SNAT: outgoing-interface
  amount of port trigger: 0
Router(config)#
```

13.3 IP Static Route

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

Figure 27 Example of Static Routing Topology



13.4 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.

Table 58 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 disables 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.

13.4.1 Static Route Commands Example

The following command sets a static route with IP address 10.10.10.1 and subnet mask 255.255.255.0 and with the next-hop interface ge1.

```
Router(config)# ip route 10.10.10.1 255.255.255.0 ge1
```

CHAPTER 14 Firewall

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

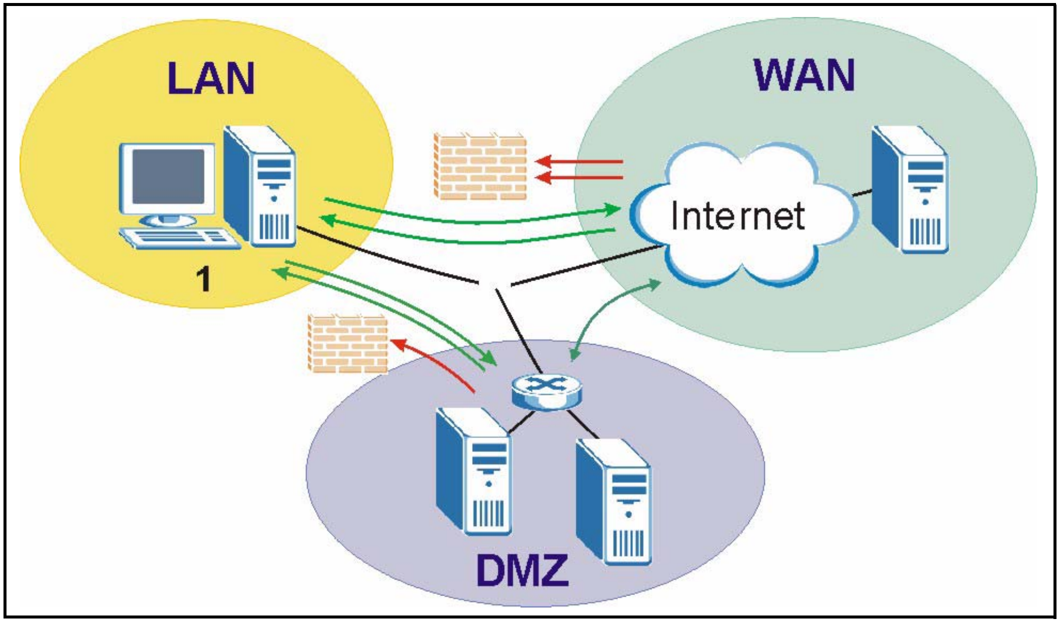
14.1 Firewall Overview

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

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

The following figure shows the ZyWALL's default firewall rules in action as well as demonstrates how stateful inspection works. User **1** can initiate a Telnet session from within the LAN zone and responses to this request are allowed. However, other Telnet traffic initiated from the WAN or DMZ zone and destined for the LAN zone is blocked. Communications between the WAN and the DMZ zones are allowed. The firewall allows VPN traffic between any of the networks.

Figure 28 Default Firewall Action



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

For example, if you want to allow a specific user from any computer to access one zone by logging in to the ZyWALL, you can set up a rule based on the user name only. If you also apply a schedule to the firewall rule, the user can only access the network at the scheduled time. A user-aware firewall rule is activated whenever the user logs in to the ZyWALL and will be disabled after the user logs out of the ZyWALL.

14.2 Firewall Commands

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

Table 59 Input Values for General Firewall 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.
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. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
schedule_object	The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
service_name	The name of the service (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

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

Table 60 Command Summary: Firewall

COMMAND	DESCRIPTION
`[no] connlimit max-per-host <1..8192>`	Sets he highest number of sessions that the ZyWALL will permit a host to have at one time. The `no` command removes the settings.
`firewall <1..5000>`	Enters the firewall sub-command mode to set a firewall rule. `<1..5000>`: the priority number of a firewall rule.
`action <allow|deny|reject>`	Sets the action the ZyWALL takes when packets match this rule.
`[no] activate`	Enables a firewall rule. The `no` command disables the firewall rule.
`[no] description` *`description`*	Sets a descriptive name (up to 60 printable ASCII characters) for a firewall rule. The `no` command removes the descriptive name from the rule.
`[no] destinationip` *`address_object`*	Sets the destination IP address. The `no` command resets the destination IP address(es) to the default (`any`). `any` means all IP addresses.
`exit`	Quits the firewall sub-command mode.
`[no] from` *`zone_object`*	Sets the zone on which the packets are received. The `no` command removes the zone on which the packets are received and resets it to the default (`any`). `any` means all interfaces or VPN tunnels.
`[no] log [alert]`	Sets the ZyWALL to create a log (and optionally an alert) when packets match this rule. The `no` command sets the ZyWALL not to create a log or alert when packets match this rule.
`[no] schedule` *`schedule_object`*	Sets the schedule that the rule uses. The `no` command removes the schedule settings from the rule.
`[no] service` *`service_name`*	Sets the service to which the rule applies. The `no` command resets the service settings to the default (`any`). `any` means all services.
`[no] sourceip` *`address_object`*	Sets the source IP address(es). The `no` command resets the source IP address(es) to the default (`any`). `any` means all IP addresses.
`[no] sourceport {tcp|udp} {eq <1..65535>|range <1..65535> <1..65535>}`	Sets the source port for a firewall rule. The `no` command removes the source port from the rule.

Table 60 Command Summary: Firewall (continued)

COMMAND	DESCRIPTION
`[no] to {zone_object|ZyWALL}`	Sets the zone to which the packets are sent. The `no` command removes the zone to which the packets are sent and resets it to the default (`any`). `any` means all interfaces or VPN tunnels.
`[no] user user_name`	Sets a user-aware firewall rule. The rule is activated only when the specified user logs into the system. The `no` command resets the user name to the default (`any`). `any` means all users.
`firewall zone_object {zone_object|ZyWALL} <1..5000>`	Enters the firewall sub-command mode to set a direction specific through-ZyWALL rule or to-ZyWALL rule. `<1..5000>`: the index number in a direction specific firewall rule list.
`firewall zone_object {zone_object|ZyWALL} append`	Enters the firewall sub-command mode to add a direction specific through-ZyWALL rule or to-ZyWALL rule to the end of the global rule list.
`firewall zone_object {zone_object|ZyWALL} delete <1..5000>`	Removes a direction specific through-ZyWALL rule or to-ZyWALL rule. `<1..5000>`: the index number in a direction specific firewall rule list.
`firewall zone_object {zone_object|ZyWALL} flush`	Removes all direction specific through-ZyWALL rule or to-ZyWALL rules.
`firewall zone_object {zone_object|ZyWALL} insert <1..5000>`	Enters the firewall sub-command mode to add a direction specific through-ZyWALL rule or to-ZyWALL rule before the specified rule number. `<1..5000>`: the index number in a direction specific firewall rule list.
`firewall zone_object {zone_object|ZyWALL} move <1..5000> to <1..5000>`	Moves a direction specific through-ZyWALL rule or to-ZyWALL rule to the number that you specified. `<1..5000>`: the index number in a direction specific firewall rule list.
`[no] firewall activate`	Enables the firewall on the ZyWALL. The `no` command disables the firewall.
`firewall append`	Enters the firewall sub-command mode to add a global firewall rule to the end of the global rule list.
`firewall delete <1..5000>`	Removes a firewall rule. `<1..5000>`: the priority number of a firewall rule.
`firewall flush`	Removes all firewall rules.
`firewall insert <1..5000>`	Enters the firewall sub-command mode to add a firewall rule before the specified rule number. `<1..5000>`: the priority number of a firewall rule.

Table 60 Command Summary: Firewall (continued)

COMMAND	DESCRIPTION
`firewall move <1..5000> to <1..5000>`	Moves a firewall rule to the number that you specified. `<1..5000>`: the priority number of a firewall rule.
`show connlimit max-per-host`	Displays the highest number of sessions that the ZyWALL will permit a host to have at one time.
`show firewall`	Displays all firewall settings.
`show firewall <1..5000>`	Displays a firewall rule's settings. `<1..5000>`: the priority number of a firewall rule.
`show firewall` *`zone_object`* `{`*`zone_object`*`|`*`ZyWALL`*`}`	Displays all firewall rules settings for the specified packet direction.
`show firewall` *`zone_object`* `{`*`zone_object`*`|`*`ZyWALL`*`} <1..5000>`	Displays a specified firewall rule's settings for the specified packet direction. `<1..5000>`: the index number in a direction specific firewall rule list.
`show firewall status`	Displays whether the firewall is active or not.

14.2.1 Firewall Command Examples

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

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

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

The following command displays the firewall rule(s) (including the default firewall rule) that applies to the packet direction from WAN to LAN. The firewall rule numbers in the menu are the firewall rules’ priority numbers in the global rule list.

```
Router# configure terminal
Router(config)# show firewall WAN LAN
firewall rule: 3
  description:
  user: any, schedule: none
  from: WAN, to: LAN
  source IP: any, source port: any
  destination IP: Dest_1, service: MyService
  log: no, action: allow, status: yes
firewall rule: 4
  description:
  user: any, schedule: none
  from: WAN, to: LAN
  source IP: any, source port: any
  destination IP: any, service: any
  log: log, action: deny, status: yes

