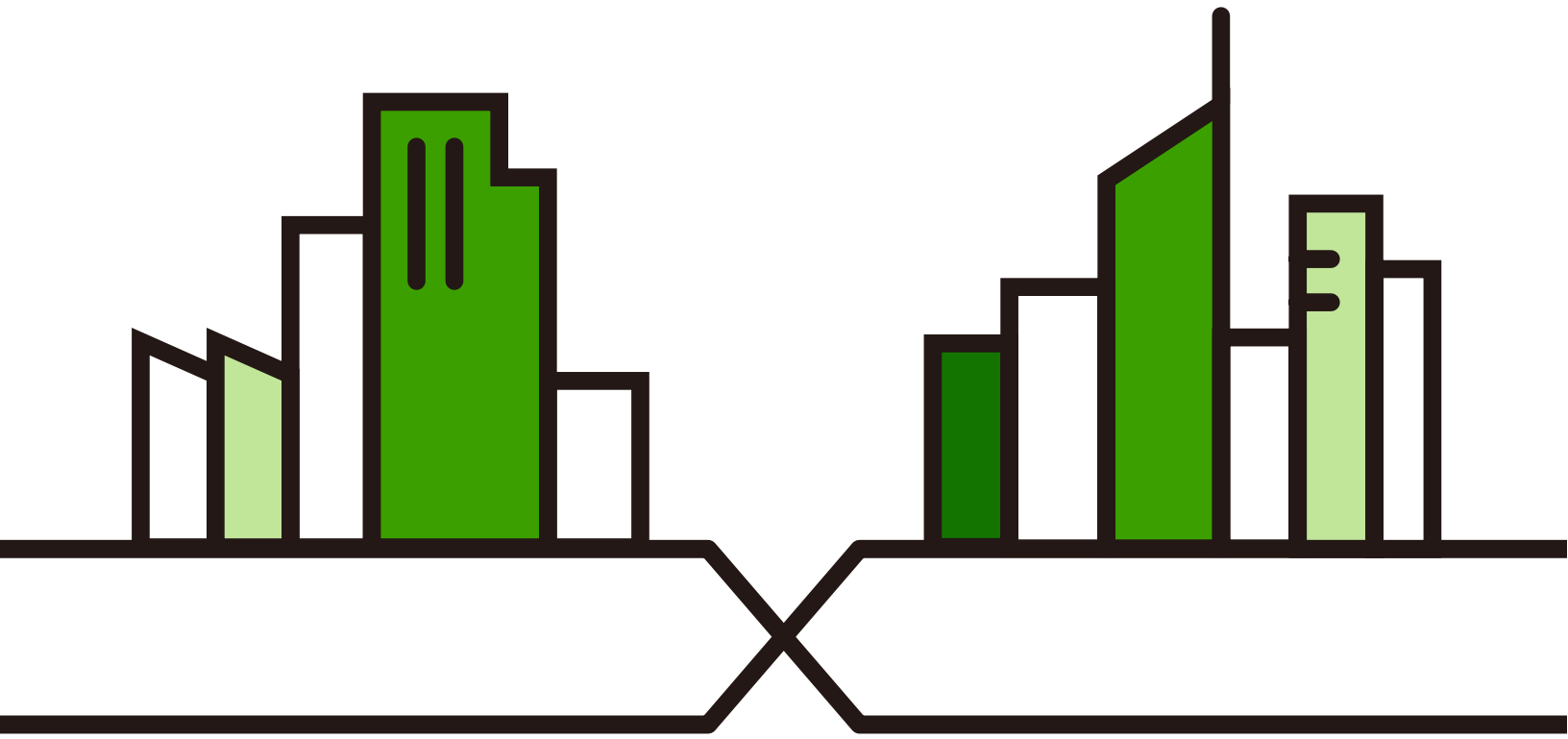
ZYXEL NETWORKS

CLI Reference Guide

USG FLEX H Series

Default Login Details	
IP Address	192.168.168.1
User Name	admin
Password	See Zyxel Device label or 1234
LAN	P3 or P4
WAN	P1 or P2

Version 1.20 Ed. 1, 5/2024



IMPORTANT!
READ CAREFULLY BEFORE USE.
KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a Reference Guide for a series of products intended for people who want to configure the Zyxel Device via Command Line Interface (CLI).

Note: The version number on the cover page refers to the latest firmware version supported by the Zyxel Device at the time of writing.

How To Use This Guide

Read Chapter 1 on page 16 for how to access and use the CLI (Command Line Interface).

Some commands or command options in this guide may not be available in your product. See your product's User's Guide for a list of supported features.
Do not use commands not documented in this guide. Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.
Some commands may be renamed in a firmware upgrade. In cases where a command has multiple names, the Reference Guide lists each variation.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the Zyxel Device and access the Web Configurator.

- User's Guide

  The USG FLEX H Series User Guides explain how to use the Web Configurator to configure the Zyxel Device. It also shows the product feature matrix for each device. General feature differences are written in the Introduction chapter while a more detailed table is in the Product Feature appendix.

- Online Help

  Click the help icon in the web configurator to access the latest online help with machine translation available.

Note: It is recommended you use the Web Configurator to configure the Zyxel Device.

- More Information

  Go to **support.zyxel.com** to find other information on Zyxel Device.

Contents Overview

Table of Contents

PART I
Introduction

CHAPTER 1
Command Line Interface

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

1.1 Overview

Zyxel Device refers to these models.

- ZyWALL USG FLEX
    - USG FLEX 100H
    - USG FLEX 100HP
    - USG FLEX 200H
    - USG FLEX 200HP
    - USG FLEX 500H
    - USG FLEX 700H

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

Use of undocumented commands or misconfiguration can damage the Zyxel Device and possibly render it unusable.

1.1.1 The Configuration File

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

You can perform the following with a configuration file:

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

Note: The Zyxel Device might force you to log out of your session if re-authentication time, lease time, or idle timeout is reached. See Chapter 24 on page 165 for more information about these settings.

1.2.1 Console Port

The default settings for the console port are as follows.

Table 1 Managing the Zyxel Device: Console Port

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

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

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

Figure 1 Console Port Power-on Display

```
U-Boot 2018.03-7.1.0-svn568 (Dec 30 2023 - 10:23:14 +0800)



BootModule Version: V1.03 Dec 30 2020 10:23:14
DRAM: Size = 4096 Mbytes

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

After the initialization, the login screen displays.

Figure 2 Login Screen

```
Welcome to USG FLEX 200HP

usgflex200hp login:
```

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 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.

Before connecting, do the following:

- Using the Web Configurator, enable SSH at **System > Settings > SSH**.
- To allow the SSH protocol from your remote computer to the Zyxel Device, add **SSH** to the service group **Default_Allow_WAN_To_ZyWALL** at **Object > Service > Service Group.** This group defines which services are allowed in the default **WAN_to_Device** security policy.

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

Figure 3 SSH Login Example

```
C:\>ssh admin@192.168.168.1
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_192.168.168.1.pub
host key for 192.168.168.1, accepted by user Tue Aug 09 2005 07:38:28
admin's password:
Authentication successful.
```

1.3 How to Find Commands in this Guide

You can search for a command, look for the command in the feature chapter or find the command in the List of Commands (Alphabetical) at the end of the guide. This section lists the commands in alphabetical order that they appear in this guide.

1.4 How Commands Are Explained

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

1.4.1 Background Information (Optional)

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

1.4.2 Command Input Values (Optional)

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

1.4.3 Command Summary

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

1.4.4 Command Examples (Optional)

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

1.4.5 Command Syntax

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

- A command or keyword in courier new must be entered literally as shown. Do not abbreviate.
- Values that you need to provide are in *italics*.
- Required fields that have multiple choices are enclosed in curly brackets {}.
- A range of numbers is enclosed in angle brackets <>.
- Optional fields are enclosed in square brackets [].
- The | symbol means OR in a list of choices or can be used as a switch in a command, such as show config running | no-pager.

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

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

1. Enter object service-object service exactly as it appears.
2. Enter the name of the object where you see *service-name.*
3. Enter tcp or udp, depending on the service object you want to create.
4. Enter two numbers between 1 and 65535.

1.4.6 Changing the Password

It is highly recommended that you change the password for accessing the Zyxel Device. See Section 24.2 on page 165 for the appropriate commands.

1.4.7 Idle Timeout

See Section 24.3 on page 166 for commands on changing the default logout time when no activity is recorded.

1.5 CLI Modes

You run CLI commands is User Mode or Edit (Staging Configuration) Mode.

After you log into the Zyxel Device, you will see this prompt `usgflex200hp>` in User Mode.

Type `edit running` and you will see this prompt `usgflex200hp running config#` in Edit mode to configure settings that are currently running on the Zyxel Device.

In Edit mode, commands are not applied to the running configuration yet. You can configure several commands in this mode, then use the Diff command to see all the commands you edited at all levels. Review, revise or remove (`del /vrf main interface`) any wrong commands before using `commit` to save all the edited commands to the running configuration.

Note: You lose all edited commands if you exit Edit mode before using `commit`.

After you commit, the changed commands are saved in the running configuration, but not the startup configuration.

Note: You must copy the running configuration to the startup configuration to retain commands after the Zyxel Device restarts - use the command `copy running startup`.

This is a summary of the modes.

Table 2 CLI Modes

	USER MODE	EDIT (STAGING CONFIGURATION) MODE	EDIT SUB-COMMAND
What **Admin** users can do	• Look at system information (like the **Dashboard** screen) and settings. • Run basic diagnostics.	• Configure simple features such as an address object. • Create or remove general features such as an interface.	• Configure specific parts of a feature such as a particular interface on the Zyxel Device.
How you enter it	Type username and password to log into the Zyxel Device.	Type **edit running**	Type the command used to enter the specific part of the feature at the **Configuration** level.

What the prompt looks like	`usgflex200hp>`	`usgflex200hp running config#`	(varies by part)
			`usgflex500h running vrf main#`
			`usgflex200hp running allow-list ...`

How you exit it	N/A	Type **exit**.	Type **exit**.

1.6 CLI Levels

The CLI has various levels of commands such as:

- root
- vrf main
- interface
- ethernet ge1

Type '/' to go to the root level

Type show config full path to display the full path for each command.

Type pwd to print out current path

Type '..' to go back one level.

1.7 CLI Tips

Use the resize command to change the width of your terminal emulation software screen (such as Tera Term) to view complete commands in a single row.

Use no-pager to display all the results of a command at once. The default is to display one page a time ending with ':'. You then press any key to continue the display.

- To disable paging for a specific command, use the no-pager switch in the command. For example, show config running | no-pager.
- To disable paging for all commands in a CLI session, use the following command: cliconfig pager enabled false
- Type Q or CTRL-C to exit the pager display.

Type show interface to see the IP address of interfaces on the Zyxel Device.

Type show version to see the current firmware version on the Zyxel Device.

Type show config text or json or xml to see the current configuration in text, JSON or XML format.

show config displays the configuration settings, while show state displays the run time state of the configuration. As a result, show state generally includes the items in show config, plus additional runtime information. This is an example.

Figure 4 show config Vs show state

```
usgflex200hp> show config nebula
nebula
    enabled true
usgflex200hp> show state nebula
nebula
    enabled true
    callhome-status Connected
```

Type `vrf main secure-policy enabled false` to disable all security policies.

Note: This is only recommended for temporary remote access or debugging of the Zyxel Device

1.8 CLI Structure

- Type `cmd` to have the Zyxel Device execute actions, such as pinging the specified IP address or rebooting.

Figure 5 `cmd` Command Example

```
usgflex200hp> cmd ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=7.41 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=9.90 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=10.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=17.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=114 time=8.64 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=114 time=8.43 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=114 time=7.58 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=114 time=7.26 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=114 time=8.20 ms
^C
--- 8.8.8.8 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8011ms
rtt min/avg/max/mdev = 7.255/9.531/17.651/3.068 ms
```

- Type `show state` to displays the status of the settings you configured that will effect the Zyxel Device and your network.

Figure 6 `show state` Command Example

```
usgflex200hp> show state two-factor-auth admin-access enabled
enabled true
```

- Type `show config` to displays the settings currently running on the Zyxel Device.

Figure 7 `show config` Command Example

```
usgflex200hp> show config object user-object admin
admin admin
    role admin
    enabled true
    logon-lease-time default
    logon-reauth-time default
    password $8$xdvd0Uhn$xVzlMpHy$LCoIrGtNtuQ8bdaw/3Mvq/
WXW1KwWiHTA+3HWjHV8xgmP7NLCjGwKkgyQaALJnDsg7trI9FVfHKJYcr9fDSCOZDnWM2bPHVjK
4XKbf+uNDoE/
l3vYcnQiOJATc2af7T89oLX+xEv5+vjBZMhWU8wP8f1056wg7ChqrpjHyhNN615WhLBxvck9x3b
ZrtuEFVjofJuazB+GgLxdqJiaF1YtKJTkEeXESKkZ5C0aEonzZF3SRinfKIXvWvHd8ketnn9Xpf
raYS6lSpqvM4Duqy+KeTmQCKth9zXURh4DV7f9Ixz7/PD97ZS3ZFo/
kNbLRX7vMMTf8bRTzm7Z2cJ2r+IT0oEIcg7Emu7NKJh/BBsOh8$
```

- Type `vrf main` to configure the Zyxel Device Internet and Internet related settings, such as the anti-malware settings or the interface settings.

Figure 8 vrf main Command Example

```
usgflex200hp> edit running
usgflex200hp running config# vrf main anti-malware
default-profile    statistics         eicar-detection    cloud-query
allow-list
block-list         default-port       enabled            scan-mode
usgflex200hp running config# vrf main anti-malware enabled true
```

- Use the commit command to apply changes to the configuration file that is currently running on the Zyxel Device.

Note: Always apply (commit) the changes you made to the running configuration file before you exit the configuration mode. All changes that are not applied will be lost after you log out of the configuration mode.

Note: Always save the changes you made in the running configuration file to the start up configuration file (startup-config.conf) before you reboot the Zyxel Device. Changes that are not saved to the start up configuration file will be lost after you reboot the Zyxel Device.

Figure 9 commit Command Example

```
usgflex200hp running config# object user-object admin admin role admin
usgflex200hp running config# commit
Configuration committed.
```

- Enter the exit command in the configuration or sub-command mode to go to the admin mode.

  Enter the exit command in the admin mode to log out of the CLI.

Figure 10 exit Command Example