Router(config)# show firewall WAN LAN 2
firewall rule: 4
  description:
  user: any, schedule: none
  from: WAN, to: LAN
  source IP: any, source port: any
  destination IP: any, service: any
  log: no, action: deny, status: yes
Router(config)#
```

CHAPTER 15 Application Patrol

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

15.1 Application Patrol Overview

Application patrol provides a convenient way to manage instant messenger (IM) and peer-to-peer (P2P) application use on the network. It can also be used to manage a few general protocols (for example, http and ftp), as well as the streaming protocol rtsp.

Note: The ZyWALL checks firewall rules before it checks application patrol rules for traffic going through the ZyWALL.

If you want to use a service, make sure both the firewall and application patrol allow the service's packets to go through the ZyWALL.

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

15.2 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 61 Input Values for Application Patrol Commands

LABEL	DESCRIPTION

protocol_name	The name of a pre-defined application. These are listed by category.
	`general`: `ftp` | `smtp` | `pop3` | `irc` | `http`
	`im`: `msn` | `aol-icq` | `yahoo` | `qq`
	`p2p`: `bittorrent` | `eDonkey` | `fasttrack` | `gnutella` | `napster` | `h323` | `sip` | `soulseek`
	`stream`: `rtsp`

The following sections list the application patrol commands.

15.2.1 Pre-defined Application Commands

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

Table 62 app Commands: Pre-Defined Applications

COMMAND	DESCRIPTION
`app` *`protocol_name`* `{forward | drop | reject}`	Specifies what action the ZyWALL should take when it identifies this application.
`[no] app` *`protocol_name`* `activate`	Enables application patrol for the specified application. The `no` command disables application patrol for the specified application.
`app` *`protocol_name`* `mode {portless | portbase}`	Specifies how the ZyWALL identifies this application.
`[no] app` *`protocol_name`* `log [alert]`	Creates log entries (and alerts) for the specified application. The `no` command does not create any log entries.
`[no] app` *`protocol_name`* `bwm`	Turns on bandwidth management for the specified application. The `no` command turns off bandwidth management for the specified application.
`app` *`protocol_name`* `bandwidth <0..102400>`	Specifies the bandwidth limit (in kilobits per second) for the specified application.
`[no] app` *`protocol_name`* `defaultport <1..65535>`	For port-base applications. Adds the specified port to the list of ports used to identify the specified application. This port number can only be included in one application's list. The `no` command removes the specified port from the list.
`[no] app` *`protocol_name`* `allowport <1..65535>`	If the default action is drop or reject. Adds the specified port to the list of ports that are forwarded in spite of the default action. The `no` command removes the specified port from the list.

15.2.2 Exception Commands for Pre-defined Applications

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

Table 63 app Commands: Exceptions in Pre-Defined Applications

COMMAND	DESCRIPTION
`app` *`protocol_name`* `{forward | drop | reject} exception {forward | drop | reject}`	Specifies the action when the exception occurs.
`app` *`protocol_name`* `exception insert <1..64>`	Creates a new rule at the specified row and enters sub-command mode.
`app` *`protocol_name`* `exception append`	Creates a new rule, appends it to the end of the list, and enters sub-command mode.
`    [no] schedule` *`profile_name`*	Adds the specified schedule to the specified exception to the specified application.
`    [no] user` *`username`*	Adds the specified user to the specified exception to the specified application.

Table 63 app Commands: Exceptions in Pre-Defined Applications (continued)

COMMAND	DESCRIPTION
`    [no] source profile_name`	Adds the specified source address to the specified exception to the specified application.
`    [no] destination profile_name`	Adds the specified destination address to the specified exception to the specified application.
`    [no] log [alert]`	Creates log entries (and alerts) for the specified exception. The `no` command does not create any log entries.
`app protocol_name exception del <1..64>`	Deletes the specified rule.
`no app protocol_name exception <1..64>`	Deletes the specified rule.
`app protocol_name exception move <1..64> <1..64>`	Moves the specified rule (first index) to the specified location. The process is (1) remove the specified rule from the table; (2) re-number; (3) insert the rule at the specified location.

15.2.3 Other Application Commands

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

Table 64 app Commands: Other Applications

COMMAND	DESCRIPTION
`app other {forward | drop | reject}`	Specifies the default action for other applications.
`[no] app other log [alert]`	Creates log entries (and alerts) for other applications. The `no` command does not create any log entries.

15.2.4 Condition Commands for Other Applications

This table lists the commands for conditions in other applications.

Table 65 app Commands: Conditions in Other Applications

COMMAND	DESCRIPTION
`app other insert <1..64>`	Creates a new rule at the specified row and enters sub-command mode.
`app other append`	Creates a new rule, appends it to the end of the list, and enters sub-command mode.
`    [no] schedule profile_name`	Adds the specified schedule to the specified condition for other applications.
`    [no] user username`	Adds the specified user to the specified condition for other applications.
`    [no] source profile_name`	Adds the specified source address to the specified condition for other applications.
`    [no] destination profile_name`	Adds the specified destination address to the specified condition for other applications.

Table 65 app Commands: Conditions in Other Applications (continued)

COMMAND	DESCRIPTION
`    [no] log [alert]`	Creates log entries (and alerts) for the specified exception. The `no` command does not create any log entries.
`    [no] protocol {tcp | udp}`	Adds the specified protocol to the specified condition for other applications.
`    [no] port <1..65535>`	Adds the specified port to the specified condition for other applications.
`    forward | drop | reject`	Adds the specified action to the specified condition for other applications.
`app other del <1..64>`	Deletes the specified condition.
`no app other <1..64>`	Deletes the specified condition.
`app other move <1..64> <1..64>`	Moves the specified condition (first index) to the specified location. The process is (1) remove the specified condition from the table; (2) re-number; (3) insert the condition at the specified location.

15.2.5 General Commands for Application Patrol

This table lists the general commands for application patrol.

Table 66 app Commands: Pre-Defined Applications

COMMAND	DESCRIPTION
`[no] app activate`	Turns on application patrol. The `no` command turns off application patrol.
`show app usage`	Displays how many address references are already used by application patrol.
`show app [all | general | im | p2p | stream]`	Displays information about the specified category(ies) in application patrol.
`show app` *`protocol_name`* `config`	Displays information about the specified application settings in application patrol.
`show app` *`protocol_name`* `allowport`	Displays the allowed ports for the specified application.
`show app` *`protocol_name`* `exception`	Displays the exceptions for the specified application.
`show app other config`	Displays information about other applications in application patrol.
`show app other rule`	Displays information about the conditions for other applications in application patrol.s

15.2.5.1 General Command Examples

The following example shows the information that is displayed by some of the `show` commands.

```
Router# configure terminal
Router# show app http config

Idx= 0
Name= http
Action= forward
Ex_action= drop
Bwm= no
Bandwidth= 0 kbps
Log= no
Alert= no
Router#
```

```
Router# configure terminal
Router(config)# show app http allowport
Index   Port
===========================================================================
 1       80
 2       8080
```

```
Router# configure terminal
Router(config)# show app http exception
Index Schedule   User    Src     Dest    Log     Alert
===========================================================================
 1    none       ENG     any     any     yes     no
2    WORKING    any     SALES   any     no      no
```

```
Router# configure terminal
Router(config)# show app other config
Default_action= forward
Default_log= no
Default_alert= no
```

```
Router# configure terminal
Router(config)# show app other rule
Index Port  Protocol Schedule User  Src     Dest    Access  Log     Alert
===========================================================================
 1    1500  tcp      none     any   any     any     forward yes     no
```

CHAPTER 16
Content Filtering

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

16.1 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.

16.2 Content Filtering Policies

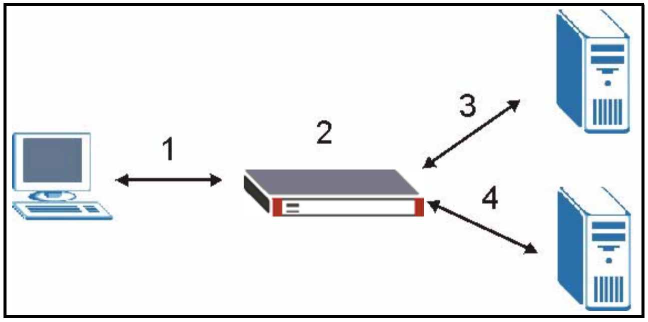
A content filtering policy allows you to do the following.

- Use schedule objects to define when to apply a content filtering profile.
- Use address and/or user/group objects to define to whose web access to apply the content filtering profile.
- Apply a content filtering profile that you have custom-tailored.

16.3 External Web Filtering Service

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

Figure 29 Content Filtering Lookup Procedure



1 A computer behind the ZyWALL tries to access a web site.

2 The ZyWALL looks up the web site in its cache. If an attempt to access the web site was made in the past, a record of that web site's category will be in the ZyWALL's cache. The ZyWALL blocks, blocks and logs or just logs the request based on your configuration.

3 Use the **Content Filter Cache** screen to configure how long a web site address remains in the cache as well as view those web site addresses. All of the web site address records are also cleared from the local cache when the ZyWALL restarts.

4 If the ZyWALL has no record of the web site, it queries the external content filtering database and simultaneously sends the request to the web server.

5 The external content filtering server sends the category information back to the ZyWALL, which then blocks and/or logs access to the web site based on the settings in the content filtering profile. The web site's address and category are then stored in the ZyWALL's content filtering cache.

16.4 Content Filtering Reports

See the web configurator User's Guide to see how to view content filtering reports after you have activated the category-based content filtering subscription service.

16.5 Content Filter Command Input Values

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

Table 67 Content Filter Command Input Values

LABEL	DESCRIPTION
policy_number	The number of the policy <0...15> to define the searching sequence of the filtering policies.
address	The name (up to 63 characters) of an existing address object or group to which the policy should be applied.
schedule	The name (up to 63 characters) of an existing schedule to control when the policy should be applied.
filtering_profile	The filtering profile defines how to filter web URLs or content. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Table 67 Content Filter Command Input Values (continued)

LABEL	DESCRIPTION
category_number	The number of a web category <0…51>. Each number corresponds to a category name.
category_name	The name of a web category (see
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.
forbid_hosts	The IP address or domain name of a forbidden web site. Use a host name such as www.bad-site.com into this text field. Do not use the complete URL of the site – that is, do not include “http://”. All subdomains are also blocked. For example, entering “bad-site.com” also blocks “www.bad-site.com”, “partner.bad-site.com”, “press.bad-site.com”, etc. Use up to 63 case-insensitive characters (0-9a-z-). You can enter a single IP address in dotted decimal notation like 192.168.2.5. You can enter a subnet by entering an IP address in dotted decimal notation followed by a slash and the bit number of the subnet mask of an IP address. The range is 0 to 32. To find the bit number, convert the subnet mask to binary and add all of the 1’s together. Take “255.255.255.0” for example. 255 converts to eight 1’s in binary. There are three 255’s, so add three eights together and you get the bit number (24). An example is 192.168.2.1/24 You can enter an IP address range by entering the start and end IP addresses separated by a hyphen, for example 192.168.2.5-192.168.2.23.
keyword	A keyword or a numerical IP address to search URLs for and block access to if they contain it. Use up to 63 case-insensitive characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,) in double quotes. For example enter “Bad_Site” to block access to any web page that includes the exact phrase “Bad_Site”. This does not block access to web pages that only include part of the phrase (such as “Bad” in this example).
message	The message to display when a web site is blocked. Use up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,) in quotes. For example, “Access to this web page is not allowed. Please contact the network administrator.”
redirect_url	The URL of the web page to which you want to send users when their web access is blocked by content filtering. The web page you specify here opens in a new frame below the denied access message. Use “http://” followed by up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%) in quotes. For example, “http://192.168.1.17/blocked access”.
license	The license key (up to 15 characters) for the external web filtering service.
service_timeout	The value specifies the maximum querying time in seconds <1…60>
cache_timeout	The value specifies the maximum cache life time in hours <1..720>.

Table 67 Content Filter Command Input Values (continued)

LABEL	DESCRIPTION
url	The URL of a web site.
rating_server	The hostname or IP address of the rating server.
query_timeout	The value specifies the maximum querying time when rating a URL in zysh. <1..60> seconds.

The following table lists the content filtering web category numbers and names.

Table 68 Category Name table

CATEGORY NUMBER	CATEGORY NAME	CATEGORY NUMBER	CATEGORY NAME
0	adult-mature-content	26	search-engines-portals
1	pornography	27	web-communications
2	sexeducation	28	job-search-careers
3	intimate-apparel-swimsuit	29	news-media
4	nudity	30	personals-dating
5	alcohol-tobacco	31	reference
6	illegal-questionable	32	chat-instant-messaging
7	gambling	33	email
8	violence-hate-racism	34	newsgroups
9	weapons	35	religion
10	abortion	36	shopping
11	arts-entertainment	37	auctions
12	business-economy	38	real-estate
13	cult-occult	39	society-lifestyle
14	illegal-drugs	40	gay-lesbian
15	education	41	restaurants-dining-food
16	cultural-institutions	42	sports-recreation-hobbies
17	financial-services	43	travel
18	brokerage-trading	44	vehicles
19	games	45	humor-jokes
20	government-legal	46	streaming-media-mp3
21	military	47	software-downloads
22	political-activist-groups	48	pay-to-surf
23	health	49	for-kids
24	computers-internet	50	web-advertisements
25	hacking-proxy-avoidance	51	web-hosting

16.6 General Content Filter Commands

The following table lists the commands that you can use for general content filter configuration such as enabling content filtering, viewing and ordering your list of content filtering policies, creating a denial of access message or specifying a redirect URL and checking your external web filtering service registration status. Use the `configure terminal` command to enter the configuration mode to be able to use these commands. See Table 67 on page 132 for details about the values you can input with these commands.

Table 69 content-filter General Commands

COMMAND	DESCRIPTION
`[no] content-filter active`	Turns on content filtering. The `no` command turns it off.
`[no] content-filter block message` *`message`*	Sets the message to display when content filtering blocks access to a web page. The `no` command clears the setting.
`[no] content-filter block redirect` *`redirect_url`*	Sets the URL of the web page to which to send users when their web access is blocked by content filtering. The `no` command clears the setting.
`[no] content-filter cache-timeout` *`cache_timeout`*	Sets how long the ZyWALL is to keep an entry in the content filtering URL cache before discarding it. The `no` command clears the setting.
`[no] content-filter default block`	Has the ZyWALL block sessions that do not match a content filtering policy. The `no` command allows sessions that do not match a content filtering policy.
`[no] content-filter license` *`license`*	Sets the license key for the external web filtering service. The `no` command clears the setting.
`[no] content-filter policy` *`policy_number address schedule filtering_profile`*	Sets a content filtering policy. The `no` command removes it.
`content-filter policy` *`policy_number`* `shutdown`	Disables a content filtering policy.
`content-filter url-cache test` *`url`*	Tests whether or not a web site is saved in the ZyWALL's database of restricted web pages.
`content-filter url-server test url [ server` *`rating_server`* `] [ timeout` *`query_timeout`* `]`	Tests whether or not a web site is saved in the external content filter server's database of restricted web pages.
`show content-filter policy`	Displays the content filtering policies.
`show content-filter settings`	Displays the general content filtering settings.
`show content-filter url-cache`	Displays the contents of the content filtering URL cache before discarding it.

16.7 Content Filter Filtering Profile Commands

The following table lists the commands that you can use to configure a content filtering policy. A content filtering policy defines which content filter profile should be applied, when it should be applied, and to whose web access it should be applied. Use the `configure terminal` command to enter the configuration mode to be able to use these commands. See Table 67 on page 132 for details about the values you can input with these commands.

Table 70 content-filter Filtering Profile Commands Summary

COMMAND	DESCRIPTION
`[no] content-filter license` *`license`*	Sets the license key for the external web filtering service. The `no` command clears the setting.
`[no] content-filter profile` *`filtering_profile`*	Creates a content filtering profile. The `no` command removes the profile.
`[no] content-filter profile` *`filtering_profile`* `custom`	Sets a content filtering profile to use a profile's custom settings (lists of trusted web sites and forbidden web sites and blocking of certain web features). The `no` command has the profile not use the custom settings.
`[no] content-filter profile` *`filtering_profile`* `custom activex`	Sets a content filtering profile to block ActiveX controls. The `no` command sets the profile to allow ActiveX.
`[no] content-filter profile` *`filtering_profile`* `custom cookie`	Sets a content filtering profile to block Cookies. The `no` command sets the profile to allow Cookies.
`[no] content-filter profile` *`filtering_profile`* `custom forbid` *`forbid_hosts`*	Adds a web site to a content filtering profile's forbidden list. The `no` command removes a web site from the forbidden list.
`[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.
`[no] content-filter profile` *`filtering_profile`* `custom keyword` *`keyword`*	Has a content filtering profile block access to Web sites with URLs that contain the specified keyword or IP address in the URL. The `no` command removes the keyword.
`[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.
`[no] content-filter profile` *`filtering_profile`* `custom trust` *`trust_hosts`*	Adds a web site to a content filtering profile's trusted list. The `no` command removes a web site from the trusted list.
`[no] content-filter profile` *`filtering_profile`* `custom trust-allow-features`	Sets a content filtering profile to permit Java, ActiveX and Cookies from sites on the trusted list. The `no` command has the content filtering profile not permit Java, ActiveX and Cookies from sites on the trusted list
`[no] content-filter profile` *`filtering_profile`* `custom trust-only`	Sets a content filtering profile to only allow access to web sites that are on the trusted list. The `no` command has the profile allow access to web sites that are not on the trusted list.
`[no] content-filter profile` *`filtering_profile`* `url category {category_number | category_name}`	Sets a content filtering profile to check for specific web site categories. The `no` command has the profile not check for the specified categories.

Table 70 content-filter Filtering Profile Commands Summary (continued)

COMMAND	DESCRIPTION
`[no] content-filter profile filtering_profile url match {block | log | block_log}`	Sets a content filtering profile to block, allow and log or block and log access to web pages that match the categories that you select for the profile. The `no` command clears the setting.
`[no] content-filter profile filtering_profile url offline {block | log | block_log}`	Sets a content filtering profile to block, allow and log or block and log access to requested web pages if the external content filtering database is unavailable. The `no` command clears the setting.
`[no] content-filter profile filtering_profile url unrate {block | log | block_log}`	Sets a content filtering profile to block, allow and log or block and log access to web pages that the external web filtering service has not categorized. The `no` command clears the setting.
`[no] content-filter profile filtering_profile url url-server`	Sets a content filtering profile to use the external web filtering service. The `no` command has the profile not use the external web filtering service.
`[no] content-filter service-timeout service_timeout`	Sets how many seconds the ZyWALL is to wait for a response from the external content filtering server. The `no` command clears the setting.
`content-filter url-cache test url`	Tests whether or not a web site is saved in the ZyWALL's database of restricted web pages.
`content-filter url-server test url [server rating_server] [timeout query_timeout]`	Tests whether or not a web site is saved in the external content filter server's database of restricted web pages.
`show content-filter profile [filtering_profile]`	Displays the specified content filtering profile's settings or the settings of all them if you don't specify one.

16.8 Content Filter Cache Commands

The following table lists the commands that you can use to view and configure your ZyWALL's URL caching. You can configure how long a categorized web site address remains in the cache as well as view those web site addresses to which access has been allowed or blocked based on the responses from the external content filtering server. The ZyWALL only queries the external content filtering database for sites not found in the cache.

Use the `configure terminal` command to enter the configuration mode to be able to use these commands. See Table 67 on page 132 for details about the values you can input with these commands.

Table 71 content-filter cache Cache Commands

COMMAND	DESCRIPTION
`[no] content-filter cache-timeout cache_timeout`	Sets how long the ZyWALL is to keep an entry in the content filtering URL cache before discarding it. The `no` command clears the setting.
`show content-filter url-cache`	Displays the contents of the content filtering URL cache before discarding it.

16.9 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. If you have a license key, you can use the `content-filter license` command to use it.

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

7 Activate the customization.

```
Router# configure terminal
Router(config)# address-object sales 172.21.3.0/24
Router(config)# schedule-object all_day 00:00 23:59
Router(config)# content-filter profile sales_CF_PROFILE
Router(config)# content-filter profile sales_CF_PROFILE url category adult-mature-
content
Router(config)# sales_CF_PROFILE url category pornography
Router(config)# content-filter profile sales_CF_PROFILE url url-server
Router(config)# content-filter profile sales_CF_PROFILE custom java
Router(config)# content-filter profile sales_CF_PROFILE custom activex
Router(config)# content-filter profile sales_CF_PROFILE custom proxy
Router(config)# content-filter profile sales_CF_PROFILE custom
```

Use this command to display the settings of the profile.

```
Router(config)# show content-filter profile sales_CF_PROFILE
service active : yes
url match      : block:  no, log:  no
url unrate     : block:  no, log:  no
service offline: block:  no, log:  no

category settings:
Adult/Mature Content      : yes, Pornography               :  no
Sex Education             :  no, Intimate Apparel/Swimsuit :  no
Nudity                    :  no, Alcohol/Tobacco           :  no
Illegal/Questionable      :  no, Gambling                  :  no
Violence/Hate/Racism      :  no, Weapons                   :  no
Abortion                  :  no, Arts/Entertainment        :  no
Business/Economy          :  no, Cult/Occult               :  no
Illegal Drugs             :  no, Education                 :  no
Cultural Institutions     :  no, Financial Services        :  no
Brokerage/Trading         :  no, Games                     :  no
Government/Legal          :  no, Military                  :  no
Political/Activist Groups :  no, Health                    :  no
Computers/Internet        :  no, Hacking/Proxy Avoidance   :  no
Search Engines/Portals    :  no, Web Communications        :  no
Job Search/Careers        :  no, News/Media                :  no
Personals/Dating          :  no, Reference                 :  no
Chat/Instant Messaging    :  no, Email                     :  no
Newsgroups                :  no, Religion                  :  no
Shopping                  :  no, Auctions                  :  no
Real Estate               :  no, Society/Lifestyle         :  no
Gay/Lesbian               :  no, Restaurants/Dining/Food   :  no
Sports/Recreation/Hobbies :  no, Travel                    :  no
Vehicles                  :  no, Humor/Jokes               :  no
Streaming Media/MP3       :  no, Software Downloads        :  no
Pay to Surf               :  no, For Kids                  :  no
Web Advertisements        :  no, Web Hosting               :  no
Unrated                   :  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

No.  Trusted Host
===============================================================================

No.  Forbidden Host
===============================================================================

No.  Keyword
===============================================================================
```

CHAPTER 17
IDP Commands

This chapter introduces IDP-related commands.

17.1 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 72 Input Values for IDP Commands

LABEL	DESCRIPTION
zone_profile	It can consist of alphanumeric characters, the underscore, and the dash, and it is 1-31 characters long. Spaces are not allowed.
idp_profile	It can consist of alphanumeric characters, the underscore, and the dash, and it is 1-31 characters long. Spaces are not allowed.

17.2 General IDP Commands

These commands correspond to the web configurator **IDP** > **General** screen.

17.2.1 IDP Activation

This table shows the IDP activation commands.

Table 73 IDP Activation

COMMAND	DESCRIPTION
`[no] idp activate`	Enables IDP service. IDP service also depends on IDP service registration. You can enable IDP if IDP service is unregistered but only traffic anomaly and protocol anomaly detection applies. You must register for IDP service in order to use packet inspection signatures. If you don't have a standard license, you can register for a once-off trial one. `no` disables IDP service.
`show idp activation`	Displays IDP service status.

17.2.1.1 Activate/Deactivate IDP Example

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

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

17.2.2 Binding an IDP Profile to a Zone

These commands show you how to bind an IDP profile to a zone.

Table 74 Binding an IDP Profile to a Zone

COMMAND	DESCRIPTION
`[no] idp bind` *`zone_profile`* `profile` *`my_profile`*	Associates the specified IDP profile to the specified zone (you need to first create the zone). `no` dissociates the profile from the zone.
`[no] idp zone` *`zone_profile`* `activate`	Activate IDP on the zone you specify. `no` deactivates IDP on the zone you specify
`show idp bindings`	Shows what IDP profiles protect which zones.

17.2.2.1 IDP Profile-Zone Binding Example

In this example, we bind IDP profile “DMZ_IDP” to zone “DMZ-2”, activate it, then show the status.