```
usgflex200hp running config# exit
usgflex200hp> exit

Welcome to USG FLEX 200HP

usgflex200hp login:
```

1.9 Shortcuts and Help

See the following sections for the shortcuts and help you can use the CLI.

1.9.1 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 11 Help: Available Commands Example 1

```
usgflex200hp>?
  cliconfig             Enable/disable pager for this session.
  cmd                   Send a command.
  copy                  Copy a configuration into another one.
  diff                  Diff configurations.
  echo                  Echo arguments.
  edit                  Edit configuration.
  exec                  Execute a cli script file.
  exit                  Quit the cli.
  export                Export a configuration file.
  flush                 Flush objects.
  help                  Show the help.
  import                Import a configuration file.
  netconf              NETCONF related commands: connect, disconnect, status.
  remove                Remove a configuration file.
  resize                Resize terminal.
  show                  Show configuration or system state.
  validate              Validate a configuration.
```

Figure 12 Help: Available Command Example 2

```
usgflex200hp>show ?
  absolute              Select display path mode (default: relative).
  all                   Select display mode (default: all).
  config                Show the configuration.
  dry-run               Display NETCONF RPC instead of sending it.
  fullpath              Select display path mode (default: relative).
  json                  Select display format (default: text).
  nodefault             Select display mode (default: all).
  relative              Select display path mode (default: relative).
  state                 Show the system state.
  text                  Select display format (default: text).
  with-deprecated      Show deprecated nodes, which are by default hidden in
                        show text state.
  xml                   Select display format (default: text).

  alg ftp               Show configuration or system state.
  app-patrol-applications
                        Show app patrol applications
  app-patrol-categories
                        Show app patrol categories
  app-patrol-signature-version
                        Show app patrol signature version
  bfd                   Show BFD information.
  bgp                   Show BGP information.
```

1.9.2 List of Sub-commands or Required User Input

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

Figure 13 Help: Required User Input Example

```
usgflex200hp running config# switch 0 port ?
  port                  Set value of configuration leaves.
  port-grouping         Set value of configuration leaves.
```

Figure 14 Help: Sub-command Information Example

```
usgflex200hp running vrf main# anti-malware allow-list logging ?
  log                   Default: no.
                        allow list log setting
  no                    Default: no.
                        allow list log setting
```

1.9.3 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 Zyxel Device automatically display the full command.

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

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

Figure 15 Non-Unique Partial Command Example

```
usgflex200hp> e [TAB]
echo      exec      exit      edit      export
usgflex200hp> ex [TAB]
exec      exit      export
```

1.9.4 Entering a ? in a Command

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

1.9.5 Command History

The Zyxel Device 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].

1.9.6 Navigation

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

1.9.7 Erase Current Command

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

1.10 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>.

```
usgflex200hp> edit running
usgflex200hp running config# object user-object admin admin description
  <description>        Description string.
```

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

Table 3 Input-Value Formats for Strings in CLI Commands

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

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

TAG	# VALUES	LEGAL VALUES
domain name	Used in content filtering	
	0+	lower-case letters, numbers, or .-
	Used in ip dns server	
	0-247	alphanumeric or .- first character: alphanumeric or -
	Used in domainname, ip dhcp , and ip domain	
	0-254	alphanumeric or ._- first character: alphanumeric or -
email	1-63	alphanumeric or .@_-
e-mail	1-64	alphanumeric or .@_-
encryption key	16-64 8-32	“0x” or “0X” + 16-64 hexadecimal values alphanumeric or ;|`~!@#$%^&*()_+\\{}':,./<>=-
file name	0-31	alphanumeric or _-
filter extension	1-256	alphanumeric, spaces, or '()+,/:=?;!*#@$_%.-
fqdn	Used in ip dns server	
	0-252	alphanumeric or .- first character: alphanumeric or -
	Used in ip ddns, time server, device HA, VPN, certificates, and interface ping check	
	0-254	alphanumeric or .- first character: alphanumeric or -
full file name	0-256	alphanumeric or _/.-
hostname	Used in hostname command	
	0-63	alphanumeric or .-_ first character: alphanumeric or -
	Used in other commands	
	0-252	alphanumeric or .- first character: alphanumeric or -
import configuration file	1-26+”.conf”	alphanumeric or ;`~!@#$%^&()_+[]{}',.=- add “.conf” at the end
import shell script	1-26+”.zysh”	alphanumeric or ;`~!@#$%^&()_+[]{}',.=- add “.zysh” at the end
initial string	1-64	alphanumeric, spaces, or '()+,/:=!*#@$_%-.&
isp account password	0-63	alphanumeric or `~!@#$%^&*()_\-+={}|\;:'<,>./
isp account username	0-30	alphanumeric or -_@$./

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

TAG	# VALUES	LEGAL VALUES
ipv6_addr		An IPv6 address. The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address 2001:0db8:1a2b:0015:0000:0000:1a2f:0000. IPv6 addresses can be abbreviated in two ways: Leading zeros in a block can be omitted. So 2001:0db8:1a2b:0015:0000:0000:1a2f:0000 can be written as 2001:db8:1a2b:15:0:0:1a2f:0. Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So 2001:0db8:0000:0000:1a2f:0000:0000:0015 can be written as 2001:0db8::1a2f:0000:0000:0015, 2001:0db8:0000:0000:1a2f::0015, 2001:db8::1a2f:0:0:15 or 2001:db8:0:0:1a2f::15.
key length	--	512, 768, 1024, 1536, 2048, 4096
license key	25	"S-" + 6 upper-case letters or numbers + "-" + 16 upper-case letters or numbers
mac address	--	aa:bb:cc:dd:ee:ff (hexadecimal)
mail server fqdn		lower-case letters, numbers, or -.
name	1-31	alphanumeric or _-
notification message	1-81	alphanumeric, spaces, or '()+,/:=?;!*#@$_%-
password: less than 15 chars	1-15	alphanumeric or `~!@#$%^&*()_\-+={}|\;:'<,>./
password: less than 8 chars	1-8	alphanumeric or ;/?:@&=+$\.-_!~*'()%,#$
password	Used in user and ip ddns	
	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<,>./
	Used in e-mail log profile SMTP authentication	
	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<>./
	Used in device HA synchronization	
	1-63	alphanumeric or ~#%^*_-={}:,.
	Used in registration	
	6-20	alphanumeric or .@_-
phone number	1-20	numbers or ,+
preshared key	16-64	"0x" or "0X" + 16-64 hexadecimal values alphanumeric or ;|`~!@#$%^&*()_+\{}':,./<>=-
profile name	0-30	alphanumeric or _- first character: letters or _-
proto name	1-16	lower-case letters, numbers, or -
protocol name	0-30	alphanumeric or _- first character: letters or _-
quoted string less than 127 chars	1-255	alphanumeric, spaces, or ;/?:@&=+$\.-_!~*'()%,

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

TAG	# VALUES	LEGAL VALUES
quoted string less than 63 chars	1-63	alphanumeric, spaces, or ;/?:@&=+$\.-_!~*'()%
quoted string	0+	alphanumeric, spaces, or punctuation marks enclosed in double quotation marks (“) must put a backslash (\) before double quotation marks that are part of input value itself
service name	0-63	alphanumeric or -_@$./
spi	2-8	hexadecimal
string less than 15 chars	1-15	alphanumeric or -_
string: less than 63 chars	1-63	alphanumeric or `~!@#$%^&*()_-+={}|\;:'<,>./
string	1+	alphanumeric or -_@
subject	1-61	alphanumeric, spaces, or '()+,./:=?;!*#@$_%-
system type	0-2	hexadecimal
timezone [-+]*hh*	--	-12 through +12 (with or without “+”)
url	1-511	alphanumeric or '()+,/:.=?;!*#@$_%-
url	Used in content filtering redirect	
	“http://”+ “https://”+	alphanumeric or ;/?:@&=+$\.-_!~*'()%, starts with “http://” or “https://” may contain one pound sign (#)
	Used in other content filtering commands	
	“http://”+	alphanumeric or ;/?:@&=+$\.-_!~*'()%, starts with “http://” may contain one pound sign (#)
user name	Used in VPN extended authentication	
	1-31	alphanumeric or _-
	Used in other commands	
	0-30	alphanumeric or _- first character: letters or _-
username	6-20	alphanumeric or .@_- registration
user name	1+	alphanumeric or -_. logging commands
user@domainname	1-80	alphanumeric or .@_-
vrrp group name: less than 15 chars	1-15	alphanumeric or _-
week-day sequence, i.e. 1=first,2=second	1	1-4
xauth method	1-31	alphanumeric or _-

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

TAG	# VALUES	LEGAL VALUES
xauth password	1-31	alphanumeric or ;|`~!@#$%^&*()_+\{}':,./<>=-
mac address	0-12 (even number)	hexadecimal for example: aa aabbcc aabbccddeeff

1.11 Ethernet Interfaces

At the time of writing, Zyxel Devices use ge*x*, *x* = 1~N, where N equals the highest numbered Ethernet interface on your Zyxel Device, as the name for the Ethernet interface.

1.12 Resetting the Zyxel Device

If you cannot access the Zyxel Device by any method, try restarting it by turning the power off and then on again. If you still cannot access the Zyxel Device by any method or you forget the administrator password(s), you'll have to reset the Zyxel Device to its factory-default settings. Any configuration files or shell scripts that you saved on the Zyxel Device should still be available afterwards.

1.13 Fast-path Acceleration

Fast-path Acceleration is a way to speed up certain traffic such as NAT, IPSec VPN, Security policies through the ZD by bypassing the kernel. SSL VPN traffic does not use fast-path acceleration.

1.13.1 Load Balancing

Enable Load Balancing to improve the processing of large volumes of encrypted traffic, such as VPN traffic.

Note: This is NOT the same as traffic load balancing using weighted round robin, least load first or the spillover algorithms.

Encrypted traffic processing is done by distributing incoming Encapsulating Security Payload (ESP) packets across different CPUs for decoding. Use these commands to enable Load Balancing and see the status.

Figure 16 Enable Encrypted Traffic Balancing

```
usgflex500h> edit running
usgflex500h running config# system fast-path-esp-rx-loading-balance enabled true
usgflex500h running config# commit
Configuration committed.
usgflex500h running config# show system fast-path esp-rx-loading-balance status
show-system-fast-path-esp-rx-loading-balance-status
    status Enabled
```

You may disable Load Balancing if your network does not have a lot of VPN traffic, or if certain data must be processed on the same CPU core or if you want to simplify the network architecture for troubleshooting.

Figure 17 Disable Encrypted Traffic Balancing

```
usgflex500h> edit running
usgflex500h running config# system fast-path-esp-rx-loading-balance enabled false
usgflex500h running config# commit
Configuration committed.
usgflex500h running config# show system fast-path esp-rx-loading-balance status
show-system-fast-path-esp-rx-loading-balance-status
    status Disabled
```

1.14 Nebula Restart

Nebula Cloud center is a cloud-based management tool. Use this command if your Zyxel Device is managed by Nebula and has connection problems with Nebula. This command will restart the connection.

Figure 18 Nebula Restart

```
usgflex500h> edit running
usgflex500h running config# cmd debug nebula callhome restart
debug-nebula-callhome-restart
    ok
```

1.15 Management Logs

Use this command to display a certain number of the latest management logs. The logs include:

- Booting time and from which partition
- When and how firmware was upgraded

Figure 19 Management Log

```
usgflex500h> edit running
usgflex500h running config# cmd debug show sys-mgnt-log max-lines <number>
```

This is an example.

Figure 20 System Logs

```
usgflex500h running config# cmd debug show sys-mgnt-log max-lines 10
[2024-04-01 17:14:04][2][1.20(ABZH.0)b5s1][CGI][file_upload] Firmware upgrading,
partition:1
[2024-04-01 17:17:51][1][1.20(ABZH.0)b6] Booting time: 146 seconds (70 services
loaded)
[2024-04-11 10:36:57][1][1.20(ABZH.0)b6][FTP] Firmware upgrading, file: /db/etc/
zyxel/ftp/firmware1/120ABZH0b6s1.bin
[2024-04-11 10:40:31][1][1.20(ABZH.0)b6s1] Booting time: 143 seconds (71 services
loaded)
[2024-04-15 15:27:44][1][1.20(ABZH.0)b6s1][CGI][file_upload] Firmware upgrading,
partition:2
[2024-04-15 15:31:24][2][1.20(ABZH.0)b7] Booting time: 148 seconds (70 services
loaded)
[2024-04-16 10:23:27][2][1.20(ABZH.0)b7][CGI][file_upload] Firmware upgrading,
partition:1
[2024-04-16 10:27:06][1][1.20(ABZH.0)] Booting time: 148 seconds (70 services
loaded)
[2024-04-23 10:22:00][1][1.20(ABZH.0)][CGI][file_upload] Firmware upgrading,
partition:2
[2024-04-23 10:25:43][2][1.20(ABZH.0)] Booting time: 149 seconds (70 services
loaded)
usgflex500h running config#
```

1.16 Kernel Console Level

Use this command to display the kernel console log level. All Kernel messages with a log level smaller than the console log level will be printed to the console command line interface. The log levels are defined as follows:

Table 4 Kernel Log Console

0 (KERN_EMERG)	System is unusable
1 (KERN_ALERT)	Action must be taken immediately
2 (KERN_CRIT)	Critical conditions
3 (KERN_ERR)	Error conditions
4 (KERN_WARNING)	Warning conditions
5 (KERN_NOTICE)	Normal but significant condition
6 (KERN_INFO)	Informational
7 (KERN_DEBUG)	Debug-level messages

The default log level is 1, so only KERN_EMERG and KERN_ALERT log types are printed to the console command line interface.

Figure 21 Kernel Log Console

```
usgflex500h> edit running
usgflex500h running config# cmd debug kernel console-level show
kernel console-level: 1
usgflex500h running config#
```

PART II
Reference

CHAPTER 2
Object Reference

This chapter describes how to use object reference commands.

2.1 Object Reference Commands

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

Table 5 show reference Commands

COMMAND	DESCRIPTION
show reference object address [*object_name*]	Displays which configuration settings reference the specified address object.
show reference object address-group [*object_name*]	Displays which configuration settings reference the specified address group object.
show reference object service [*object_name*]	Displays which configuration settings reference the specified service object.
show reference object service-group [*object_name*]	Displays which configuration settings reference the specified service group object.
show reference object schedule [*object_name*]	Displays which configuration settings reference the specified schedule object.
show reference object schedule-group [*object_name*]	Displays which configuration settings reference the specified schedule group object.
show reference object zone [*object_name*]	Displays which configuration settings reference the specified zone object.
show reference object user [*username*]	Displays which configuration settings reference the specified user object.
show reference object user-group [*username*]	Displays which configuration settings reference the specified user group object.
show reference object {aaa-radius| aaa-ldap| aaa-ad} [*object_name*]	Displays which configuration settings reference the specified AAA RADIUS, AAA LDAP or AAA AD group object.
show reference profile {app-patrol| content-filter| dos-prevention| ssl-inspection| certManager}	Displays which configuration settings reference the specified: • App patrol profile. • Content filter profile. • DoS prevention profile. • SSL inspection profile. • Certificate profile.

2.1.1 Object Reference Command Example

This example shows how to check which configuration is using the HTTP service.

```
usgflex200hp> show reference object service HTTP
show-reference-object
    ok
        reference 1
            category "Service Group"
            sub_category ""
            priority ""
            rule_name Default_Allow_WAN_To_ZyWALL
            description ""
```

CHAPTER 3
Status

This chapter explains some commands you can use to display information about the Zyxel Device's current operational state.

Table 6 Status Show Commands

COMMAND	DESCRIPTION
show config	Displays the settings you configured.
show state	Displays the status of the specified settings.
show all	Displays all settings in the specified category.
show fullpath	Displays all settings in the specified category.
show bgp	Displays border gateway protocol (BGP) information.
show object	Displays the Zyxel Device zones.
show geo-ip	Displays the Geo IP database and country list.
show cloud-helper	Displays cloud helper firmware information and download status.
show debug myzyxel-server status	Displays myzyxel server status.
show fast-path	Displays fast-path memory, cpu-usage, table-usage and service statistics.
show interface	Displays the Zyxel Device interfaces information.
show certificate	Displays the Zyxel Device certificates information.
show filter	Displays the protocols list.
show ntp	Displays network time protocol (NTP) information.
show port	Displays the Zyxel Device ports status.
show firmware	Displays the Zyxel Device firmware and reboot options.
show gui dashboard boot-status	Displays when the Zyxel Device was last updated with new firmware. For example, 'status OK. detail "Firmware update at 2024-02-02 09:31"'
show certManager	Displays the Zyxel Device SSL certificate.
show reference	Displays which configuration settings reference a specific object.
show logging	Displays the logs.
show summary	Displays a summary of the Zyxel Device system status.
show conntracks	Displays connection tracking records.
show product	Displays the Zyxel Device model name and firmware version.
show date	Displays the current date of your Zyxel Device.
show neighbors	Displays neighbors information.
show ipv4-routes	Displays the IPv4 routing table.
show ospf	Displays OSPFv2 information.
show dhcp-server	Displays the DHCP unique identifier (DUID).
show dns-server	Displays DNS server information.

Table 6 Status Show Commands

COMMAND	DESCRIPTION
show ike	Displays security association (SA) status.
show log	Displays log information.
show rip	Displays RIP information.
show version	Displays the Zyxel Device firmware information.
show users	Displays the Zyxel Device user accounts information.
show lockout-users	Displays the user accounts that are locked out of the Zyxel Device.
show service-inspect	Displays the services available on the Zyxel Device.
show mac	Displays the Zyxel Device MAC address.
show serial-number	Displays the serial number of this Zyxel Device.
show system traffic-statistics-chart summary host_ip filter application <application name>	Displays traffic statistics in a chart by application.
show system traffic-statistics-chart summary application range begin <1 - 1000> end <1 - 1000>	Displays traffic statistics in a chart by range of traffic size.
show system traffic-statistics summary host_ip filter application <application name>	Displays traffic statistics summary of host IP addresses by application.
show system traffic-statistics summary host_ip range begin <1 - 1000> end <1 - 1000>	Displays traffic statistics summary of host IP addresses by range of IP addresses.
show system database status	Displays the number of traffic sessions that went through the Zyxel Device and the file size in the database. for example, “session_count 10000, db_usage "7673 kB”.

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

Use show cpu all to check all the Zyxel Device CPU utilization. Use show cpu status to check the Zyxel Device average CPU utilization. You can use these commands to check your cpu status if you feel the Zyxel Device’s performance is becoming slower

Use `show users` to check the account that logs into the Zyxel Device.

```
usgflex200hp> show users
show-users
    admin-list admin
        role admin
        from console
        tunnel-ip 0.0.0.0
        service console
        login-time 0:03:41
        lease-timeout 23:56:19
        reauth-timeout 23:56:19
        user-info admin(admin)
        unique ttyS1
```

Here are examples of the commands that display the MAC address, serial number, and firmware version.

```
usgflex200hp> show mac
MAC address: D8:EC:E5:5C:0D:04-D8:EC:E5:5C:0D:0C
usgflex200hp> show serial-number
serial number: S212L16295036
usgflex200hp> show version
show-version
    firmware 1
        model-id "USG FLEX 200HP"
        firmware-version 7.00(ABXE.0)b2
        build-date "2022-08-30 14:58:48"
        boot-status Standby
        ..
    firmware 2
        model-id "USG FLEX 200HP"
        firmware-version 1.00(ABXE.0)b2s1
        build-date "2022-09-21 11:55:41"
        boot-status Running
```

Here is an example of the command that displays the Zyxel Device interfaces information.

```
usgflex200hp> show interface
No.Name           Status    Ip Address              IP Assignment  Interface  Type
================================================================================
====================
0  ge1            DOWN      fe80::daec:e5ff:fe5c:d04/64   Link Local   ethernet
1  ge2            DOWN      fe80::daec:e5ff:fe5c:d05/64   Link Local   ethernet
2  ge3            DOWN      192.168.168.1/24              Static       ethernet
                            fe80::daec:e5ff:fe5c:d06/64   Link Local
3  ge4            DOWN      192.168.169.1/24              Static       ethernet
                            fe80::daec:e5ff:fe5c:d0a/64   Link Local
================================================================================
```

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

```
usgflex200hp> show port statistic
show-port-statistics
    ok
        port-list 1
            name p1
            rx_bypes 0
            rx_pkts 0
            rx_errs 0
            rx_drops -2007148728
            rx_bps 0
            tx_bytes 0
            tx_pkts 0
            tx_errs 0
            tx_colls 0
            tx_bps 0
            uptime 0
        port-list 2
            name p2
            rx_bypes 0
            rx_pkts 0
            rx_errs 0
            rx_drops -1237797048
            rx_bps 0
            tx_bytes 0
            tx_pkts 0
            tx_errs 0
            tx_colls 0
            tx_bps 0
            uptime 0
        port-list 3
            name p3
            rx_bypes 194620
            rx_pkts 1995
            rx_errs 0
            rx_drops -1183496376
            rx_bps 204
            tx_bytes 1461644
            tx_pkts 1783
            tx_errs 0
            tx_colls 0
            tx_bps 162
            uptime 69
        port-list 4
            name p4
            rx_bypes 0
            rx_pkts 0
            rx_errs 0
            rx_drops -1192970424
            rx_bps 0
            tx_bytes 0
            tx_pkts 0
            tx_errs 0
            tx_colls 0
            tx_bps 0
            uptime 0
```

Here are examples of the commands that display the system uptime.

```
usgflex200hp> show system uptime
show-uptime
    ok
        uptime 0:12:09
```

CHAPTER 4
USER LED

4.1 User LED

The **USER** LED is located at the front panel of the Zyxel Device. Use this LED to check one of the following:

- Admin account login status.
- User IP address locked out status.
- License status.
- New firmware available for update.

Use the command to configure the **USER** LED settings. You must use the `edit running` command before you can use the command.

Table 7 USER LED Command

COMMAND	DESCRIPTION
`system user-defined-led type {Admin_login(green_on)| user_lockout(amber_on)| license_expired(green_blinking)| new_firmware_available(green_blinking) | Off}`	Select how you want the **USER** LED to behave. • Select **Admin login (green on)** if you want the **USER** LED to be steady green when there are admin accounts logged into the Zyxel Device. • Select **User Lockout (amber on)** if you want the **USER** LED to be steady amber when a user IP address is locked out of the Zyxel Device. A user IP address will be locked out when the user has logged into the Zyxel Device unsuccessfully (for example, wrong password) for more than three times. • Select **License Expired (amber on)** if you want the **USER** LED to be steady amber when a Zyxel Device service license has expired. • Select **New Firmware Available (green blinking)** if you want the **USER** LED to blink green when there is new firmware available for upload. • Select **Off** to turn off the **USER** LED.

CHAPTER 5
Interfaces

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 interfaces can belong to the same zone.

Some characteristics do not apply to some types of interfaces.

5.1.1 Types of Interfaces

You can create several types of interfaces in each Zyxel Device model. The types supported vary by Zyxel Device model.

- **Ethernet interfaces** are the foundation for defining other interfaces and network policies.
- **VLAN interfaces** receive and send tagged frames. The Zyxel Device 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 Zyxel Device. You can also assign an IP address and subnet mask to the bridge.
- **Trunk interfaces** manage load balancing between interfaces.
- **PPPoE interfaces** support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE interfaces.
- **VPN Tunnel Interface (VTI)** encrypts or decrypts IPv4 traffic from or to the interface according to the IP routing table.

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

Table 8 Interface Characteristics

CHARACTERISTICS	ETHERNET	VLAN	BRIDGE	PPPOE
Name*	gex	vlanx	brx	pppx
IP Address Assignment				
Static IP Address	Yes	Yes	Yes	Yes
DHCP Client	Yes	Yes	Yes	Yes (Auto)
Interface Parameters				
Packet Size (MTU)	Yes	Yes	Yes	Yes

Table 8 Interface Characteristics

CHARACTERISTICS	ETHERNET	VLAN	BRIDGE	PPPOE
Data Size (MSS)	Yes	Yes	Yes	Yes
Traffic Prioritization	Yes	Yes	Yes	Yes
DHCP				
DHCP Server	Yes	Yes	Yes	No
DHCP Relay	Yes	Yes	Yes	No
Ping Check	Yes	Yes	Yes	Yes

Note: 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.

5.1.2 Relationships Between Interfaces

In the Zyxel Device, 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 9 Interface Characteristics

CHARACTERISTICS	ETHERNET	ETHERNET	VLAN	PPPOE	BRIDGE
Name*	wan1, wan2	lan1, lan2	vlan*x*	pppx	br*x*
Configurable Zone	No	No	Yes		Yes
IP Address Assignment				Yes	
Static IP address	Yes	Yes	Yes	Yes	Yes
DHCP client	Yes	No	Yes	Yes	Yes
Interface Parameters				Yes	
Packet size (MTU)	Yes	Yes	Yes	Yes	Yes
DHCP				Yes (Auto)	
DHCP server	No	Yes	Yes		Yes
DHCP relay	No	Yes	Yes	No	Yes
Connectivity Check	Yes	No	Yes	No	Yes

5.2 Interface Command Input Values

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

Table 10 Interface Command Input Values

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

The following sections introduce commands that are supported by several types of interfaces.

5.3 Ethernet Interface Commands

This table lists the Ethernet interface commands.

Table 11 Ethernet Interface Commands

COMMAND	DESCRIPTION
`vrf main interface ethernet <interface-name> default-snat enabled {true| false}`	Enables default SNAT settings for the specified interface.
`vrf main interface ethernet <interface-name> ipv4 dhcp enabled {true| false}`	Makes the specified interface a DHCP client; the DHCP server gives the specified interface its IP address, subnet mask, and gateway.
`vrf main interface ethernet <interface-name> ipv4 dhcp dhcp-lease-time <0...4294967295>`	Sets how long the specified interface can use the information (especially the IP address) received from the DHCP server before it has to request the information again. The default value is 7200.
`vrf main interface ethernet <interface-name> ipv4 address <ipv4-address>`	Enters the IP address for this interface.

Table 11 Ethernet Interface Commands

COMMAND	DESCRIPTION
`vrf main interface ethernet <interface-name> ipv4 gateway <ipv4-address>`	Enters the IP address of the router through which this connection will send traffic.
`vrf main interface ethernet <interface-name> enabled {true|false}`	Enables or disables the specified interface.
`vrf main interface ethernet <interface-name> type {internal|external}`	Sets the type of network you will connect this interface. `internal` is for connecting to a local network. `external` is for connecting to an external network, such as the Internet.
`vrf main interface ethernet <interface-name> description <description>`	Enters a description of the specified interface. You can use up to 30 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-"
`vrf main interface ethernet <interface-name> mtu <0...4294967295>`	Sets the Maximum Transmission Unit, which is the maximum number of bytes in each packet moving through this interface. The default value is 1500.
`show state vrf main interface ethernet`	Displays configuration details for each interface.

5.3.1 Ethernet Interface Command Example

The following command shows you the configuration details for interface ge2.