```
Router# configure terminal
Router(config)# idp bind DMZ-2 profile DMZ_IDP
Router(config)# idp zone DMZ-2 activate
Router(config)# show idp bindings
Zone Name                       Bind Profile                    Activate
========================================================================
LAN                             LAN_IDP                         yes
WAN                             none                            no
DMZ                             DMZ_IDP                         yes
DMZ-2                           DMZ_IDP                         yes
Router(config)#
```

17.3 IDP Profile Commands

These commands correspond to the web configurator **IDP** > **Profile** screen.

17.3.1 Global Profile Commands

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

Table 75 Global Profile Commands

COMMAND	DESCRIPTION
idp rename *profile1 profile2*	Rename profile originally named *profile1* to *profile2.*
no idp *profile3*	Delete profile named *profile3*.
show idp base profile	Displays all IDP base profiles.
show idp profiles	Displays all IDP profiles.

17.3.1.1 Example of Global Profile Commands

In this example we rename a profile from *old_profile* to *new_profile*, delete the *bye_profile* and show all base profiles available.

```
Router# configure terminal
Router(config)# idp rename old_profile new_profile
Router(config)# no idp bye_profile
Router(config)# show idp base profile
No.  Base Profile Name
==============================================================
1    none
2    all
3    wan
4    lan
5    dmz
Router(config)#
```

17.3.2 Editing/Creating Profiles

Use these commands to create a new profile or edit an existing one. It is recommended you use the web configurator to create/edit profiles. If you not specify a base profile, the default base profile is none.

Note: You CANNOT change the base profile later!

Table 76 Editing/Creating Profiles

COMMAND	DESCRIPTION
idp *newpro*	Creates a new profile called *newpro*. *newpro* uses the "none" base profile in this example. You are now in sub-command mode. All the following commands relate to the new profile. Use `exit` to quit sub-command mode.
scan-detection sensitivity {low | medium | high}	Sets scan-detection sensitivity.

Table 76 Editing/Creating Profiles (continued)

COMMAND	DESCRIPTION
`no scan-detection sensitivity`	Clears scan-detection sensitivity. The default sensitivity is medium.
`[no] scan-detection {tcp-xxx} activate`	Activates TCP scan detection options where {tcp-xxx} = {tcp-portscan | tcp-decoy-portscan | tcp-portsweep | tcp-distributed-portscan | tcp-filtered-portscan | tcp-filtered-decoy-portscan | tcp-filtered-distributed-portscan | tcp-filtered-portsweep}. `no` deactivates TCP scan detection options.
`[no] scan-detection {tcp-xxx} log [alert]`	Sets TCP scan-detection logs or alerts.
`[no] scan-detection {udp-xxx} activate`	Activates or deactivates UDP scan detection options where {udp-xxx} = {udp-portscan | udp-decoy-portscan | udp-portsweep | udp-distributed-portscan | udp-filtered-portscan | udp-filtered-decoy-portscan | udp-filtered-distributed-portscan | udp-filtered-portsweep}
`scan-detection {udp-xxx} log [alert]`	Sets UDP scan-detection logs or alerts.
`no scan-detection {udp-xxx} log`	Deactivates UDP scan-detection logs.
`[no] scan-detection {ip-xxx} activate`	Activates or deactivates IP scan detection options where {ip-xxx} = {ip-protocol-scan | ip-decoy-protocol-scan | ip-protocol-sweep | ip-distributed-protocol-scan | ip-filtered-protocol-scan | ip-filtered-decoy-protocol-scan | ip-filtered-distributed-protocol-scan | ip-filtered-protocol-sweep}
`scan-detection {ip-xxx} log [alert]`	Sets IP scan-detection logs or alerts.
`no scan-detection {ip-xxx} log`	Deactivates IP scan-detection logs.
`[no] scan-detection {icmp-sweep | icmp-filtered-sweep} activate`	Activates or deactivates ICMP scan detection options.
`scan-detection {icmp-sweep | icmp-filtered-sweep} log [alert]`	Sets ICMP scan-detection logs or alerts.
`no scan-detection {icmp-sweep | icmp-filtered-sweep} log`	Deactivates ICMP scan-detection logs.
`[no] scan-detection open-port activate`	Activates or deactivates open port scan detection options.
`scan-detection open-port log [alert]`	Sets open port scan-detection logs or alerts.
`no scan-detection open-port log`	Deactivates open port scan-detection logs.
`flood-detection sensitivity {low | medium | high}`	Sets IDP flood-detection sensitivity level.
`[no] flood-detection sensitivity`	Clears IDP flood-detection sensitivity. The default sensitivity is medium.
`[no] flood-detection {tcp-flood | udp-flood | ip-flood | icmp-flood} activate`	Activates or deactivates TCP, UDP, IP or ICMP flood detection.
`flood-detection {tcp-flood | udp-flood | ip-flood | icmp-flood} log [alert]`	Sets TCP, UDP, IP or ICMP flood detection logs or alerts.
`no flood-detection {tcp-flood | udp-flood | ip-flood | icmp-flood} log`	Deactivates TCP, UDP, IP or ICMP flood detection logs.

Table 76 Editing/Creating Profiles (continued)

COMMAND	DESCRIPTION
`[no] http-inspection {http-xxx} activate`	Activates or deactivates http-inspection options where http-xxx = {ascii-encoding | double-encoding | u-encoding | bare-byte-unicode-encoding | base36-encoding | utf-8-encoding | iis-unicode-codepoint-encoding | multi-slash-encoding | iis-backslash-evasion | self-directory-traversal | directory-traversal | apache-whitespace | non-rfc-http-delimiter | non-rfc-defined-char | oversize-request-uri-directory | oversize-chunk-encoding | webroot-directory-traversal}
`http-inspection {http-xxx} log [alert]`	Sets http-inspection log or alert.
`no http-inspection {http-xxx} log`	Deactivates http-inspection logs.
`[no] http-inspection {http-xxx} action {drop | reject-sender | reject-receiver | reject-both}}`	Sets http-inspection action
`[no] tcp-decoder {tcp-xxx} activate`	Activates or deactivates tcp decoder options where {tcp-xxx} = {undersize-len | undersize-offset | oversize-offset | bad-length-options | truncated-options | ttcp-detected | obsolete-options | experimental-options}
`tcp-decoder {tcp-xxx} log [alert]`	Sets tcp decoder log or alert options.
`no tcp-decoder {tcp-xxx} log`	Deactivates tcp decoder log or alert options.
`[no] tcp-decoder {tcp-xxx} action {drop | reject-sender | reject-receiver | reject-both}}`	Sets tcp decoder action
`[no] udp-decoder {truncated-header | undersize-len | oversize-len} activate`	Activates or deactivates udp decoder options
`udp-decoder {truncated-header | undersize-len | oversize-len} log [alert]`	Sets udp decoder log or alert options.
`no udp-decoder {truncated-header | undersize-len | oversize-len} log`	Deactivates udp decoder log options.
`udp-decoder {truncated-header | undersize-len | oversize-len} action {drop | reject-sender | reject-receiver | reject-both}`	Sets udp decoder action
`no udp-decoder {truncated-header | undersize-len | oversize-len} action`	Deactivates udp decoder actions.
`[no] icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} activate`	Activates or deactivates icmp decoder options
`icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} log [alert]`	Sets icmp decoder log or alert options.
`no icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} log`	Deactivates icmp decoder log options.

Table 76 Editing/Creating Profiles (continued)

COMMAND	DESCRIPTION
icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} action {drop | reject-sender | reject-receiver | reject-both}}	Sets icmp decoder action
no icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} action	Deactivates icmp decoder actions.
[no] signature *SID* activate	Activates or deactivates an IDP signature.
signature *SID* log [alert]	Sets log or alert options for an IDP signature
no signature *SID* log	Deactivates log options for an IDP signature
signature *SID* action {drop | reject-sender | reject-receiver | reject-both}	Sets an action for an IDP signature
no signature *SID* action	Deactivates an action for an IDP signature.
show idp *profile* scan-detection [all details]	Shows all scan-detection settings of the specified IDP profile.
show idp *profile* scan-detection {tcp-portscan | tcp-decoy-portscan | tcp-portsweep | tcp-distributed-portscan | tcp-filtered-portscan | tcp-filtered-decoy-portscan | tcp-filtered-distributed-portscan | tcp-filtered-portsweep} details	Shows selected TCP scan-detection settings for the specified IDP profile.
show idp *profile* scan-detection {udp-portscan | udp-decoy-portscan | udp-portsweep | udp-distributed-portscan | udp-filtered-portscan | udp-filtered-decoy-portscan | udp-filtered-distributed-portscan | udp-filtered-portsweep} details	Shows UDP scan-detection settings for the specified IDP profile.
show idp *profile* scan-detection {ip-protocol-scan | ip-decoy-protocol-scan | ip-protocol-sweep | ip-distributed-protocol-scan | ip-filtered-protocol-scan | ip-filtered-decoy-protocol-scan | ip-filtered-distributed-protocol-scan | ip-filtered-protocol-sweep} details	Shows IP scan-detection settings for the specified IDP profile.
show idp *profile* scan-detection {icmp-sweep | icmp-filtered-sweep | open-port} details	Shows ICMP scan-detection settings for the specified IDP profile.
show idp *profile* flood-detection [all details]	Shows all flood-detection settings for the specified IDP profile.
show idp *profile* flood-detection {tcp-flood | udp-flood | ip-flood | icmp-flood} details	Shows flood-detection settings for the specified IDP profile.
show idp *profile* http-inspection all details	Shows http-inspection settings for the specified IDP profile.

Table 76 Editing/Creating Profiles (continued)

COMMAND	DESCRIPTION
show idp *profile* http-inspection {ascii-encoding | double-encoding | u-encoding | bare-byte-unicode-encoding | base36-encoding | utf-8-encoding | iis-unicode-codepoint-encoding | multi-slash-encoding | iis-backslash-evasion | self-directory-traversal | directory-traversal | apache-whitespace | non-rfc-http-delimiter | non-rfc-defined-char | oversize-request-uri-directory | oversize-chunk-encoding | webroot-directory-traversal} details	Shows http-inspection settings for the specified IDP profile.
show idp *profile* tcp-decoder all details	Shows tcp-decoder settings for the specified IDP profile.
show idp *profile* tcp-decoder {undersize-len | undersize-offset | oversize-offset | bad-length-options | truncated-options | ttcp-detected | obsolete-options | experimental-options} details	Shows tcp-decoder settings for the specified IDP profile.
show idp *profile* udp-decoder all details	Shows udp-decoder settings for the specified IDP profile.
show idp *profile* udp-decoder {truncated-header | undersize-len | oversize-len} details	Shows specified udp-decoder settings for the specified IDP profile.
show idp *profile* icmp-decoder all details	Shows all icmp-decoder settings for the specified IDP profile.
show idp *profile* icmp-decoder {truncated-header | truncated-timestamp-header | truncated-address-header} details	Shows specified icmp-decoder settings for the specified IDP profile.
show idp *profile* signature SID details	Shows signature ID details of the specified profile.
show idp *profile* signature {all | custom-signature} details	Shows the signature details of the specified profile.

17.3.2.1 Creating a Profile Example

In this example we create a profile named *test*, configure some settings, display them, and then return to global command mode.