```
usgflex500h> show state vrf main interface ethernet
ethernet ge2
    mtu 1500
    promiscuous false
    enabled true
    oper-status DOWN
    counters
        in-octets 0
        in-unicast-pkts 0
        in-discards 0
        in-errors 0
        out-octets 0
        out-unicast-pkts 0
        out-discards 0
        out-errors 0
        ..
    network-stack
        ipv4
            send-redirects true
            accept-redirects false
            accept-source-route false
            arp-announce any
            arp-filter false
            arp-ignore any
            log-invalid-addresses false
            ..
        ipv6
            autoconfiguration true
            accept-router-advert never
            accept-redirects false
            accept-source-route false
            router-solicitations -1
            use-temporary-addresses never
            ..
        ..
    ports p2
    ethernet
        mac-address d8:ec:e5:60:94:ff
        ..
    op
```

5.4 VLAN Interface Commands

This section covers commands that are specific to VLAN interfaces. VLAN interfaces also use many of the general interface commands discussed at the beginning of Section 5.2 on page 44.

This table lists the VLAN interface commands.

Table 12 VLAN Interface Commands

COMMAND	DESCRIPTION
vrf main interface vlan <*interface-name*> default-snat enabled {true| false}	Enables default SNAT settings for the specified interface.
vrf main interface vlan <*interface-name*> ipv4 dhcp enabled {true| false}	Makes the specified interface a DHCP client; the DHCP server gives the specified interface its IP address, subnet mask, and gateway.
vrf main interface vlan <*interface-name*> ipv4 dhcp dhcp-lease-time <*0...4294967295*>	Sets how long each computer can use the information (especially the IP address) before it has to request the information again. The default value is 7200.
vrf main interface vlan <*interface-name*> ipv4 address <*ipv4-address*>	Enters the IP address for this interface.
vrf main interface vlan <*interface-name*> ipv4 gateway <*ipv4-address*>	Enters the IP address of the router through which this connection will send traffic.
vrf main interface vlan <*interface-name*> enabled {true| false}	Enables or disables the specified interface.
vrf main interface vlan <*interface-name*> type {internal| external}	Sets the type of network you will connect this interface. `internal` is for connecting to a local network. `external` is for connecting to an external network, such as the Internet.
vrf main interface vlan <*interface-name*> description <*description*>	Enters a description of the specified interface. You can use up to 30 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-"
vrf main interface vlan <*interface-name*> mtu <*0...4294967295*>	Sets the Maximum Transmission Unit, which is the maximum number of bytes in each packet moving through this interface. The default value is 1500.
vrf main interface vlan <*interface-name*> vlan-id <1...4094>	Sets the VLAN ID used to identify the VLAN.
vrf main interface vlan <*interface-name*> vlan-priority-code <0...7>	Sets the 802.1p priority for VLAN outgoing traffic from 0 to 7 where 0 is the lowest priority (background traffic) and 7 the highest (network control traffic).

5.4.1 VLAN Interface Command Examples

The following commands show you how to set up VLAN vlan100 with the following parameters: VLAN ID 100, interface port p1, IP 1.2.3.4, MTU 598, gateway 2.2.2.2.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main interface vlan vlan100 vlan-id 100
usgflex200hp running config#! vrf main interface vlan vlan100 ipv4 address 1.2.3.4
usgflex200hp running config#! vrf main interface vlan vlan100 ipv4 gateway 2.2.2.2
usgflex200hp running config#! vrf main interface vlan vlan100 mtu 598
usgflex200hp running config#! vrf main interface vlan vlan100 link-port p1
usgflex200hp running config# commit
Configuration committed.
```

5.5 Bridge Interface Commands

This section covers commands that are specific to bridge interfaces. Bridge interfaces also use many of the general interface commands discussed at the beginning of Section 5.2 on page 44.

A bridge interface creates a software bridge between the members of the bridge interface, and becomes the Zyxel Device's interface for the resulting network. To use the whole Zyxel Device as a transparent bridge, add all of the Zyxel Device's interfaces to a bridge interface.

A bridge interface may consist of the following members:

- Zero or one VLAN interfaces (and any associated virtual VLAN interfaces)
- Any number of Ethernet interfaces (and any associated virtual Ethernet interfaces)

When you create a bridge interface, the Zyxel Device removes the members' entries from the routing table and adds the bridge interface's entries to the routing table. .

Table 13 Bridge Interface Commands

COMMAND	DESCRIPTION
`vrf main interface bridge <interface-name> default-snat enabled {true| false}`	Enables default SNAT settings for the specified interface.
`vrf main interface bridge <interface-name> enabled {true| false}`	Enables or disables the interface.
`vrf main interface bridge <interface-name> type {internal| external}`	Sets the type of network you will connect this interface. `internal` is for connecting to a local network. `external` is for connecting to an external network, such as the Internet.
`vrf main interface bridge <interface-name> mtu <0...4294967295>`	Sets the Maximum Transmission Unit, which is the maximum number of bytes in each packet moving through this interface. The default value is 1500.
`vrf main interface bridge <interface-name> description <description>`	Enters a description of the specified interface. You can use up to 30 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-"

5.6 VTI Interface Commands

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

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

Create a trunk using VPN tunnel interfaces for load balancing.

5.6.1 Restrictions for IPsec Virtual Tunnel Interface

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

This table lists the VTI-specific interface commands. See Table 11 on page 44 for common `interface` commands.

Table 14 VTI Interfaces Commands

COMMAND	DESCRIPTION
`vrf main interface legacy-vti <interface-name>`	Sets the name of the interface.
`enabled {true| false}`	Enables the specified interface.
`ipv4 address <ipv4-address>`	Sets the IP address for the specified interface.
`ipv4 gateway <ipv4-address>`	Sets the gateway IP address to which the Zyxel Device routes to.
`ping-check enabled {true| false}`	Enables the connection check. The interface can regularly check the connection to the gateway you specified to make sure it is still available. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.
`ping-check method {icmp| tcp}`	Sets the connection check method to `icmp` to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Sets the connection check method to `tcp` to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it si still available.
`ping-check period <5...600>`	Sets the number of seconds between connection check attempts. The default value is 30.
`ping-check timeout <1...10>`	Sets the number of seconds to wait for a response before the attempt is a failure. The default value is 5.
`ping-check fail-tolerance <1...10>`	Sets the number of consecutive failures before the Zyxel Device stops routing through the gateway. The default value is 5.

Table 14 VTI Interfaces (continued)Commands

COMMAND	DESCRIPTION
ping-check probe-condition {any| all}	Sets the probe condition to any if you want the check to pass if at least one of the domain names or IP addresses responds. Sets the probe condition to all if you wan the check to pass only if both domain names or IP addresses respond.
ping-check target <*ipv4-address*| *domain-name*>	Specifies one or two domain names or IP addresses for the connectivity check.

5.7 Network Debug Commands

If you're having problems with the Zyxel Device, customer support may request the output from certain debug commands such as these.

Table 15 Network Debug Commands

COMMAND	DESCRIPTION
cmd debug network brctl show	Displays members in all bridge interfaces.
cmd debug network brctl showmacs <bridge interface>	Displays the MAC addresses of members in a specific bridge interface.
cmd debug network brctl showstp <bridge interface>	Displays spanning tree details of a bridge interface.
cmd debug network zone info	Displays zone IDs, interfaces and zone names.
cmd debug network ipset list	Displays IP set details. An IP set is a framework for storing IP addresses, port numbers, IP and MAC address pairs, or IP address and port number pairs.
cmd debug network socket	Displays network socket details. A socket is one endpoint of a two-way communication link between two programs running on the network. An endpoint is a combination of an IP address and a port number.
cmd debug network interface	Displays network interface details such as number of bytes, packets, errors, packets dropped, overrun, multicast packets received or transmitted on an interface.
cmd debug network statistics	Displays network statistics details on IP, ICMP, ICMP messages, TCP, UDP, UdpLite, TcpExt, IpExt, and SCTP (Stream Control Transmission Protocol) similar to the 'netstat –s' command in Linux.

5.7.1 Network Debug Command Examples

The following are some example network debug commands.

Figure 22 Debug Zones

```
usgflex500h running config# cmd debug network zone info
zone id, interface: ready?
==============================
2 ge1:1
2 ge2:1
3 ge3:1
3 ge4:1
3 cat:1
4 DMZ:1

zone id, zone name
==============================
2 WAN
3 LAN
4 DMZ
5 IPSec_VPN
6 SSL_VPN
usgflex500h running config#
```

Figure 23 Debug IP Sets

```
usgflex500h running config#cmd debug network ipset list
Name: zyset-address4-0
Type: zyip
Revision: 0
Header: family inet count 1
Size in memory: 40
References: 4294967295
Members:
192.88.99.1
 count 1

Name: zyset-service-0
Type: zyport
Revision: 0
Header: family inet count 1
Size in memory: 12
References: 4294967295
Members:
AH
.
.
```

Figure 24 Debug Network Sockets

```
usgflex500h running config# cmd debug network socket
Netid State  Recv-Q Send-Q      Local Address:Port    Peer Address:Port Process
raw   UNCONN 0      0                0.0.0.0:255          0.0.0.0:*
raw   UNCONN 0      0                0.0.0.0:255          0.0.0.0:*
raw   UNCONN 229376 0                     *:58                 *:*
raw   UNCONN 0      0                     *:255                *:*
raw   UNCONN 0      0                     *:255                *:*
udp   UNCONN 0      0                0.0.0.0:3799         0.0.0.0:*
udp   UNCONN 0      0             172.21.56.19:53         0.0.0.0:*
udp   UNCONN 0      0           192.168.169.1:53          0.0.0.0:*
udp   UNCONN 0      0         169.254.148.254:53          0.0.0.0:*
udp   UNCONN 0      0           192.168.168.1:53          0.0.0.0:*
udp   UNCONN 0      0               127.0.0.1:53          0.0.0.0:*
udp   UNCONN 0      0                 0.0.0.0:68          0.0.0.0:*
udp   UNCONN 0      0                 0.0.0.0:161         0.0.0.0:*
udp   UNCONN 0      0                 0.0.0.0:4500        0.0.0.0:*
.......
```

Figure 25 Debug Network Interfaces

```
usgflex500h running config# cmd debug network interface
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    RX: bytes  packets  errors  dropped overrun mcast
    237666657  447661   0       0       0       0
    RX errors: length   crc     frame   fifo    missed
               0        0       0       0       0
    TX: bytes  packets  errors  dropped carrier collsns
    237666657  447661   0       0       0       0
    TX errors: aborted  fifo   window heartbeat transns
               0        0       0       0       0
2: ifb0: <BROADCAST,NOARP> mtu 1500 qdisc noop state DOWN mode DEFAULT group
default qlen 32
    link/ether ea:fa:e7:1c:57:a7 brd ff:ff:ff:ff:ff:ff
    RX: bytes  packets  errors  dropped overrun mcast
    0          0        0       0       0       0
    RX errors: length   crc     frame   fifo    missed
               0        0       0       0       0
    TX: bytes  packets  errors  dropped carrier collsns
    0          0        0       0       0       0
    TX errors: aborted  fifo   window heartbeat transns
               0        0       0       0       0
```

Figure 26 Debug Network Statistics

```
usgflex500h running config# cmd debug network statistics
Ip:
    Forwarding: 1
    4741765 total packets received
    53 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    1298780 incoming packets delivered
    954581 requests sent out
    323 dropped because of missing route
    28 reassemblies required
    14 packets reassembled ok
Icmp:
    280 ICMP messages received
    0 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 11
        echo requests: 16
        echo replies: 253
    613 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 57
        echo requests: 540
        echo replies: 16
IcmpMsg:
        InType0: 253
        InType3: 11
        InType8: 16
....
```

CHAPTER 6
Trunks

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

6.2 Trunk Scenario Examples

Suppose one of the Zyxel Device'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 Load Balancing Algorithms

The following sections describe the load balancing algorithms the Zyxel Device can use to decide which interface the traffic (from the LAN) should use for a session. In the load balancing section, a session may refer to normal connection-oriented, UDP or SNMP2 traffic. The available bandwidth you configure on the Zyxel Device refers to the actual bandwidth provided by the ISP and the measured bandwidth refers to the bandwidth an interface is currently using.

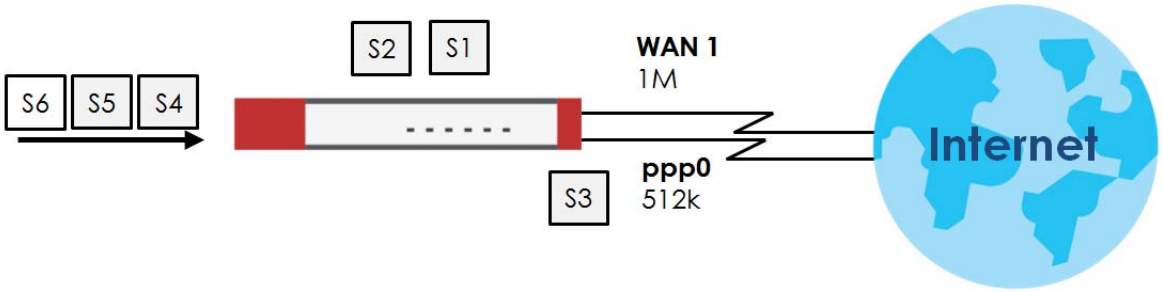
6.3.1 Weighted Round Robin

Round Robin scheduling services queues on a rotating basis and is activated only when an interface has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that interface. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

The Weighted Round Robin (WRR) algorithm is best suited for situations when the bandwidths set for the two WAN interfaces are different. Similar to the Round Robin (RR) algorithm, the Weighted Round Robin (WRR) algorithm sets the Zyxel Device to send traffic through each WAN interface in turn. In addition, the WAN interfaces are assigned weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight.

For example, in the figure below, the configured available bandwidth of WAN1 is 1M and WAN2 is 512K. You can set the Zyxel Device to distribute the network traffic between the two interfaces by setting the weight of wan1 and wan2 to 2 and 1 respectively. The Zyxel Device assigns the traffic of two sessions to wan1 and one session's traffic to wan2 in each round of 3 new sessions.

Figure 27 Weighted Round Robin Algorithm Example



6.3.2 Least Load First

The least load first algorithm uses the current (or recent) outbound bandwidth utilization of each trunk member interface as the load balancing index(es) when making decisions about to which interface a new session is to be distributed. The outbound bandwidth utilization is defined as the measured outbound throughput over the available outbound bandwidth.

The outbound bandwidth utilization is used as the load balancing index. In this example, the measured (current) outbound throughput of WAN 1 is 412K and WAN 2 is 198K. The Zyxel Device calculates the load balancing index as shown in the table below.

Since WAN 2 has a smaller load balancing index (meaning that it is less utilized than WAN 1), the Zyxel Device will send the subsequent new session traffic through WAN 2.

Table 16 Least Load First Example

INTERFACE	OUTBOUND		LOAD BALANCING INDEX (M/A)
	AVAILABLE (A)	MEASURED (M)	
WAN 1	512 K	412 K	0.8
WAN 2	256 K	198 K	0.77

6.3.3 Spillover

The spillover load balancing algorithm sends network traffic to the first interface in the trunk member list until the interface's maximum allowable load is reached, then sends the excess network traffic of new sessions to the next interface in the trunk member list. This continues as long as there are more member interfaces and traffic to be sent through them.

Suppose the first trunk member interface uses an unlimited access Internet connection and the second is billed by usage. Spillover load balancing only uses the second interface when the traffic load exceeds the threshold on the first interface. This fully utilizes the bandwidth of the first interface to reduce Internet usage fees and avoid overloading the interface.

6.4 Trunk Commands Input Values

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

Table 17 Trunk 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-name	The name of an interface, it could be an Ethernet, PPP, VLAN or bridge interface. The possible number of each interface type and the abbreviation to use are as follows. Ethernet interface: ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. PPPoE interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your Zyxel Device model supports. VLAN interface: vlan*x*, *x* = 0 - 4094 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your Zyxel Device model supports.
num	The interface's position in the trunk's list of members <1..8>.

6.5 Trunk Commands

The following table lists the trunk commands. You must use the `edit running` command to enter the configuration mode before you can use these commands. See Table 17 on page 56 for details about the values you can input with these commands.

Table 18 Trunk Commands

COMMAND	DESCRIPTION
`vrf main interface-group <group-name> algorithm <wrr| spill-over|llf>.`	Sets the trunk's load balancing algorithm.
`vrf main interface-group <group-name> interface <interface-name> passive {true| false} weight <1...10>`	Sets the interface's weight or sets it to be passive to have the Zyxel Device only use this connection when all of the connections set to active are down. You can only set one of a group's interfaces to passive mode.
`vrf main interface-group <group-name> loadbalancing-index <outbound | inbound| total>`	Sets the load balancing index interface for spill-over or llf algorithms. The load balancing index sets the interface for which a new session is to be distributed.
`vrf main interface-group <group-name> limit <1.. 2097152 >`	Sets the upper throughput threshold in bytes for spill-over or llf algorithms. Throughput is the moving average of traffic passing through the Zyxel Device in the last 10 seconds updated every 1 second.
`show config vrf main interface-group <group-name>`	Displays the interface group settings you configured.
`show state vrf main interface-group <group-name>`	Displays the default interface group settings and the interface group settings you configured.

6.6 Trunk Command Examples

The following example creates a weighted round robin trunk for Ethernet interfaces ge3 and ge4. The Zyxel Device sends twice as much traffic as it does through ge4.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main interface-group Example1 interface ethernet
ge3 weight 2
usgflex200hp running config# vrf main interface-group Example1 interface ethernet
ge4 weight 1
usgflex200hp running config# commit
Configuration committed.
```

CHAPTER 7
Route

7.1 Policy Route

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

7.1.1 Source Network Address Translation (SNAT)

SNAT allows the Zyxel Device to rewrite the source IP address of packets in a policy route. This means you can make packets coming from an IP address appear to originate from a different IP address.

7.1.1.1 SNAT with the ZyWALL Interface

You can apply SNAT to packets sent from the ZyWALL interface. This can be used to separate internally generated Zyxel Device traffic from other traffic.

For example: The Zyxel Device has two IP addresses, 6.6.6.6 and 6.6.6.7, on a WAN interface. There is a firewall in front of the Zyxel Device with the following security rules:

- IP address 6.6.6.6 is client traffic. There are no restrictions.
- IP address 6.6.6.7 is Zyxel Device traffic, Packets can only go to *.myzyxel.com and *.cloud.zyxel.com.

If clients are connected to ge3 on the Zyxel Device, then you need to create two policy routes with SNAT enabled:

- Client_Route - Incoming interface: ge3, SNAT: 6.6.6.6.
- Device_Route - Incoming interface: ZyWALL, SNAT: 6.6.6.7.

7.2 Policy Route and Static Route Input Values

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

Table 19 Policy Route and Static Route Command Input Values

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	The name of the interface. Ethernet interface: ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. VLAN interface: vlan*x*, *x* = 0 - 4094 virtual interface on top of VLAN interface: vlan*x*:*y*, *x* = 0 - 4094, *y* = 1 - 12 bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your Zyxel Device model supports. virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE interfaces your Zyxel Device model supports.
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.

7.3 Policy Route Commands

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

Table 20 Policy Route Commands

COMMAND	DESCRIPTION
`vrf main routing policy-route rule <profile-name> enabled {true| false}`	Activates the profile.
`vrf main routing policy-route rule <`*profile-name*`> description <`*description*`>`	Enter a description for this profile, You can use 1 to 60 single-byte characters.
`vrf main routing policy-route rule <profile-name> override-direct-route {true| false}`	Has the Zyxel Device forward packets that match a policy route according to the policy route instead of sending the packets to a directly connected network.
`vrf main routing policy-route rule <`*profile-name*`> match user {admin-object` *admin-object*`| user-object` *user-object*`| group` *group*`| any}`	Sets a user name or user group from which the packets are sent.
`vrf main routing policy-route rule <`*profile-name*`> match schedule {object` *schedule-profile*`| group` *schedule-object*`| none}`	Sets a schedule to control when the policy route is active. none means the route is active at all times if enabled.

Table 20 Policy Route Commands

COMMAND	DESCRIPTION
vrf main routing policy-route rule <*profile-name*> match from <*interface*>	Sets where the packets are coming from.
vrf main routing policy-route rule <*profile-name*> match source {object *object*| group *group*| any}	Sets a source IP address object, including geographic address and FQDN (group) objects, from which the packets are sent.
vrf main routing policy-route rule <*profile-name*> match destination {object *object*| group *group*| any}	Sets a destination IP address object, including geographic address and FQDN (group) objects, to which the traffic is being sent.
vrf main routing policy-route rule <*profile-name*> match service {object *object*| group *group*| any}	Sets a service or service group to identify the type of traffic to which this policy route applies.
vrf main routing policy-route rule <*profile-name*> match srcport {object *object*| group *group*| any}	Sets a service or service group to identify the source ort of packets to which the policy route applies.
vrf main routing policy-route rule <profile-name> match dscp <*dscp-code*>	Sets a DSCP code point value of incoming packets to which this policy route applies. The lower the number the higher the priority with exception of 0 which is usually given only best-effort treatment. any means all DSCP value or no DSCP marker. default means traffic with a DSCP value of 0. This is usually best effort traffic. The **af** choices stand for Assured Forwarding. The number following the **af** identifies one of four classes and one of three drop preferences. See Section 7.3.1 on page 61 for more information.
vrf main routing policy-route rule <profile-name> action next-hop {gateway *address-object*| gateway-ip *ipv4-address*| interface *interface*| trunk *trunk*| auto}	Sets the next-hop to which the matched packets are routed. auto means to have the Zyxel Device use the routing table to find a next-hop and forward the matched packets automatically.
vrf main routing policy-route rule <*profile-name*> action snat {pool *address-group*| outgoing-interface *address-object*| none}	Use none to not use SNAT for this profile. Use outgoing-interface to use the IP address of the outgoing interface as the source IP address of the packets that matches this route. To use SNAT for a virtual interface that is in the same WAN trunk as the physical interface to which the virtual interface is bound, the virtual interface and physical interface must be in different subnet. Use pool to set a pre-defined address or address group to use as the source IP addresses of the packets that match this route. Note: If the address object is a group or range of IP addresses, then the Zyxel Device picks one IP address randomly from the group or range, and then assigns the address permanently to the policy.

Table 20 Policy Route Commands

COMMAND	DESCRIPTION
`vrf main routing policy-route rule <profile-name> action dscp-marking <dscp-code>`	Sets how the Zyxel Device handles the DSCP value of the outgoing packets that match this route. Set this to `default` to have the Zyxel Device set the DSCP value of the packets to 0. Set this to an "af" class (including af11~af13, af21~af23, af31~af33, and af41~af43) which stands for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences. See Section 7.3.1 on page 61 for more information.
`show state vrf main routing`	Displays the Zyxel Device routing status, such as the number of connected routes and each routing function settings.
`show config vrf main routing`	Displays if the override direct route feature is enabled.
`show state vrf main routing policy-route`	Displays details of a Zyxel Device policy routing, such as the match rule, action and number of matching packets.

7.3.1 Assured Forwarding (AF) PHB for DiffServ

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

Table 21 Assured Forwarding (AF) Behavior Group

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

7.3.2 Policy Route Command Example

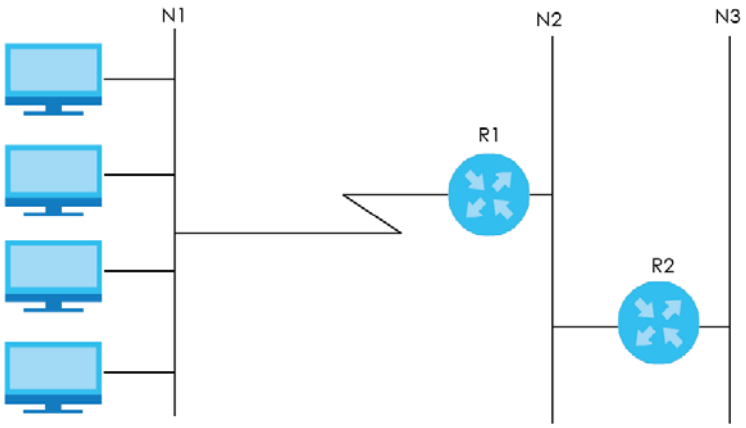
The following commands create two address objects (TW_SUBNET and GW_1) and create a policy that routes the packets (with the source IP address TW_SUBNET and any destination IP address) to the next-hop router GW_1.

```
usgflex200hp> edit running
usgflex200hp running config# object address-object address TW_SUBNET type host
192.168.2.0
usgflex200hp running config# object address-object address TW_SUBNET type host
255.255.255.0
usgflex200hp running config# object address-object address GW_1 type host
192.168.2.250
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# vrf main routing policy-route rule Rule1 description
example
usgflex200hp running config#! vrf main routing policy-route rule Rule1 match
destination any
usgflex200hp running config#! vrf main routing policy-route rule Rule1 match source
object TW_SUBNET
usgflex200hp running config#! vrf main routing policy-route rule Rule1 action snat
outgoing-interface
usgflex200hp running config#! vrf main routing policy-route rule Rule1 action next-
hop gateway GW_1
usgflex200hp running config#! vrf main routing policy-route rule Rule1 match user
admin-object admin
usgflex200hp running config#! vrf main routing policy-route rule Rule1 match
schedule none
usgflex200hp running config#! vrf main routing policy-route rule Rule1 match from
any
usgflex200hp running config#! vrf main routing policy-route rule Rule1 match
service any
usgflex200hp running config#! vrf main routing policy-route rule Rule1 match
srcport any
usgflex200hp running config# vrf main routing policy-route rule Rule1 match dscp
default
usgflex200hp running config# commit
Configuration committed.
```

7.4 Static Route

The Zyxel Device has no knowledge of the networks beyond the network that is directly connected to the Zyxel Device. For instance, the Zyxel Device knows about network **N2** in the following figure through gateway **R1**. Use a static route to define a route when there is a single route or a preferred route for traffic to reach a destination.

Figure 28 Example of Static Routing Topology



7.5 Static Route Commands

The following table describes the commands available for static route. You must use the `edit running` command to enter the configuration mode before you can use these commands. See Section Table 19 on page 59 for information on input values.

Table 22 Static Route Commands

COMMAND	DESCRIPTION
`vrf main routing static-route rule <profile-name> description <description>`	Enter a description for this profile.
`vrf main routing static-route rule <profile-name> metric <1...127>`	Sets a number that approximates the cost for this link. Metric represents the cost of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for direct connected networks.
`vrf main routing static-route rule <profile-name> destination {cidr cidr| object address-object}`	Specifies the IP network address of the final destination.
`vrf main routing static-route rule <profile-name> via {gateway-object address-object| gateway ipv4-address| interface interface}`	`gateway-object/ gateway`: Enters the IP address or selects the address object of the next-hop gateway. `interface`: Sets a pre-defined interface through which the traffic is sent.

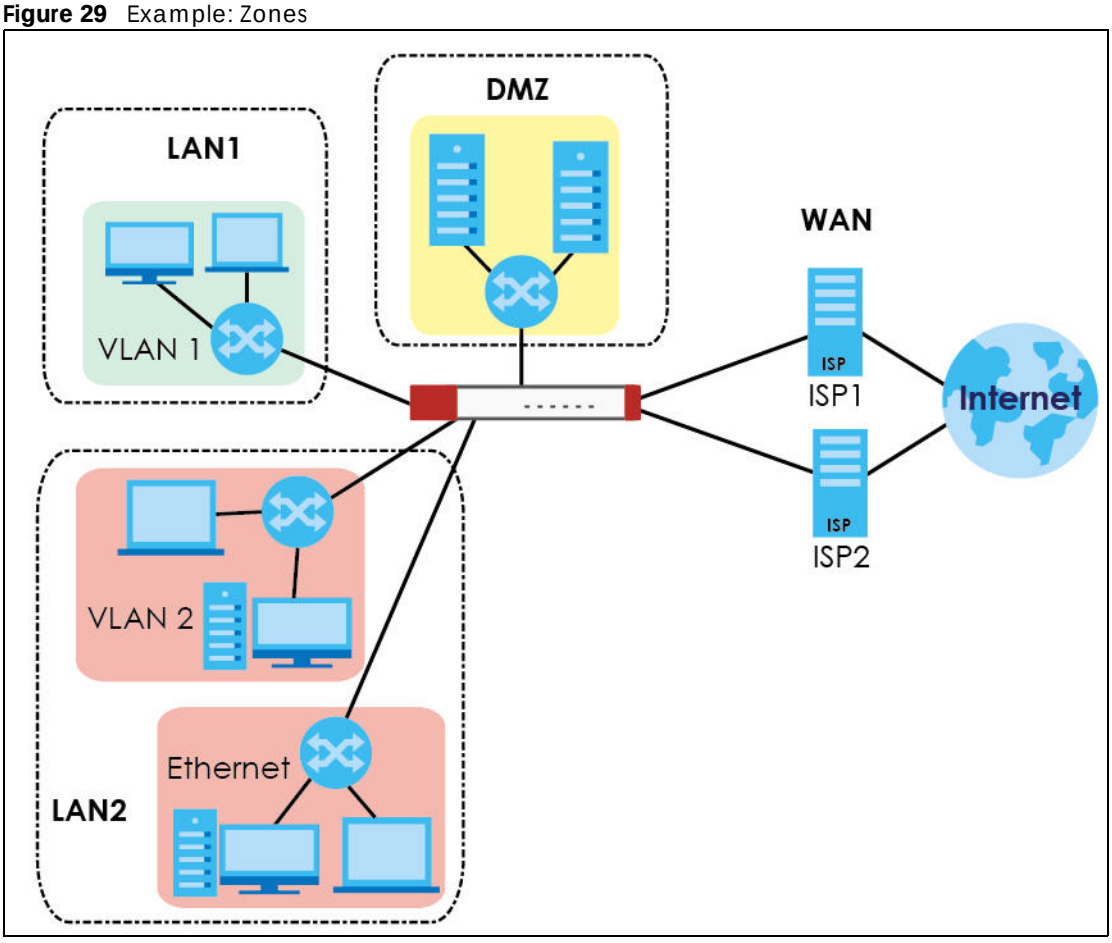
CHAPTER 8
Zones

8.1 Zones Overview

A zone is a group of interfaces and VPN tunnels. Set up zones to configure network security and network policies in the Zyxel Device. The Zyxel Device 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 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 29 Example: Zones



8.2 Zone Command Input Values

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

Table 23 Zone Command Input Values

LABEL	DESCRIPTION
profile-name	The name of a zone, or the name of a VPN tunnel. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.

8.3 Zone Commands

This table lists the zone commands.

Table 24 Zone Commands

COMMAND	DESCRIPTION
`object zone-object zone <profile-name> interface-list <interface>`	Adds the specified interface to the specified zone.
`object zone-object zone <profile-name> description <description>`	Enters a description associated with the specified zone.
`show object zone none-binding`	Displays the interfaces, tunnels and IPSec VPNs that are not associated with a zone yet.
`show object zone system-default`	Displays the pre-configured default zones that you cannot delete from the Zyxel Device.
`show object zone user-define`	Displays all customized zones.
`show object zone default-binding`	Displays the pre-configured interface and zone mappings that come with the Zyxel Device.
`show object zone binding-iface`	Displays each interface and zone mappings.

8.3.1 Zone Command Examples

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