```
Router# configure terminal
Router(config)# idp test
Router(config-idp-profile-test)# tcp-decoder oversize-offset action drop
Router(config-idp-profile-test)# tcp-decoder oversize-offset log alert
Router(config-idp-profile-test)# tcp-decoder oversize-offset activate
Router(config-idp-profile-test)# no tcp-decoder oversize-offset activate
Router(config-idp-profile-test)# exit
Router(config)# show idp test tcp-decoder oversize-offset details
message: (tcp_decoder) OVERSIZE-OFFSET ATTACK
  keyword: tcp-decoder oversize-offset
  activate: no
  action: drop
  log: log alert
Router(config)#
```

17.3.3 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 77 Signature Search Command

COMMAND	DESCRIPTION
`idp search` *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.

17.3.3.1 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 78 Severity, Platform and Policy Type Command Values

SEVERITY	PLATFORM	POLICY TYPE
1 = Very Low 2 = Low 3 = Medium 4 = High 5 = Severe	1 = All 2 = Win95/98 4 = WinNT 8 = WinXP/2000 16 = Linux 32 = FreeBSD 64 = Solaris 128 = SGI 256 = Other-Unix 512 = Network-Device	1 =DoS 2 =Buffer-Overflow 3 = Access-Control 4 = Scan 5 = Backdoor/Trojan 6 = Others 7 = P2P 8 = IM 9 = Virtus/Worm 10 = Porn 11 = Web-Attack 12 = Spam

The following table displays the command line service and action equivalent values. If you want to combine services in a search, then add their respective numbers together. For example, to search for signatures for DNS, Finger and FTP services, then type "7" as the service parameter.

Table 79 Service and Action Command Values

SERVICE	SERVICE	ACTION
1 = DNS 2 = FINGER 4 = FTP 8 = MYSQL 16 = ICMP 32 = IM 64 = IMAP 128 = MISC 256 = NETBIOS 512 = NNTP 1024 = ORACLE 2048 = P2P 4096 = POP2 8192 = POP3 16384 = RPC 32768 = RSERVICES	65536 = SMTP 131072 = SNMP 262144 = SQL 524288 = TELNET 1048576 = TFTP 2097152 = n/a 4194304 = WEB_ATTACKS 8388608 = WEB_CGI 16777216 = WEB_FRONTPAGE 33554432 = WEB_IIS 67108864 = WEB_MISC 134217728 = WEB_PHP 268435456 = MISC_BACKDOOR 536870912 = MISC_DDOS 1073741824 = MISC_EXPLOIT	1 = None 2 = Drop 4 = Reject-sender 8 = Reject-receiver 16 = Reject-both

17.3.3.2 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 LAN_IDP name “worm” sid 12345 severity 1
-> platform 4 policytype 4 service 1 activate yes log log action 2
```

17.4 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 **IDP > Custom Signatures** screen.

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

Table 80 Custom Signatures

COMMAND	DESCRIPTION
`idp customize signature` *quoted_string*	Create a new custom signature. The quoted string is the signature command string enclosed in quotes. for example. "alert tcp any any <> any any (msg: \"test\"; sid: 9000000 ;)".
`idp customize signature edit` *quoted_string*	Edits an existing custom signature.
`no idp customize signature` *custom_sid*	Deletes a custom signature.
`show idp signatures custom-signature` *custom_sid* `{details | contents | non-contents}`	Displays custom signature information.
`show idp signatures custom-signature all details`	Displays all custom signatures’ information.
`show idp signatures custom-signature number`	Displays the total number of custom signatures.

17.4.1 Custom Signature Examples

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

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

This example shows you how to edit a custom signature.

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

This example shows you how to display custom signature details.

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

This example shows you how to display custom signature contents.

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

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

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

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

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

17.5 Update IDP Signatures

Use these commands to update new signatures.You should have already registered for IDP service. You can also update signatures using the web configurator **IDP > Update** screen.

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

Table 81 Update Signatures

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

17.5.1 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 update signatures
IDP signature update in progress.
Please check system log for future information.
Router(config)# idp update auto
Router(config)# no idp update auto
Router(config)# idp update hourly
Router(config)# idp update daily 10
Router(config)# idp update weekly fri 13
Router(config)# show idp update
auto: yes
schedule: weekly at Friday 13 o'clock
Router(config)# show idp 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 signatures version
version: 1.2000
Router(config)# show idp signatures number
signatures: 2000
Router(config)# show idp signatures date
date: 2005/11/13 13:56:03
```

CHAPTER 18 Virtual Servers

This chapter describes how to set up, manage, and remove virtual servers.

18.1 Virtual Server Overview

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

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

18.2 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 82 Input Values for Virtual Server Commands

LABEL	DESCRIPTION
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 83 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 `*`ip`*` map-type any [deactivate]`	Creates or modifies the specified virtual server and maps the specified destination IP address (for all destination ports) to the specified destination 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*).

Table 83 ip virtual-server Commands (continued)

COMMAND	DESCRIPTION
ip virtual-server *profile_name* interface *interface_name* original-ip {any | *ip* | *address_object*} map-to *ip* map-type port protocol {any | tcp | udp} original-port <1..65535> mapped-port <1..65535> [deactivate]	Creates or modifies the specified virtual port 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*).
ip virtual-server *profile_name* interface *interface_name* original-ip {any | *ip* | *address_object*} map-to *ip* map-type ports protocol {any | tcp | udp} original-port-begin <1..65535> original-port-end <1..65535> mapped-port-begin <1..65535> [deactivate]	Creates or modifies the specified virtual port 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*).
ip virtual-server {activate | deactivate} *profile_name*	Activates or deactivates the specified virtual server.
ip virtual-server rename *profile_name* *profile_name*	Renames the specified virtual server from the first *profile_name* to the second *profile_name*.

18.2.1 Virtual Server Command Examples

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

```
Router# configure terminal
Router(config)# show ip virtual-server
virtual server: VR1
  active: yes
  interface: ge1
  original IP: any, mapped IP: 192.168.3.2
  mapping type: any, protocol type: any
  original start port: none, original end port: none
  mapped start port: none, mapped end port: none
```

The following command creates virtual server VR1 on interface ge1 that maps ge1 IP addresses to 192.168.3.2.

```
Router# configure terminal
Router(config)# ip virtual-server VR1 interface ge1 original-ip any map-to
192.168.3.2 map-type any
```

CHAPTER 19 HTTP Redirect

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

19.1 HTTP Redirect Overview

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

19.1.1 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.

19.2 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 84 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: ge*x*, *x* = 1 - 5 virtual interface on top of Ethernet interface: ge*x*:*y*, *x* = 1 - 5, *y* = 1 - 12 VLAN interface: vlan*x*, *x* = 0 - 15 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 15, *y* = 1 - 12 bridge interface: br*x*, *x* = 0 - 11 virtual interface on top of bridge interface: br*x*:*y*, *x* = 0 - 11, *y* = 1 - 12 PPPoE/PPTP interface: ppp*x*, *x* = 0 - 11

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 85 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.

19.2.1 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
```

CHAPTER 20
VoIP Pass Through

This chapter covers how to use the ZyWALL's VoIP pass through feature to allow SIP and H.323 VoIP applications to pass through the ZyWALL.

20.1 VoIP Pass Through Introduction

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

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

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

You do not need to use STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) for VoIP devices behind the ZyWALL when you enable the SIP ALG.

20.2 VoIP Pass Through 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 86 alg Commands

COMMAND	DESCRIPTION
`alg sip [ (signal-extra-port <1025..65535>) | ( media-timeout <1..86400>) | (signal-timeout <1..86400>) ]`	Turns on or configures the SIP ALG. Use `signal-extra-port` with a listening port number (1025 to 65535) if you are using SIP on a port other than UDP 5060. 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.
`alg h323`	Turns on the H.323 ALG.
`no alg {sip | h323}`	Turns off an ALG.
`show alg type`	Displays the current ALG configuration.

20.3 VoIP Pass Through 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
```

CHAPTER 21 User/Group

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

21.1 User Account Overview

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

21.1.1 User Types

There are the types of user accounts the ZyWALL uses.

Table 87 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
Admin	Change ZyWALL configuration (web, CLI)	WWW, TELNET, SSH, FTP
Limited-Admin	Look at ZyWALL configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH
Access Users		
User	Access network services Browse user-mode commands (CLI)	WWW, TELNET, SSH
Guest	Access network services	WWW
Ext-User	See Section 21.2 on page 164.	WWW

Note: The default **admin** account is always authenticated locally, regardless of the authentication method setting. (See Chapter 26 on page 187 for more information about authentication methods.)

21.2 User/Group Commands Summary

The following table identify the values required for many `username/groupname` commands. Other input values are discussed with the corresponding commands.

Table 88 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.

21.2.1 User Commands

The first table lists the commands for users.

Table 89 username/groupname Commands Summary: Users

COMMAND	DESCRIPTION
show username [*username*]	Displays information about the specified user or about all users set up in the ZyWALL.
username *username* nopassword user-type {admin | guest | limited-admin | user}	Creates the specified user (if necessary), disables the password, and sets the user type for the specified user.
username *username* password *password* user-type {admin | guest | limited-admin | user}	Creates the specified user (if necessary); enables and sets the password; and sets the user type for the specified user. *password*: You can use 1-63 printable ASCII characters, except double quotation marks (“) and question marks (?).
username *username* user-type ext-user	Creates the specified user (if necessary) and sets the user type to **Ext-User**.
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.

Table 89 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).

21.2.2 User Group Commands

This table lists the commands for groups.

Table 90 username/groupname Commands Summary: Groups

COMMAND	DESCRIPTION
`show groupname [*groupname*]`	Displays information about the specified user group or about all user groups set up in the ZyWALL.
`[no] groupname *groupname*`	Creates the specified user group if necessary and enters sub-command mode. The `no` command deletes the specified user group.
`    [no] description *description*`	Sets the description for the specified user group. The `no` command clears the description for the specified user group.
`    [no] groupname *groupname*`	Adds the specified user group (second *groupname*) to the specified user group (first *groupname*).
`    [no] user *username*`	Adds the specified user to the specified user group.
`    show`	Displays information about the specified user group.
`groupname rename *groupname* *groupname*`	Renames the specified user group (first *groupname*) to the specified group-name (second *groupname*).

21.2.3 User Setting Commands

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

Table 91 username/groupname Commands Summary: Settings

COMMAND	DESCRIPTION
`show users default-setting`	Displays information about the default settings for new users.
`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.

Table 91 username/groupname Commands Summary: Settings (continued)

COMMAND	DESCRIPTION
`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 {guest | limited-admin | user}`	Sets the default user type for each new user. The `no` command sets the default user type to user.
`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.

21.2.3.1 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
```

21.2.4 Force User Authentication Commands

This table lists the commands for forcing user authentication.

Table 92 username/groupname Commands Summary: Forcing User Authentication

COMMAND	DESCRIPTION
`force-auth policy <1..1024>`	Creates the specified condition for forcing user authentication, if necessary, and enters sub-command mode. The conditions are checked in sequence, starting at 1.
`force-auth policy append`	Creates a new condition for forcing user authentication at the end of the current list and enters sub-command mode.
`force-auth policy insert <1..1024>`	Creates a new condition for forcing user authentication at the specified location, renumbers the other conditions accordingly, and enters sub-command mode.
`[no] activate`	Activates the specified condition. The `no` command deactivates the specified condition.
`[no] description` *`description`*	Sets the description for the specified condition. The `no` command clears the description. *description*: You can use alphanumeric and `()+/:=?!*#@$_%–` characters, and it can be up to 60 characters long.
`[no] destination {`*`address_object`*` | `*`group_name`*`}`	Sets the destination criteria for the specified condition. The `no` command removes the destination criteria, making the condition effective for all destinations.
`[no] force`	Forces users to log in to the ZyWALL if the specified condition is satisfied. The `no` command means that users do not log in to the ZyWALL.
`[no] schedule` *`schedule_name`*	Sets the time criteria for the specified condition. The `no` command removes the time criteria, making the condition effective all the time.
`[no] source {`*`address_object`*` | `*`group_name`*`}`	Sets the source criteria for the specified condition. The `no` command removes the source criteria, making the condition effective for all sources.
`show`	Displays information about the specified condition.
`force-auth policy delete <1..1024>`	Deletes the specified condition.