```
usgflex200hp> edit running
usgflex200hp running config# object zone-object zone
WAN          LAN          DMZ          IPSec_VPN
usgflex200hp running config# object zone-object zone WAN
interface-list    description
usgflex200hp running config# object zone-object zone WAN interface-list ethernet
ge1 ethernet ge2
usgflex200hp running config# commit
Configuration committed.
```

CHAPTER 9
DDNS

9.1 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: The Zyxel Device WAN interface must have a public WAN IP address to use Dynamic DNS.

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

Table 25 Network > DDNS

DDNS SERVICE PROVIDER	SERVICE TYPES SUPPORTED	WEBSITE
DynDNS	Dynamic DNS, Static DNS, and Custom DNS	www.dyndns.com)
Dynu	Basic, Premium	www.dynu.com
No-IP	No-IP	www.no-ip.com
Selfhost	Selfhost	selfhoost.de

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

After, you configure the Zyxel Device, it automatically sends updated IP addresses to the DDNS service provider, which updates domain name mapping accordingly.

9.2 DDNS Command Input Values

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

Table 26 DDNS Command Input Value

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

9.3 DDNS Commands

The following table lists the DDNS commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 27 DDNS Commands

COMMAND	DESCRIPTION
`vrf main ddns rule <profile-name>`	Creates or edits the specified DDNS profile and enters the sub-command mode.
`enabled {true| false}`	Enables the specified DDNS profile.
`ddns-type {user-custom| dyndns| dyndns-static| dyndns-custom| no-ip| selfhost| dynu-basic| dynu-premium}`	Sets the service type in the specified DDNS profile.
`account username username password password`	Sets the username and password in the specified DDNS profile. *username*: You can use up to 31 single-byte characters and :_.-@ *password*: You can use up to 64 single-byte characters and the underscore (_).
`setting primary-binding interface <interface-name| any>`	Sets the primary interface to use for updating the IP address mapped to the domain name. any allows the domain name to be used with any interface.
`setting primary-binding ip-address <interface | custom ip ipv4-address| object object-name| auto| public ip>`	Configures the primary interface to use for updating the IP address mapped to the domain name. `interface`: The Zyxel Device sends the IP address of the specified interface to the DDNS server. `custom ip`: Select this if you're using a static IPv4 address for the domain name. The Zyxel Device sends your configured static IP address or the specified address object to the DDNS server. `auto`: Use this if the DDNS server supports it, there are one or more NAT routers between the Zyxel Device and the DDNS server, and the Zyxel Device interface has a dynamic IP address. The DDNS server checks the source IP address of packets from the Zyxel Device and uses that for the domain name. The Zyxel Device may not determine the proper IP address if there is an HTTP proxy server between the Zyxel Device and the DDNS server. `public ip`: The DDNS server uses this public IP address for the domain name. If you choose this, you must configure the `check-public-ip` commands, so that the Zyxel Device may know the public IP address (of the NAT router in front of the Zyxel Device, for example) and inform the DDNS server.
`settings check-public-ip URL`	If the DDNS server uses a public IP address for the domain name, this command has the Zyxel Device check the public IP address given to the URL it is using as its domain name.

Table 27 DDNS Commands (continued)

COMMAND	DESCRIPTION
`settings check-public-ip period`	If the The DDNS server uses a public IP address for the domain name, this command sets how often (5 to 1,440 minutes) the Zyxel Device should check the public IP address given to its URL.
`setting backup-binding interface <`*`interface-name`*`| any| none>`	Sets an alternate interface to map the domain name to when the interface specified in the `primary-binding` command is not available. none means to not use a backup address.
`setting backup-binding ip-address <interface | custom ip `*`ipv4-address`*`| object `*`object-name`*`| auto| public ip>`	Configures an alternate interface to map the domain name to when the interface specified in the `primary-binding` command is not available. `interface`: The Zyxel Device sends the IP address of the specified interface to the DDNS server. `custom ip`: Select this if you're using a static IPv4 address for the domain name. The Zyxel Device sends your configured static IP address or the specified address object to the DDNS server. `auto`: Use this if the DDNS server supports it, there are one or more NAT routers between the Zyxel Device and the DDNS server, and the Zyxel Device interface has a dynamic IP address. The DDNS server checks the source IP address of packets from the Zyxel Device and uses that for the domain name. The Zyxel Device may not determine the proper IP address if there is an HTTP proxy server between the Zyxel Device and the DDNS server. `public ip`: The DDNS server uses this public IP address for the domain name. If you choose this, you must configure the `check-public-ip` commands, so that the Zyxel Device may know the public IP address (of the NAT router in front of the Zyxel Device, for example), and inform the DDNS server.
`setting domain-name <`*`domain-name`*`>`	Enter the domain name you registered. You can use up to 255 characters.
`setting wildcard {true| false}`	Enables to alias subdomains to be aliased to the same IP address as your (dynamic) domain name. Please note that you can only use this command with DDNS type set to DnyDNS.
`setting mail-exchanger <`*`email-address`*`>`	Enter the host record of your mail server. DynDNS can route email for your domain name to a mail server. For example, DynDNS routes email for john-doe@yourhost.dyndns.org to the host record specified as the mail exchanger. Please note that you can only use this command with DDNS type set to DnyDNS.
`setting backup-mail-exchanger {true| false}`	Lets DynDNS store your email if your mail server is not available. Once your mail server is available again, the DynDNS server delivers the mail to you. Please note that you can only use this command with DDNS type set to DnyDNS.

Table 27 DDNS Commands (continued)

COMMAND	DESCRIPTION
https {true| false}	Encrypts traffic using SSL, including traffic with username and password, to the DDNS server.
show config vrf main ddns rule	Displays DDNS rules settings.
cmd ddns update rule <*profile-name*>	Has the Zyxel Device update the specified rule.
show ddns status	Displays DDNS rules status, last update time and the IP address of the domain name.

CHAPTER 10
Virtual Servers

10.1 Virtual Server Overview

NAT is also known as virtual server, port forwarding or port translation.

Virtual servers are computers on a private network behind the Zyxel Device that you want to make available outside the private network. If the Zyxel Device 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.

10.1.1 1:1 NAT and Many 1:1 NAT

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

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

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

10.2 Virtual Server Command Input Values

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

Table 28 Virtual Server Command Input Values

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

10.3 Virtual Server Commands

Please note that if you create a NAT rule using the IP address of the Web Configurator and set the external port to 80 (HTTP) or 443 (HTTPS), the rule will conflict with the Zyxel Device's default HTTP server port. You will not be able to access the Web Configurator through this interface.

Table 29 Virtual Server Commands

COMMAND	DESCRIPTION
vrf main virtual-server rule <*profile-name*> nat-1-1-map {true| false}	Enables 1:1 NAT type.
vrf main virtual-server rule <*profile-name*> nat-loopback {true| false}	Allows local users to use a domain name to access the virtual server.
vrf main virtual-server rule <*profile-name*> enabled {true| false}	Enables the virtual server profile.
vrf main virtual-server rule <*profile-name*> interface <*interface-name*>	Sets the interface on which packets for the virtual server profile must be received.
vrf main virtual-server rule <*profile-name*> source-ip {object *service-object*| address *ipv4-address*| cidr *cidr*| any| range from *ipv4-address* to *ipv4-address*}	Specifies the source IP address of the packets received by the virtual server profile's specified incoming interface. any means to use all of the incoming interface's IP addresses including dynamic address.
vrf main virtual-server rule <*profile-name*> original-ip {object *service-object*| address *ipv4-address*| cidr *cidr*| any| range from *ipv4-address* to *ipv4-address*}	Specifies the destination IP address of the packets received by the virtual server profile's specified incoming interface. The specified IP address will be translated to the internal IP address. any means to user all of the incoming interface's IP addresses including dynamic address or those of any virtual interfaces built upon the selected incoming interface.
vrf main virtual-server rule <profile-name> map-to {object *service-object*| address *ipv4-address*| cidr *cidr*| any| range from *ipv4-address* to *ipv4-address*}	Maps the specified destination IP address to the specified destination address object or IP address.
vrf main virtual-server rule <profile-name> map-type {any| port| ports| service| service-group}	Sets how many original destination ports the virtual server profile supports for the original IP you set. any: The virtual server profile supports all the destination ports. port: The virtual server profile supports one destination port. ports: The virtual server profile supports a range of destination ports. You might use a range of destination ports for unknown services or when one server supports more than one service. service: The virtual server profile supports a service such as FTP. service-group: The virtual server profile supports a group of services such as all service objects related to DNS.
show config vrf main virtual-server rule	Displays the virtual server profiles settings.

10.3.1 Virtual Server Command Examples

The following command creates virtual server profile Profile1 on the ge1 interface that maps IP addresses 10.0.0.8 to 192.168.1.56. for TCP protocol traffic on port 1720. It also enables NAP loopback.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main virtual-server rule Profile1 interface ge1
enabled true
usgflex200hp running config#! vrf main virtual-server rule Profile1 original-ip
address 10.0.0.8
usgflex200hp running config#! vrf main virtual-server rule Profile1 source-ip
address 192.168.1.56
usgflex200hp running config#! vrf main virtual-server rule Profile1 map-type port
protocol tcp original-port 1720 mapped-port 1720
usgflex200hp running config#! vrf main virtual-server rule Profile1 nat-loopback
true
usgflex200hp running config#! vrf main virtual-server rule Profile1 map-to address
192.168.1.56
usgflex200hp running config# commit
Configuration committed.
```

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

```
usgflex200hp running config# show config vrf main virtual-server rule
virtual-server Profile
    enabled true
    interface LAN1_SUBNET
    source-ip address 2.2.2.2
    original-ip address 3.3.3.3
    map-to address 1.1.1.1
    nat-1-1-map
        false
        ..
    nat-loopback
        false
        ..
    map-type any
    ..
virtual-server Profile1
    enabled true
    interface ge1
    source-ip address 192.168.1.56
    original-ip address 10.0.0.8
    map-to address 192.168.1.56
    nat-1-1-map
        false
        ..
    nat-loopback
        true
        ..
    map-type port protocol tcp original-port 1720 mapped-port 1720
    ..
```

CHAPTER 11
ALG

11.1 ALG Introduction

The Zyxel Device can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as FTP) to operate properly through the Zyxel Device'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 Zyxel Device examines and uses IP address and port number information embedded in the FTP traffic's data stream. When a device behind the Zyxel Device uses an application for which the Zyxel Device has FTP passed through enabled, the Zyxel Device 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 Zyxel Device only needs to use the ALG feature for traffic that goes through the Zyxel Device's NAT. The firewall allows related sessions for FTP applications that register with a server. The firewall allows or blocks peer to peer FTP traffic based on the firewall rules.

11.2 ALG Commands

The following table lists the ALG commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 30 ALG Commands

COMMAND	DESCRIPTION
`vrf main alg ftp enabled {true| false}`	Enables the ALG for FTP.
`vrf main alg ftp transformation {true| false}`	Lets the Zyxel Device modify IP addresses and port numbers embedded in the FTP data payload. You do not need to use this if you have an FTP device or server that can modify IP addresses and port numbers embedded in the FTP data payload.
`vrf main alg ftp signal-port <1025...65535>`	Sets a listening port number if you are using FTP on a TCP port other than 21.
`vrf main alg ftp signal-extra-port <1025...65535>`	Sets a listening port number if you are using FTP on an additional TCP port.
`show config vrf main alg ftp`	Displays the ALG for FTP settings.

11.3 ALG Commands Example

The following example uses ALG to allow FTP through the Zyxel Device NAT.

```
usgflex200hp running config# vrf main alg ftp enabled true
usgflex200hp running config# commit
Configuration committed.
```

CHAPTER 12
Secure Policy

12.1 Secure Policy Overview

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

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

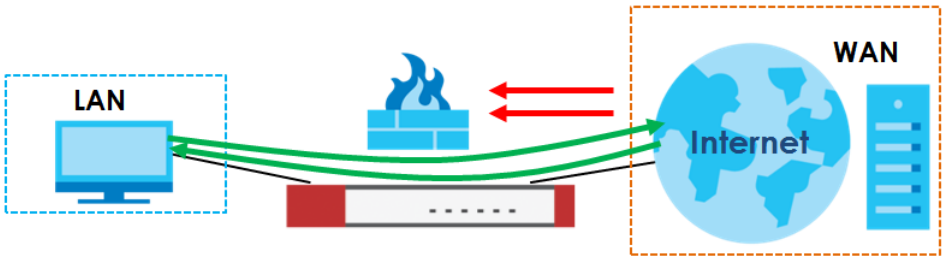
The policy can be configured:

- to allow or deny traffic that matches the criteria above
- send a log or alert for traffic that matches the criteria above
- to apply the actions configured in the security service profiles (such as application patrol, content filter, SSL inspection) to traffic that matches the criteria above

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

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

Figure 30 Default Directional Policy Example



12.1.1 Asymmetrical Routes

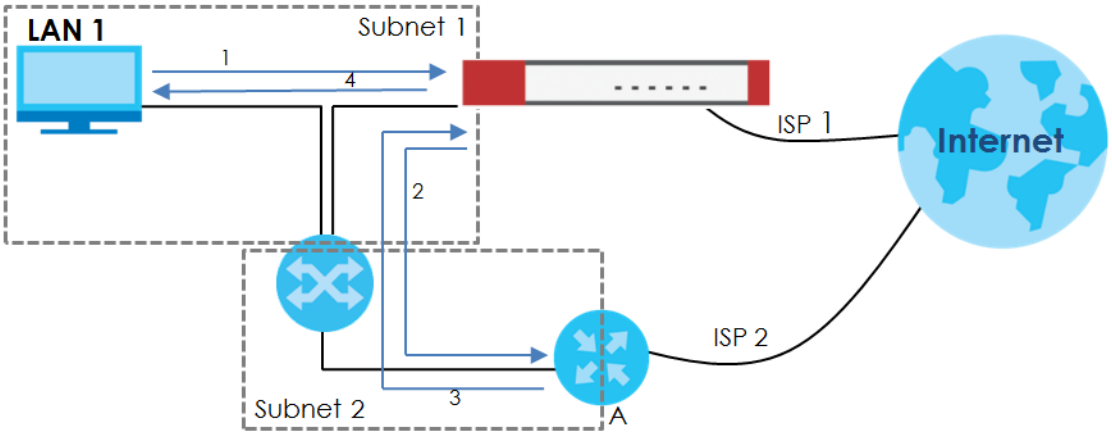
If an alternate gateway on the LAN has an IP address in the same subnet as the Zyxel Device's LAN IP address, return traffic may not go through the Zyxel Device. This is called an asymmetrical or "triangle" route. This causes the Zyxel Device to reset the connection, as the connection has not been acknowledged.

You can have the Zyxel Device permit the use of asymmetrical route topology on the network (not reset the connection). However, allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the Zyxel Device. A better solution is to use virtual interfaces to put the Zyxel Device and the backup gateway on separate subnets. Virtual interfaces allow you to partition your network into logical sections over the same interface. See the chapter about interfaces for more information.

By putting LAN 1 and the alternate gateway (**A** in the figure) in different subnets, all returning network traffic must pass through the Zyxel Device to the LAN. The following steps and figure describe such a scenario.

1. A computer on the LAN1 initiates a connection by sending a SYN packet to a receiving server on the WAN.
2. The Zyxel Device reroutes the packet to gateway **A**, which is in **Subnet 2**.
3. The reply from the WAN goes to the Zyxel Device.
4. The Zyxel Device then sends it to the computer on the LAN1 in **Subnet 1**.

Figure 31 Using Virtual Interfaces to Avoid Asymmetrical Routes



12.2 Secure Policy Command Input Values

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

Table 31 Secure Policy Command Input Values

LABEL	DESCRIPTION
address-object	The name of the IP address object. You may use 1-30 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
user-object	The name of the user. You may use 1-30 single-byte characters, including 0-9a-zA-Z._-. This value is case-sensitive.

Table 31 Secure Policy Command Input Values (continued)

LABEL	DESCRIPTION
zone-object	The name of the zone. For some Zyxel Device models, use up to 30 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive. For other Zyxel Devicemodels, use pre-defined zone names like DMZ, LAN1, SSL VPN, IPSec VPN, OPT, and WAN.
schedule-object	The name of the schedule. You may use 1-30 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
service-object	The name of the service. You may use 1-30 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

12.3 Secure Policy Commands

The following table describes the commands available for the secure policy. You must use the `edit running` command to enter the configuration mode before you can use the configuration commands.

Table 32 Secure Policy Commands

COMMAND	DESCRIPTION
`vrf main secure-policy enabled {true| false}`	Enables secure policy on the Zyxel Device.
`vrf main secure-policy default-rule action {allow| deny| reject} logging {no| log| log-alert}`	Sets how the secure policy handles packets that do not match any other secure policy rule.
`vrf main secure-policy asymmetrical-route enabled {true| false}`	Allows or disallows asymmetrical route topology.
`vrf main secure-policy rule <profile-name> action {allow| deny| reject}`	Sets the action the Zyxel Device takes when packets match this rule.
`vrf main secure-policy rule <profile-name> logging {no| log| log-alert}`	Sets the Zyxel Device to create a log or a log and an alert when packets match this rule. The no command sets the Zyxel Device not to create a log or alert when packets match this rule.
`vrf main secure-policy rule <profile-name> description <description>`	Sets a descriptive name (up to 60 printable ASCII characters) for a secure policy rule.
`vrf main secure-policy rule <profile-name> enabled {true| false}`	Activates the specified secure policy.
`vrf main secure-policy rule <profile-name> user {admin| user-object user-object| user-group user-group| any}`	Sets a user name or user group to which to apply the policy. The secure policy is activated only when the specified user logs into the system. The policy will be disabled when the user logs out. Sets this value to any to apply the policy to all users or user groups.
`vrf main secure-policy rule <profile-name> schedule {schedule-object schedule-object| schedule-group schedule-group| any}`	Sets the schedule that the policy uses.

Table 32 Secure Policy Commands

COMMAND	DESCRIPTION
vrf main secure-policy rule <*profile-name*> from {zone-object *zone-object*| any}	Sets the zone on which the packets are received.
vrf main secure-policy rule <*profile-name*> to {zone-object *zone-object*| any| ZyWALL}	Sets the zone from which the packets are sent.
vrf main secure-policy rule <*profile-name*> source-ip {address-object *address-object*| address-group *address-group*| any}	Sets an IPv4 address or address group object to apply the policy to traffic coming from it. Set this value to any to apply the policy to all traffic coming from IPv4 addresses.
vrf main secure-policy rule <*profile-name*> destination-ip {address-object *address-object*| address-group *address-group*| any}	Sets an IPv4 address or address group object to apply the policy to traffic going to it. Set this value to any to apply the policy to all traffic going to IPv4 addresses.
vrf main secure-policy rule <*profile-name*> service {service-object *service-object*| service-group *service-group*| any}	Sets a service or service group for the secure policy profile.
vrf main secure-policy rule <*profile-name*> content-filter-profile none	Uses this command if no content filter profiles have been created.
vrf main secure-policy rule <*profile-name*> content-filter-profile profile enabled {true| false} name <*profile-name*> log {no| by-profile}	Applies the (already-created) content filter profile to traffic that matches the secure-policy rule. log by-profile: Generates a log for all traffic that matches criteria in the content filter profile.
vrf main secure-policy rule <*profile-name*> ssl-inspection-profile none	Use this command if no SSL inspection profiles have been created.
vrf main secure-policy rule <*profile-name*> ssl-inspection-profile profile enabled {true| false} name <*profile-name*> log {no| by-profile}	Applies the (already-created) SSL inspection profile to traffic that matches the secure-policy rule. log by-profile: Generates a log for all traffic that matches criteria in the SSL inspection profile.
vrf main secure-policy rule <*profile-name*> app-patrol-profile none	Use this command if no app patrol profiles have been created.
vrf main secure-policy rule <*profile-name*> app-patrol-profile profile enabled {true| false} name <*profile-name*> log {no| by-profile}	Applies the (already-created) app patrol profile to traffic that matches the secure-policy rule. log by-profile: Generates a log for all traffic that matches criteria in the app patrol profile.
show config vrf main secure-policy	Displays the secure policy settings.
show state vrf main secure-policy	Displays the secure policy settings including matching packets.

12.3.1 Secure Policy Command Examples

These are IPv4 secure policy configuration examples.

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

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

```
usgflex200hp> edit running
usgflex200hp running config# object address-object address Dest_1 type range
10.0.0.10-10.0.0.15
t service MyService type tcp 1234
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# vrf main secure-policy rule Rule1 from zone-object WAN
usgflex200hp running config#! vrf main secure-policy rule Rule1 to zone-object LAN
usgflex200hp running config#! vrf main secure-policy rule Rule1 destination-ip
address-object Dest_1
usgflex200hp running config#! vrf main secure-policy rule Rule1 service service-
object MyService
usgflex200hp running config#! vrf main secure-policy rule Rule1 action allow
usgflex200hp running config#! vrf main secure-policy rule Rule1 user any
usgflex200hp running config#! vrf main secure-policy rule Rule1 schedule any
usgflex200hp running config#! vrf main secure-policy rule Rule1 source-ip any
usgflex200hp running config#! vrf main secure-policy rule Rule1 content-filter-
profile none
usgflex200hp running config#! vrf main secure-policy rule Rule1 ssl-inspection-
profile none
usgflex200hp running config#! vrf main secure-policy rule Rule1 app-patrol-profile
none
usgflex200hp running config# commit
Configuration committed.
```

12.4 DoS Prevention Overview

DoS attacks can flood your Internet connection with invalid packets and connection request, using so much bandwidth and so many resources that Internet access becomes unavailable. The goal of DoS attacks is not to steal information, but to disable a device or network on the Internet.

DoS prevention protects against anomalies based on violations of protocol standards (RFCs – Requests for Comments) and abnormal flows such as port scans. This section introduces DoS prevention profiles and applying a DoS prevention profile to a traffic direction.

Traffic Anomalies

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

12.5 DoS Prevention Command Input Values

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

Table 33 DoS Prevention Command Input Values

LABEL	DESCRIPTION
zone	The name of a zone. Use up to 30 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case- sensitive.
profile-name	The name of a DoS prevention profile. It can consist of alphanumeric characters, the underscore, and the dash, and it is 1-31 characters long. Spaces are not allowed.

12.6 DoS Prevention Commands

The following table describes the DoS prevention commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 34 DoS Prevention Commands

LABEL	DESCRIPTION
`vrf main dos-prevention enabled {true| false}`	Enables DoS prevention.
`vrf main dos-prevention profile <profile-name> description <description>`	Enter a description for the profile. You can use up to 60 printable ASCII characters .
`vrf main dos-prevention profile <profile-name> scan-detection {ip-protocol-scan| tcp-portscan| udp-portscan| icmp-sweep| ip-protocol-sweep| tcp-port-sweep| udp-port-sweep} action {none| block} enabled {true| false} logging {no| log| log-alert}`	Sets the scan detection options and actions. Generates a log (`log`) or a log and an alert (`log-alert`) when traffic matches the scan detection options you set.
`vrf main dos-prevention profile <profile-name> scan-detection sensitivity {low| medium| high}`	Sets scan-detection sensitivity.

Table 34 DoS Prevention Commands (continued)

LABEL	DESCRIPTION
vrf main dos-prevention profile <*profile-name*> scan-detection block-period <*1...3600*>	Sets how many seconds the Zyxel Device blocks all packets from being sent to the victim (destination) of a DoS attack.
vrf main dos-prevention profile <*profile-name*> flood-detection {icmp-flood| ip-flood| tcp-flood| udp-flood} action {none| block} enabled {true| false} logging {no| log| log-alert} threshold <*1...65535*>	Sets the flood detection options and actions. Generates a log (log) or a log and an alert (log-alert) when traffic matches the flood detection options you set. Sets a suitable threshold level (the number of packets per second that match the flood detection criteria) for your network. If you set a low threshold, most flood attacks will be detected, but you may have more logs and false positives. If you set a high threshold, some flood attacks may not be detected, but you will have fewer logs and false positives.
vrf main dos-prevention profile <*profile-name*> flood-detection block-period <*1...3600*>	Sets how many seconds the Zyxel Device blocks all packets from being sent to the victim (destination) of a DoS attack.
vrf main dos-prevention policy <*policy-name*> enabled {true| false}	Enables or disables the DoS prevention policy.
vrf main dos-prevention policy <*policy-name*> from-zone zone-object {any| zone *zone*}	Specifies the zone the traffic is coming from.
vrf main dos-prevention policy <*policy-name*> bind-profile <*profile-name*> enabled {true| false}	Binds the DoS prevention profile to the entry's traffic direction.
show config vrf main dos-prevetion	Displays DoS prevention settings.

12.7 System Protection Signature Commands

Use these commands to view the system protection signature information and update the signatures if necessary.

Table 35 System Protection Signature Commands

COMMAND	DESCRIPTION
show system protection signature version	Displays system protection signatures of the Zyxel Device. These signatures do not require a license. The Zyxel Device will synch with the Cloud Helper Server every day to update these signatures automatically. You can also update manually using the command below. Please note that in the web configurator, the system protection signature version displays in **Dashboard** > **About**. System protection signatures protect your Zyxel Device and local networks from web attacks, such as command injection, cross-site scripting and path traversal. Command injection: This is an attack in which an attacker uses the Zyxel Device vulnerabilities to execute commands to control your Zyxel Device. Cross-site scripting: This is an attack in which an attacker implants malicious scripts in a website. When you visit this website, the malicious scripts are sent and executed on your web browser. Path traversal: This is an attack that allows an attacker to access files you store in the web root folder.
show system protection signature update status	Displays if the system protection signatures are updated to the latest version.
cmd system protection signatures update signature	Use this command to update the system protection signatures to the latest version. Make sure the Zyxel Device can access the Cloud Helper Server when you want to update the signatures.

CHAPTER 13
IPSec VPN

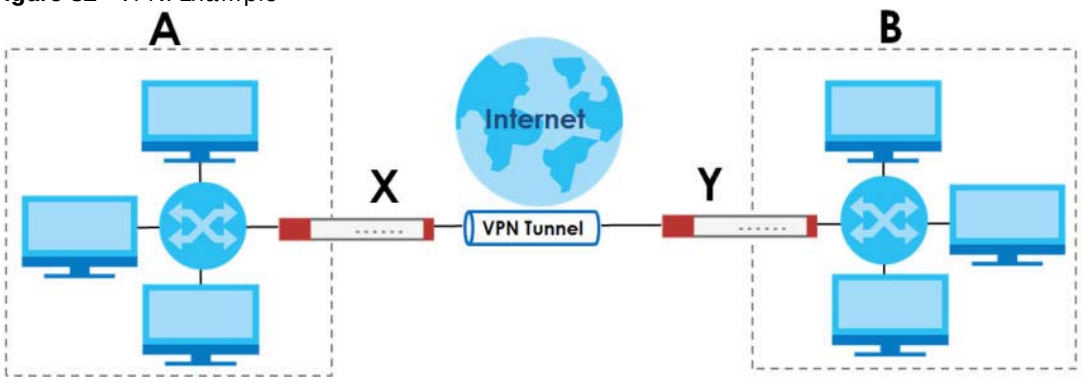
13.1 IPSec VPN Overview

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.