Table 92 username/groupname Commands Summary: Forcing User Authentication (continued)

COMMAND	DESCRIPTION
`force-auth policy flush`	Deletes every condition.
`force-auth policy move <1..1024> to <1..1024>`	Moves the specified condition to the specified location and renumbers the other conditions accordingly.

21.2.5 Additional User Commands

This table lists additional commands for users.

Table 93 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	Unlocks the specified IP address.
users force-logout *ip* | *username*	Logs out the specified logins.

21.2.5.1 Additional User Command Examples

The following commands display the users that are currently logged in to the ZyWALL and forces the logout of all logins from a specific IP address.

```
Router# configure terminal
Router(config)# show users all
No.  Name                            Type            From            Service
     Session Time    Idle Time       Lease Timeout   Re-Auth. Timeout
===========================================================================
1    admin                         admin          192.168.1.34    http/https
     00:33:27        unlimited       23:45:18        23:26:33
2    admin                         admin          192.168.1.34    http/https
     00:14:31        unlimited       23:48:38        23:45:29
3    admin                         admin          172.23.23.83    http/https
     00:04:07        unlimited       23:58:32        23:55:53
4    admin                           admin           172.23.23.83    telnet
     00:03:30        unlimited       23:59:59        23:56:30
Router(config)# users force-logout 192.168.1.34
Logout user 'admin'(from 192.168.1.34): OK
Logout user 'admin'(from 192.168.1.34): OK
Total 2 users have been forced logout
Router(config)# show users all
No.  Name                            Type            From            Service
     Session Time    Idle Time       Lease Timeout   Re-Auth. Timeout
===========================================================================
1    admin                         admin          172.23.23.83    http/https
     00:04:31        unlimited       23:58:08        23:55:29
2    admin                           admin           172.23.23.83    telnet
     00:03:54        unlimited       24:00:00        23:56:06
```

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    172.23.23.60    2                       46

Router(config)# unlock lockout-users 172.23.23.60
User from 172.23.23.60 is unlocked
Router(config)# show lockout-users
No.  Username Tried                  From            Lockout Time Remaining
===========================================================================
No.  From            Failed Login Attempt    Record Expired Timer
===========================================================================
```

CHAPTER 22
Addresses

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

22.1 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.

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.

22.2 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 94 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.

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

22.2.1 Address Object Commands

This table lists the commands for address objects.

Table 95 address-object Commands: Address Objects

COMMAND	DESCRIPTION
`show address-object [`*`object_name`*`]`	Displays information about the specified address or all the addresses.
`address-object` *`object_name`* `{`*`ip`*` | `*`ip_range`*` | `*`ip_subnet`*`}`	Creates the specified address 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>
`no address-object` *`object_name`*	Deletes the specified address.
`address-object rename` *`object_name object_name`*	Renames the specified address (first *object_name*) to the second *object_name*.

22.2.1.1 Address Object Command Examples

The following commands create the three types of address objects and then delete 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
```

22.2.2 Address Group Commands

This table lists the commands for address groups.

Table 96 object-group Commands: Address Groups

COMMAND	DESCRIPTION
`show object-group address [`*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.
`[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*.

22.2.2.1 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
```

CHAPTER 23 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.

23.1 Services Overview

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

23.2 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 97 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.

23.2.1 Service Object Commands

The first table lists the commands for service objects.

Table 98 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 98 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*.

23.2.1.1 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
```

23.2.2 Service Group Commands

The first table lists the commands for service groups.

Table 99 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.
[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*.

23.2.2.1 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
```

CHAPTER 24 Schedules

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

24.1 Schedule Overview

The ZyWALL supports two types of schedules: one-time and recurring. One-time schedules are effective only once, while recurring schedules usually repeat. Both types of schedules are based on the current date and time in the ZyWALL.

Note: Schedules are based on the current date and time in the ZyWALL.

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.

24.2 Schedule Commands Summary

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

Table 100 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.

The following table lists the schedule commands.

Table 101 schedule Commands

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

Table 101 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> *time*: 24-hour time; <0..23>:<0..59>
`schedule-object` *`object_name time time`* `[`*`day`*`] [`*`day`*`] [`*`day`*`] [`*`day`*`] [`*`day`*`] [`*`day`*`] [`*`day`*`]`	Creates or updates a recurring schedule. *time*: 24-hour time; <0..23>:<0..59> *day*: 3-character day of the week; sun | mon | tue | wed | thu | fri | sat

24.2.1 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
```

CHAPTER 25
AAA Server

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

25.1 AAA Server Overview

You can use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network.

The following lists the types of authentication server the ZyWALL supports.

- Local user database

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

- LDAP (Lightweight Directory Access Protocol)

  LDAP (Lightweight Directory Access Protocol) 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.

- 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.

25.2 Authentication Server Command Summary

This section describes the commands for authentication server settings.

25.2.1 ldap-server Commands

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

Table 102 ldap-server Commands

COMMAND	DESCRIPTION
`show ldap-server`	Displays current LDAP server settings.
`[no] ldap-server basedn` *`BaseDN`*	Sets a base distinguished name (DN) for the default LDAP server. A base DN identifies an LDAP directory. The `no` command clears this setting.
`[no] ldap-server binddn` *`BindDN`*	Sets the user name the ZyWALL uses to log into the default LDAP server. The `no` command clears this setting.
`[no] ldap-server cn-identifier` *`uid`*	Sets the unique common name (cn) to identify a record. The `no` command clears this setting.
`[no] ldap-server host` *`LDAP_Server`*	Sets the LDAP server address. Enter the IP address (in dotted decimal notation) or the domain name. The `no` command clears this setting.
`[no] ldap-server password` *`password`*	Sets the bind password. The `no` command clears this setting.
`[no] ldap-server port` *`port_no`*	Sets the LDAP port number. Enter a number between 1 and 65535. The default is 389. The `no` command clears this setting.
`[no] ldap-server search-time-limit` *`time`*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The `no` command clears this setting.
`[no] ldap-server ssl`	Enables the ZyWALL to establish a secure connection to the LDAP server. The `no` command disables this feature.

25.2.2 radius-server Commands

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

Table 103 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.

Table 103 radius-server Commands (continued)

COMMAND	DESCRIPTION
`[no] radius-server key` *`secret`*	Sets a password (up to 15 alphanumeric characters) as the key to be shared between the RADIUS server and the ZyWALL. The `no` command clears this setting.
`[no] radius-server timeout` *`time`*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The `no` command clears this setting.

25.2.3 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)#
```

25.2.4 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 104 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` *`group-name`*	
`   [no] server basedn` *`BaseDN`*	Sets the base DN to point to the LDAP directory on the LDAP server. The `no` command clears this setting.

Table 104 aaa group server ldap Commands (continued)

COMMAND	DESCRIPTION
`[no] server binddn` *`BindDN`*	Sets the user name the ZyWALL uses to log into the default LDAP server. The `no` command clears this setting.
`[no] server cn-identifier` *`uid`*	Sets the user name the ZyWALL uses to log into the default LDAP server. The `no` command clears this setting.
`[no] server host` *`LDAP_Server`*	Sets the LDAP server address. Enter the IP address (in dotted decimal notation) or the domain name of an LDAP server to add to this group. The `no` command clears this setting.
`[no] server password` *`password`*	Sets the bind password (up to 15 characters). The `no` command clears this setting.
`[no] server port` *`port_no`*	Sets the LDAP port number. Enter a number between 1 and 65535. The default is 389. The `no` command clears this setting.
`[no] server search-time-limit` *`time`*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The `no` command clears this setting and set this to the default setting of 5 seconds.
`[no] server ssl`	Enables the ZyWALL to establish a secure connection to the LDAP server. The `no` command disables this feature.

25.2.5 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 105 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.
`aaa group server radius` *`group-name`*	

Table 105 aaa group server radius Commands (continued)

COMMAND	DESCRIPTION
`[no] server host` *`RADIUS_Server`*	Sets the RADIUS server address. Enter the IP address (in dotted decimal notation) or the domain name of a RADIUS server to add to this server group. The `no` command clears this setting.
`[no] server key` *`secret`*	Sets a password (up to 15 alphanumeric characters) as the key to be shared between the RADIUS server(s) and the ZyWALL. The `no` command clears this setting.
`[no] server timeout` *`time`*	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The `no` command clears this setting and set this to the default setting of 5 seconds.

25.2.6 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.

```
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
No.  Name                            Reference
==========================================================================
1    RADIUSGroup1                    0
Router(config)#
```

CHAPTER 26 Authentication Objects

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

26.1 Authentication Objects Overview

After you have created the AAA server objects, you can specify the authentication objects (containing the AAA server information) that the ZyWALL uses to authenticate users (using VPN or managing through HTTP/HTTPS).

26.2 aaa authentication Commands

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

Table 106 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` *`profile-name`*`[no]` *`member1`* `[`*`member2`*`] [`*`member3`*`]`	Sets the profile to use the authentication method(s) in the order specified. `member` = **`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. Use the `no` command to clear the authentication method settings for the profile.

26.2.1 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)#
```

CHAPTER 27
Certificates

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

27.1 Certificates Overview

The ZyWALL can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner’s identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyWALL to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

27.2 Certificate Commands

This section describes the commands for configuring certificates.

27.3 Certificates Commands Input Values

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

Table 107 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.

Table 107 Certificates Commands Input Values (continued)

LABEL	DESCRIPTION
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.
organization	Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
country	Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
key_length	Type a number to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
password	When you have the ZyWALL enroll for a certificate immediately online, the certification authority may want you to include a key (password) to identify your certification request. Use up to 31 of the following characters. a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
CA_name	When you have the ZyWALL enroll for a certificate immediately online, you must have the certification authority’s certificate already imported as a trusted certificate. Specify the name of the certification authority’s certificate. It can be up to 31 alphanumeric and ;‘~!@#$%^&()_+[]{}’,.=- characters.
url	When you have the ZyWALL enroll for a certificate immediately online, enter the IP address (or URL) of the certification authority server. You can use up to 511 of the following characters. a-zA-Z0-9'()+,/:.=?;!*#@$_%-

27.4 Certificates Commands Summary

The following table lists the commands that you can use to display and manage the ZyWALL’s summary list of certificates and certification requests. You can also create certificates or certification requests. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

Table 108 ca Commands Summary

COMMAND	DESCRIPTION
ca enroll cmp name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa} key-len *key_length* num <0..99999999> password *password* ca *CA_name* url *url;*	Enrolls a certificate with a CA using Certificate Management Protocol (CMP). The certification authority may want you to include a reference number and key (password) to identify your certification request.
ca enroll scep name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa} key-len *key_length* password *password* ca *CA_name* url *url*	Enrolls a certificate with a CA using Simple Certificate Enrollment Protocol (SCEP). The certification authority may want you to include a key (password) to identify your certification request.

Table 108 ca Commands Summary (continued)

COMMAND	DESCRIPTION
ca generate pkcs10 name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa} key-len *key_length*	Generates a PKCS#10 certification request.
ca generate pkcs12 name *name* password *password*	Generates a PKCS#12 certificate.
ca generate x509 name *certificate_name* cn-type {ip cn *cn_address*|fqdn cn *cn_domain_name*|mail cn *cn_email*} [ou *organizational_unit*] [o *organization*] [c *country*] key-type {rsa|dsa} key-len *key_length*	Generates a self-signed x509 certificate.
ca rename category {local|remote} *old_name* *new_name*	Renames a local (my certificates) or remote (trusted certificates) certificate.
ca validation *remote_certificate*	Enters the sub command mode for validation of certificates signed by the specified remote (trusted) certificates.
ca validation *remote_certificate* cdp {activate|deactivate}	Has the ZyWALL check (or not check) incoming certificates that are signed by this certificate against a Certificate Revocation List (CRL) or an OCSP server. You also need to configure the OSCP or LDAP server details.
ca validation *name* ldap {activate|deactivate}	Has the ZyWALL check (or not check) incoming certificates that are signed by this certificate against a Certificate Revocation List (CRL) on a LDAP (Lightweight Directory Access Protocol) directory server.
ca validation NAME ldap ip {*IPv4*|*FQDN*} port <1..65535> [id *name* password *password*] [deactivate]	Sets the validation configuration for the specified remote (trusted) certificate where the directory server uses LDAP. ip: Type the IP address (in dotted decimal notation) or the domain name of the directory server. The domain name can use alphanumeric characters, periods and hyphens. Up to 255 characters. port: Specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP. The ZyWALL may need to authenticate itself in order to access the CRL directory server. Type the login name (up to 31 characters) from the entity maintaining the server (usually a certification authority). You can use alphanumeric characters, the underscore and the dash. Type the password (up to 31 characters) from the entity maintaining the CRL directory server (usually a certification authority). You can use the following characters: a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-
ca validation *name* ocsp {activate|deactivate}	Has the ZyWALL check (or not check) incoming certificates that are signed by this certificate against a directory server that uses OCSP (Online Certificate Status Protocol).

Table 108 ca Commands Summary (continued)

<table>
<tr><th>COMMAND</th><th>DESCRIPTION</th></tr>
<tr><td>   ca validation *name* ocsp url *url* [id *name* password *password*] [deactivate]</td><td>Sets the validation configuration for the specified remote (trusted) certificate where the directory server uses OCSP.
url: Type the protocol, IP address and pathname of the OCSP server.
name: The ZyWALL may need to authenticate itself in order to access the OCSP server. Type the login name (up to 31 characters) from the entity maintaining the server (usually a certification authority). You can use alphanumeric characters, the underscore and the dash.
password: Type the password (up to 31 characters) from the entity maintaining the OCSP server (usually a certification authority). You can use the following characters: a-zA-Z0-9;|`~!@#$%^&*()_+\{}':,./<>=-</td></tr>
<tr><td>no ca category {local|remote} *certificate_name*</td><td>Deletes the specified local (my certificates) or remote (trusted certificates) certificate.</td></tr>
<tr><td>no ca validation *name*</td><td>Removes the validation configuration for the specified remote (trusted) certificate.</td></tr>
<tr><td>show ca category {local|remote} name *certificate_name* certpath</td><td>Displays the certification path of the specified local (my certificates) or remote (trusted certificates) certificate.</td></tr>
<tr><td>show ca category {local|remote} [name *certificate_name* format {text|pem}]</td><td>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.</td></tr>
<tr><td>show ca validation name *name*</td><td>Displays the validation configuration for the specified remote (trusted) certificate.</td></tr>
<tr><td>show ca spaceusage</td><td>Displays the storage space in use by certificates.</td></tr>
</table>

27.5 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
```

CHAPTER 28 System

This chapter provides information on the system screens.

28.1 System Overview

The system screens can help you configure general ZyWALL information, the system time and the console port connection speed for a terminal emulation program. The screens also allow you to configure DNS settings and determine which services/protocols can access which ZyWALL zones (if any) from which computers.

28.2 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 109 Command Summary: Host Name

COMMAND	DESCRIPTION
`[no] domainname` *`domain_name`*	Sets the domain name. The `no` command removes the domain name. *`domain_name:`* This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
`[no] hostname` *`hostname`*	Sets a descriptive name to identify your ZyWALL. The `no` command removes the host name.
`show fqdn`	Displays the fully qualified domain name.

28.3 Time and Date

For effective scheduling and logging, the ZyWALL system time must be accurate. The ZyWALL's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server.

28.3.1 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 110 Command Summary: Date/Time

COMMAND	DESCRIPTION
`clock date YYYY-MM-DD time HH:MM:SS`	Sets the new date in year, month and day format manually and the new time in hour, minute and second format.
`[no] clock daylight-saving`	Enables daylight saving. The `no` command disables daylight saving.
`[no] clock saving-interval begin {apr|aug|dec|feb|jan|jul|jun|mar|may|nov|oct|sep} {1|2|3|4|last} {fri|mon|sat|sun|thu|tue|wed} hh:mm end {apr|aug|dec|feb|jan|jul|jun|mar|may|nov|oct|sep} {1|2|3|4|last} {fri|mon|sat|sun|thu|tue|wed} hh:mm offset`	Configures the day and time when Daylight Saving Time starts and ends. The `no` command removes the day and time when Daylight Saving Time starts and ends. *offset*: a number from 1 to 5.5 (by 0.5 increments)
`clock time HH:MM:SS`	Sets the new time in hour, minute and second format.
`[no] clock time-zone {-|+hh}`	Sets your time zone. The `no` command removes time zone settings.
`[no] ntp`	Saves your date and time and time zone settings and updates the data and time every 24 hours. The `no` command stops updating the data and time every 24 hours.
`[no] ntp server {FQDN|W.X.Y.Z}`	Sets the IP address or URL of your NTP time server. The `no` command removes time server information.
`ntp sync`	Gets the time and date from a NTP time server.
`show clock date`	Displays the current date of your ZyWALL.
`show clock status`	Displays your time zone and daylight saving settings.
`show clock time`	Displays the current time of your ZyWALL.
`show ntp server`	Displays time server settings.

28.4 Console Port Speed

This section shows you how to set the console port speed when you connect to the ZyWALL via the console port using a terminal emulation program. The following table describes the console port commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 111 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.

28.5 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.

28.5.1 DNS Commands

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

Table 112 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: ge*x*, *x* = 1 - 5 virtual interface on top of Ethernet interface: ge*x*:*y*, *x* = 1 - 5, *y* = 1 - 12 VLAN interface: vlan*x*, *x* = 0 - 15 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 15, *y* = 1 - 12 bridge interface: br*x*, *x* = 0 - 11 virtual interface on top of bridge interface: br*x*:*y*, *x* = 0 - 11, *y* = 1 - 12 PPPoE/PPTP interface: ppp*x*, *x* = 0 - 11

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 113 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 cache.
[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..64>|append|insert <1..64>} access-group {ALL|*address_object*} zone {ALL|*address_object*} action {accept|deny}	Sets a service control rule for DNS requests.
ip dns server rule move <1..64> to <1..64>	Changes the number of a service control rule.
[no] ip dns server zone-forwarder {<1..32>|append|insert <1..32>} {*domain_name*|*} {interface *interface_name* |user-defined *W.X.Y.Z*}	Sets a zone forwarder record that specifies a DNS server's IP address. The `no` command deletes a zone forwarder record.
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..64>	Deletes a service control rule.
show ip dns server cache	Displays all DNS cache entries.
show ip dns server database	Displays all configured records.
show ip dns server status	Displays whether this service is enabled or not.

28.5.2 DNS Command Example

This command sets an A record that specifies the mapping of a fully qualified domain name (www.abc.com) to an IP address (210.17.2.13).

```
Router# configure terminal
Router(config)# ip dns server a-record www.abc.com 210.17.2.13
```

CHAPTER 29 System Remote Management

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

Note: To allow the ZyWALL to be accessed from a specified computer using a service, make sure you do not have a service control rule or to-ZyWALL rule to block that traffic.

29.1 Remote Management Overview

You may manage your ZyWALL from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (LAN&WAN&DMZ)
- DMZ only

To disable remote management of a service, deselect **Enable** in the corresponding service screen.

29.1.1 Remote Management Limitations

Remote management will not work when:

1. You have disabled that service in the corresponding screen.
2. The accepted IP address in the **Service Control** table does not match the client IP address. If it does not match, the ZyWALL will disconnect the session immediately.
3. There is a firewall rule that blocks it.

29.1.2 System Timeout

There is a lease timeout for administrators. The ZyWALL automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the ZyWALL for authentication again when the reauthentication time expires.

29.2 HTTP/HTTPS Commands

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

Table 114 Input Values for General HTTP/HTTPS 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.
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.

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 115 Command Summary: HTTP/HTTPS

COMMAND	DESCRIPTION
`[no] ip http authentication` *auth_method*	Sets an authentication method used by the HTTP/HTTPS server. The `no` command resets the authentication method used by the HTTP/HTTPS server to the factory default (`default`). *auth_method:* The name of the authentication method. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`[no] ip http port <1..65535>`	Sets the HTTP service port number. The `no` command resets the HTTP service port number to the factory default (80).
`[no] ip http secure-port <1..65535>`	Sets the HTTPS service port number. The `no` command resets the HTTPS service port number to the factory default (443).
`[no] ip http secure-server`	Enables HTTPS access to the ZyWALL web configurator. The `no` command disables HTTPS access to the ZyWALL web configurator.
`[no] ip http secure-server auth-client`	Sets the client to authenticate itself to the HTTPS server. The `no` command sets the client not to authenticate itself to the HTTPS server.
`[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.

Table 115 Command Summary: HTTP/HTTPS (continued)

COMMAND	DESCRIPTION
`[no] ip http secure-server force-redirect`	Redirects all HTTP connection requests to a HTTPS URL. The `no` command disables forwarding HTTP connection requests to a HTTPS URL.
ip http secure-server table {admin|user} rule {<1..64>|append|insert <1..64>} 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 <1..64> to <1..64>	Changes the index number of a HTTPS service control rule.
`[no] ip http server`	Allows HTTP access to the ZyWALL web configurator. The `no` command disables HTTP access to the ZyWALL web configurator.
ip http server table {admin|user} rule {<1..64>|append|insert <1..64>} 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 <1..64> to <1..64>	Changes the number of a HTTP service control rule.
no ip http secure-server table {admin|user} rule <1..64>	Deletes a service control rule for HTTPS service.
no ip http server table {admin|user} rule <1..64>	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.

29.2.1 HTTP/HTTPS Command Examples

This following example adds a service control rule that allowed an administrator from the computers with the IP addresses matching the Marketing address object to access the WAN zone using HTTP service.

```
Router# configure terminal
Router(config)# ip http server table admin rule append access-group
Marketing zone WAN action accept
```

This command sets an authentication method used by the HTTP/HTTPS server to authenticate the client(s).

```
Router# configure terminal
Router(config)# ip http authentication Example
```

This following example sets a certificate named MyCert used by the HTTPS server to authenticate itself to the SSL client.

```
Router# configure terminal
Router(config)# ip http secure-server cert MyCert
```

29.3 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.

29.3.1 SSH Implementation on the ZyWALL

Your ZyWALL supports SSH versions 1 and 2 using RSA and DSA authentication and four encryption methods (AES, 3DES, Archfour and Blowfish). The SSH server is implemented on the ZyWALL for remote management on port 22 (by default).

29.3.2 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ZyWALL over SSH.

29.3.3 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 116 Command Summary: SSH

COMMAND	DESCRIPTION
`[no] ip ssh server`	Allows SSH access to the ZyWALL CLI. The `no` command disables SSH access to the ZyWALL CLI.
`[no] ip ssh server cert` *`certificate_name`*	Sets a certificate whose corresponding private key is to be used to identify the ZyWALL for SSH connections. The `no` command resets the certificate used by the SSH server to the factory default (`default`). *`certificate_name:`* The name of the certificate. You can use up to 31 alphanumeric and ;‘~!@#$%^&()_+[]{}’,.=- characters.
`[no] ip ssh server port <1..65535>`	Sets the SSH service port number. The `no` command resets the SSH service port number to the factory default (22).

Table 116 Command Summary: SSH (continued)

COMMAND	DESCRIPTION
`ip ssh server rule {<1..64>|append|insert <1..64>} 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. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`ip ssh server rule move <1..64> to <1..64>`	Changes the index number of a SSH service control rule.
`[no] ip ssh server v1`	Enables remote management using SSH v1. The `no` command stops the ZyWALL from using SSH v1.
`no ip ssh server rule <1..64>`	Deletes a service control rule for SSH service.
`show ip ssh server status`	Displays SSH settings.

29.3.4 SSH Command Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using SSH service.

```
Router# configure terminal
Router(config)# ip ssh server rule 2 access-group Marketing zone WAN action
accept
```

This command sets a certificate (Default) to be used to identify the ZyWALL.

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

29.4 Telnet

You can configure your ZyWALL for remote Telnet access.

29.5 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 117 Command Summary: Telnet

COMMAND	DESCRIPTION
`[no] ip telnet server`	Allows Telnet access to the ZyWALL CLI. The `no` command disables Telnet access to the ZyWALL CLI.
`[no] ip telnet server port <1..65535>`	Sets the Telnet service port number. The `no` command resets the Telnet service port number back to the factory default (23).
ip telnet server rule {<1..64>|append|insert <1..64>} 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. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`ip telnet server rule move <1..64> to <1..64>`	Changes the index number of a service control rule.
`no ip telnet server rule <1..64>`	Deletes a service control rule for Telnet service.
`show ip telnet server status`	Displays Telnet settings.

29.5.1 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)#
```

29.6 Configuring FTP

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

29.6.1 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 118 Command Summary: FTP

COMMAND	DESCRIPTION
`[no] ip ftp server`	Allows FTP access to the ZyWALL. The `no` command disables FTP access to the ZyWALL.
`[no] ip ftp server cert` *`certificate_name`*	Sets a certificate to be used to identify the ZyWALL. The `no` command resets the certificate used by the FTP server to the factory default.
`[no] ip ftp server port <1..65535>`	Sets the FTP service port number. The `no` command resets the FTP service port number to the factory default (21).
`[no] ip ftp server tls-required`	Allows FTP access over TLS. The `no` command disables FTP access over TLS.
`ip ftp server rule {<1..64>|append|insert <1..64>} 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. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`ip ftp server rule move <1..64> to <1..64>`	Changes the index number of a service control rule.
`no ip ftp server rule <1..64>`	Deletes a service control rule for FTP service.
`show ip ftp server status`	Displays FTP settings.

29.6.2 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
========================================================================
```

29.7 SNMP

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

29.7.1 Supported MIBs

The ZyWALL supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

29.7.2 SNMP Traps

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

Table 119 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the ZyWALL is turned on or an agent restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.

Table 119 SNMP Traps (continued)

OBJECT LABEL	OBJECT ID	DESCRIPTION
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.

29.7.3 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 120 Command Summary: SNMP

COMMAND	DESCRIPTION
`[no] snmp-server`	Allows SNMP access to the ZyWALL. The `no` command disables SNMP access to the ZyWALL.
`[no] snmp-server community` *`community_string`* `{ro|rw}`	Enters up to 64 characters to set the password for read-only (ro) or read-write (rw) access. The `no` command resets the password for read-only (`ro`) or read-write (`rw`) access to the default.
`[no] snmp-server contact` *`description`*	Sets the contact information (of up to 60 characters) for the person in charge of the ZyWALL. The `no` command removes the contact information for the person in charge of the ZyWALL.
`[no] snmp-server enable {informs|traps}`	Enables all SNMP notifications (informs or traps). The `no` command disables all SNMP notifications (informs or traps).
`[no] snmp-server host {`*`W.X.Y.Z`*`} [`*`community_string`*`]`	Sets the IP address of the host that receives the SNMP notifications. The `no` command removes the host that receives the SNMP notifications.
`[no] snmp-server location` *`description`*	Sets the geographic location (of up to 60 characters) for the ZyWALL. The `no` command removes the geographic location for the ZyWALL.
`[no] snmp-server port <1..65535>`	Sets the SNMP service port number. The `no` command resets the SNMP service port number to the factory default (`161`).
`snmp-server rule {<1..64>|append|insert <1..64>} 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. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`snmp-server rule move <1..64> to <1..64>`	Changes the index number of a service control rule.

Table 120 Command Summary: SNMP (continued)

COMMAND	DESCRIPTION
`no snmp-server rule <1..64>`	Deletes a service control rule for SNMP service.
`show snmp status`	Displays SNMP Settings.

29.7.4 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
```

CHAPTER 30
Logs

This chapter provides information about the ZyWALL's logs.

The following table displays the maximum number of system log messages in the ZyWALL.

Table 121 Specifications: Logs

LABEL	DESCRIPTION
Maximum Number of Log Messages (System Log)	512
Maximum Number of Log Messages (Debug Log)	1024

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.

30.1 Log Commands Summary

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

Table 122 Input Values for Log Commands

LABEL	DESCRIPTION
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.

The following sessions list the logging commands.

30.1.1 Log Entries Commands

This table lists the commands to look at log entries.

Table 123 logging Commands: Log Entries

COMMAND	DESCRIPTION
show logging entries [priority *pri*] [category *module_name*] [srcip *ip*] [dstip *ip*] [service *service_name*] [begin <1..512> end <1..512>] [keyword *keyword*]	Displays the selected 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 selected fields in the system log. *field*: time | msg | src | dst | note | pri | cat | all

30.1.2 System Log Commands

This table lists the commands for the system log settings.

Table 124 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.
clear logging system-log buffer	Clears the system log.

30.1.2.1 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 , account           : normal ,
    port-grouping      : normal , force-auth        : normal ,
    traffic-log        : no     , file-manage       : normal ,
    default            : all    ,
```

30.1.3 Debug Log Commands

This table lists the commands for the debug log settings.

Table 125 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`*`] [dstip` *`ip`*`] [service` *`service_name`*`] [begin <1..512> end <1..512>] [keyword` *`keyword`*`]`	Displays the selected entries in the debug 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 selected fields in the debug log. *field*: time | msg | src | dst | note | pri | cat | all
`[no] logging debug suppression`	Enables log consolidation in the debug log. The `no` command disables log consolidation in the debug log.
`[no] logging debug suppression interval <10..600>`	Sets the log consolidation interval for the debug log. The `no` command sets the interval to ten.
`clear logging debug buffer`	Clears the debug log.

This table lists the commands for the remote syslog server settings.

Table 126 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.

30.1.4 E-mail Profile Commands

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

Table 127 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> 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.

Table 127 logging Commands: E-mail Profile Settings (continued)

COMMAND	DESCRIPTION
[no] logging mail <1..2> {send-log-to | send-alerts-to} *e_mail*	Sets the e-mail address for logs or alerts. The no command clears the specified field. *e_mail*: You can use up to 63 alphanumeric characters, underscores (_), or dashes (-), and you must use the @ character.
[no] logging mail <1..2> subject *subject*	Sets the subject line when the ZyWALL mails to the specified e-mail profile. The no command clears this field. *subject*: You can use up to 60 alphanumeric characters, underscores (_), dashes (-), or !@#$%*()+=;:’,./ characters.
[no] logging mail <1..2> category *module_name* level {alert | all}	Specifies what kind of information is logged for the specified category. The no command disables logging for the specified category.
[no] logging mail <1..2> schedule {full | hourly}	Sets the e-mail schedule for the specified e-mail profile. The no command clears the schedule field.
logging mail <1..2> schedule daily hour <0..23> minute <0..59>	Sets a daily e-mail schedule for the specified e-mail profile.
logging mail <1..2> schedule weekly day *day* hour <0..23> minute <0..59>	Sets a weekly e-mail schedule for the specified e-mail profile. *day*: sun | mon | tue | wed | thu | fri | sat

30.1.4.1 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
```

30.1.5 Console Port Logging Commands

This table lists the commands for the console port settings.

Table 128 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.

CHAPTER 31
Reports and Reboot

This chapter provides information about the report associated commands and how to restart the ZyWALL using commands.

31.1 Report Commands Summary

The following sections list the report and session commands.

31.1.1 Report Commands

This table lists the commands for reports.

Table 129 report Commands

COMMAND	DESCRIPTION
`[no] report`	Begins data collection. The `no` command stops data collection.
`show report status`	Displays whether or not the ZyWALL is collecting data and how long it has collected data.
`clear report [`*`interface_name`*`]`	Clears the report for the specified interface or for all interfaces.
`show report [`*`interface_name`*` {ip | service | url}]`	Displays the traffic report for the specified interface and controls the format of the report. Formats are: `ip` - traffic by IP address and direction `service` - traffic by service and direction `url` - hits by URL

31.1.2 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
```

31.1.3 Session Commands

This table lists the command to display the current sessions.

Table 130 session Commands

COMMAND	DESCRIPTION
`show conn [user` *`username`*`] [service` *`service-name`*`] [source` *`ip`*`] [destination` *`ip`*`] [begin <1..128000>] [end <1..128000>]`	Displays information about the selected sessions or about all sessions. You can select sessions by user name, service object, source IP, destination IP, or session number(s).
`show conn status`	Displays the number of active sessions.

31.2 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.

CHAPTER 32
Packet Trace and Traceroute

This chapter introduces the `packet-trace` and `traceroute` commands.

Table 131 Diagnostic Commands

COMMAND	DESCRIPTION
packet-trace [interface *interface_name*] [ip-proto {<0..255> | *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*] trace-route {*ip* | *hostname*}	Sends traffic through the specified interface with the specified protocol, source address, destination address, and/or port number. If you specify `file`, the ZyWALL dumps the traffic to `/packet_trace/packet_trace_interface`. Use FTP to retrieve the files (see Section 4.6 on page 60). If you do not assign the duration, the ZyWALL keeps dumping traffic until you use Ctrl-C. Use the extension filter to extend the use of this command. *protocol_name*: You can use the name, instead of the number, for some IP protocols, such as `tcp`, `udp`, `icmp`, and so on. The names consist of 1-16 alphanumeric characters, underscores (_), 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` when you want to return to the prompt.

Some 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  * * *
```

Command Index