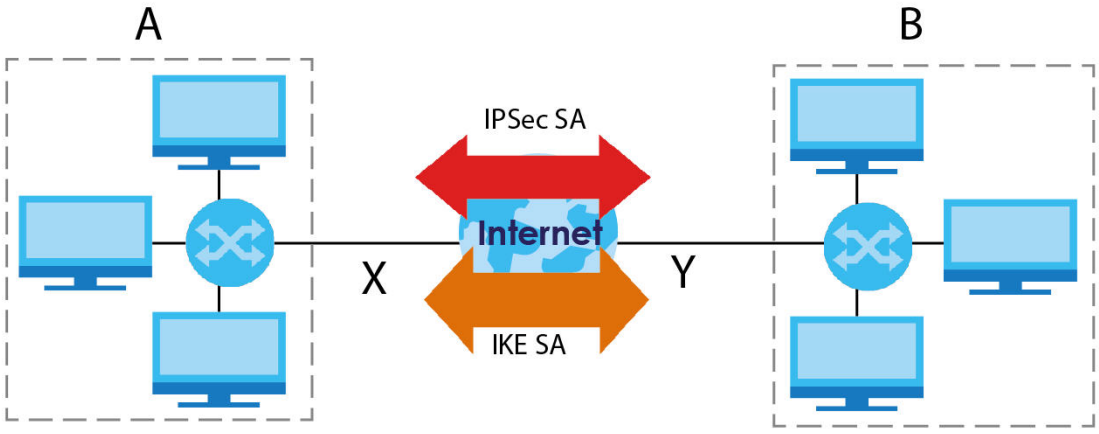
The following figure is one example of a VPN tunnel. Here local Zyxel Device **X** uses an IPSec VPN runnel to remote (peer) Zyxel Device **Y** to connect the local (**A**) and remote (**B**) networks.

Figure 32 VPN: Example



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

Figure 33 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.

13.2 IPSec VPN Command Input Values

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

Table 36 IPSec VPN Command Input Values

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

13.2.1 IPSec VPN Commands: Site-to-Site

This table lists the commands for site-to-site IPSec VPN.

Table 37 IPSec VPN Commands: Site-to-Site

COMMAND	DESCRIPTION
`vrf main ike enabled {true| false}`	Enables the IPSec VPN connection.
`vrf main ike pre-shared-key <key>`	Enter a password for authentication. Enter 8-128 alphanumeric characters (0-9a-zA-Z) or 8-128 pairs of hexadecimal characters (0-9A-F) beginning with 0x.

Table 37 IPSec VPN Commands: Site-to-Site

COMMAND	DESCRIPTION
vrf main ike ike-policy-template <*policy-name*>	Enter the name used to identify this rule. You may use 1-31 single-byte characters, including 0-9a-zA-Z, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
ike-proposal <*proposal*> {enc-alg <aes128-cbc| aes192-cbc| aes256-cbc| des-cbc| 3des-cbc>| auth-alg <hmac-md5| hmac-sha1| hmac-sha256| hmc-sha384| hmac-sha512>| dh-group <modp1024| modp1536| modp2048| modp3072| modp4096| ecp256| ecp384| ecp521| ecp256bp| ecp384bp| ecp512bp>}	Sets the encryption and authentication algorithms for each IKE SA proposal.
{remote-auth-method| local-auth-method} {pre-shared-key| certificate| eap-md5| eap-mschapv2}	Sets the authentication method for the remote IPSec router or the Zyxel Device. Sets the authentication method to pre-shared-key to use a password for authentication. Sets the authentication method to certificate to use one of the Zyxel Device certificates for authentication. Sets the authentication method to eap-md5 or eap-mschapv2 to use the selected algorithm for authentication.
aggressive {true| false}	Set aggressive to true to set IKEv1 to aggressive mode to establish an IKE SA faster. Set aggressive to false to set IKEv1 to main mode to establish an IKE SA in a more secure way.
vrf main ike ipsec-policy-template <*policy-name*>	Enter the name used to identify this rule. You may use 1-31 single-byte characters, including 0-9a-zA-Z, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
esp-proposal <*proposal*> {enc-alg <aes128-cbc| aes192-cbc| aes256-cbc| des-cbc| 3des-cbc>| auth-alg <hmac-md5| hmac-sha1| hmac-sha256| hmc-sha384| hmac-sha512>| dh-group <modp1024| modp1536| modp2048| modp3072| modp4096| ecp256| ecp384| ecp521| ecp256bp| ecp384bp| ecp512bp>}	Sets the active protocol to ESP and sets the encryption and authentication algorithms for each proposal.
dpd-action {clear| restart| trap}	Sets the DPD action the Zyxel Device performs.
replay-window <*0...4096*>	Sets the replay window size. The default value is 32. Sets the value to 0 to disable replay detection.
rekey-time <*180...3000000*>	Sets the IKE SA life time to the specified value. The default value is 28800.
rekey-packets <*0...65535*>	Sets the number of packets the Zyxel Device sends or receives before renegotiateing the IKE SA
rekey-bytes <*0...65535*>	Sets the number of bytes the Zyxel Device sends or receives before renegotiateing the IKE SA

Table 37 IPSec VPN Commands: Site-to-Site

COMMAND	DESCRIPTION
`vrf main ike vpn <policy-name>`	Enter the name used to identify this rule. You may use 1-31 single-byte characters, including 0-9a-zA-Z, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`ike-policy template <policy-name>`	Sets the IKE SA rule for the VPN rule.
`ipsec-policy template <policy-name>`	Sets the remote IPSec router rule for the VPN rule.
`version <0...2>`	Sets IKEv1 or IKEv2. IKEv1 applies to IPv4 traffic only. IKEv2 applies to both IPv4 and IPv6 traffic. Sets the value to 0 to have the Zyxel Device accept both IKEv1 and IKEv2.
`local-address <ipv4| subnet>`	Type the IP address of a computer on your network that can use the tunnel. You can also specify a subnet. This must match the remote IP address configured on the remote IPSec device.
`remote-address <ipv4| subnet>`	Type the IP address of a computer behind the remote IPSec device. You can also specify a subnet. This must match the local IP address configured on the remote IPSec device.
`local-id <ipv4| domain-name| email>`	Enter one of the followings to identify the Zyxel Device during authentication. IPv4 - the Zyxel Device is identified by an IP address DNS - the Zyxel Device is identified by a domain name E-mail - the Zyxel Device is identified by the string specified in this field
`remote-id <ipv4| domain-name| email| any| subject-name>`	Enter one of the followings to identify the remote IPSec router during authentication. IPv4 - the remote IPSec router is identified by an IP address DNS - the remote IPSec router is identified by a domain name E-mail - the remote IPSec router is identified by the string specified in this field Any - the Zyxel Device does not check the identity of the remote IPSec router If the Zyxel Device and remote IPSec router use certificates, there is one more choice. Subject Name - the remote IPSec router is identified by the subject name in the certificate

13.2.2 IPSec VPN Commands: Remote Access

This table lists the commands for remote access IPSec VPN.

Table 38 IPSec VPN Commands: Remote Access

COMMAND	DESCRIPTION
`vrf main ike ike-policy-template RemoteAccessike-t allowed-users <user>`	Sets a user or user group to associate the user or user group to the remote access IPSec VPN policy.
`vrf main ike ike-policy-template Remote Accessike-t ike-proposal 1 enc-alg {aes128-cbc| aes192-cbc| aes256-cbc| des-cbc| 3des-cbc}`	Sets the key size and encryption algorithm. des-cbc - a 56-bit key with the DES encryption algorithm 3des-cbc - a 168-bit key with the DES encryption algorithm aes128-cbc - a 128-bit key with the AES encryption algorithm aes192-cbc - a 192-bit key with the AES encryption algorithm aes256-cbc - a 256-bit key with the AES encryption algorithm The Zyxel Device and the remote IPSec router must both have at least one proposal that uses use the same encryption and the same key. Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.
`vrf main ike ike-policy-template Remote Accessike-t ike-proposal 1 auth-alg {hmac-md5| hmac-sha1| hmac-sha256| hmac-sha384| hmac-sha512}`	Sets the hash algorithm to use to authenticate packet data. SHA is generally considered stronger than MD5, but it is also slower. The Zyxel Device and the remote IPSec router must both have a proposal that uses the same authentication algorithm.
`vrf main ike ike-policy-template Remote Accessike-t ike-proposal 1 dh-group <dh-group>`	Sets the Diffie-Hellman key group you want to use to create encryption keys. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. The Zyxel Device and the remote IPSec router must use the same DH key group. Different operating systems may support different DH key groups. Check your operating system documentation. • For Windows VPN clients, Zyxel SecuExtender perpetual VPN clients versions 3.8.203.61.32 and earlier support DH1 to DH14. • For macOS VPN clients, Zyxel SecuExtender subscription VPN clients versions 1.2.0.7 and later support DH14 to DH21. For Windows VPN clients, Zyxel SecuExtender subscription VPN clients versions 5.6.80.007 and later support DH14 to DH21. • Windows versions 7, 10, 11 built-in IKEv2 VPN clients support DH2 by default. • macOS versions 14.2 and later built-in IKEv2 VPN clients support DH14 by default. • iOS versions 10.15 and later built-in IKEv2 VPN clients support DH14 by default.

Table 38 IPSec VPN Commands: Remote Access

COMMAND	DESCRIPTION
vrf main ike ike-policy-template Remote Accessike-t ike-proposal 1 {local-auth-method| remote-auth-method} {pre-shared-key| certificate| xauth| eap-md5| eap-mschapv2}	Sets the authentication method for the remote IPSec router or the Zyxel Device. Sets the authentication method to pre-shared-key to use a password for authentication. Sets the authentication method to certificate to use one of the Zyxel Device certificates for authentication. Set the authentication method to xauth to use extended authentication. Sets the authentication method to eap-md5 or eap-mschapv2 to use the selected algorithm for authentication.
vrf main ike ike-policy-template Remote Accessike-t auth-server *<1...2>* *<auth-server>*	Sets a specified RADIUS server for the Zyxel Device to use for authentication.
vrf main ike ike-policy-template Remote Accessike-t aggressive {true| false}	Set aggressive to true to use aggressive mode to establish an IKE SA faster. Set aggressive to false to use main mode to establish an IKE SA in a more secure way.
vrf main ike ike-policy-template Remote Accessike-t rekey-time *<180...3000000>*	Sets the IKE SA life time to the specified value. The default value is 86400.

13.3 IPSec VPN Debug Commands

This table lists the IPSec VPN debug commands.

Table 39 IPSec VPN Debug Commands

COMMAND	DESCRIPTION
cmd debug ipsec trace log debug-level *<0...4>*	Generates IPSec debug logs. Enter 0-4 to set the debug-level. The higher the number, the more detailed the log is.
cmd debug ipsec save log debug-level *<0...4>*	Saves the IPSec debug logs to the Zyxel Device with the specified debug level. To see details on errors, download the log file using FTP from /tmp/ipsecvpn.log. Enter 0-4 to set the debug-level. The higher the number, the more detailed the log is.

13.4 IPSec VPN Command Examples

These are some other example IPSec VPN usage commands.

```
usgflex200hp> edit running
usgflex200hp running config# cmd debug ipsec trace log debug-level 2
no events, waiting
created thread 02 [23369]no events, waiting
created thread 03 [23370]
started worker thread 03
watcher going to poll() 2 fds
watched FD 8 ready to read
watcher going to poll() 1 fds

started worker thread 02
created thread 04 [23371]
started worker thread 04
watcher got notification, rebuilding
watcher going to poll() 2 fds
usgflex200hp running config# cmd debug ipsec save log debug-level 2
ipsec-save-log
    ok
        msg ""
        ..
    .
```

CHAPTER 14
SSL VPN

14.1 SSL Access Policy

An SSL access policy allows the Zyxel Device to perform the following tasks:

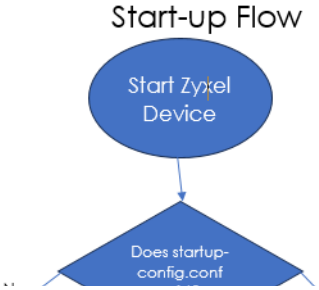
- Limit user access to specific applications or files on the network
- Allow user access to specific networks
- Assign private IP addresses and provide DNS/WINS server information to remote users to access internal networks.

14.1.1 What You Need to Know

Full Tunnel Mode

In full tunnel mode, a virtual connection is created for remote users with private IP addresses in the same subnet as the local network. This allows them to access network resources in the same way as if they were part of the internal network.

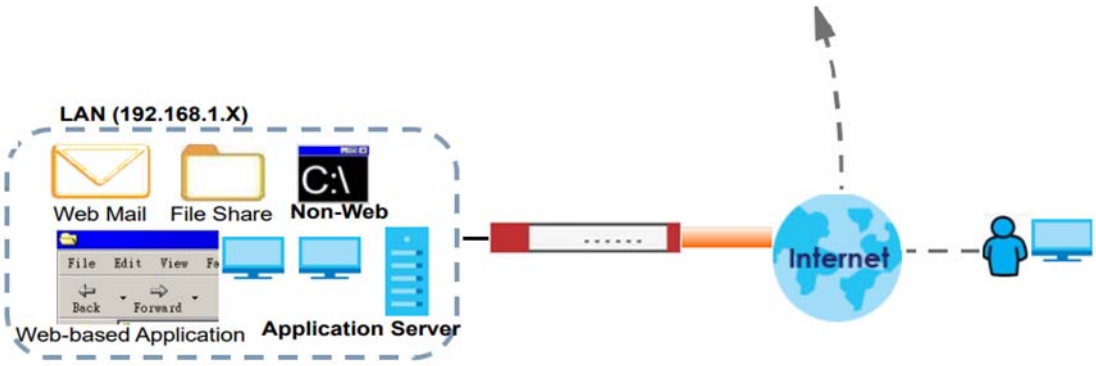
Figure 34 Network Access Mode: Full Tunnel Mode



Split Tunnel Mode

In split tunnel mode, only the traffic going to the networks behind the Zyxel Device is encrypted. Traffic going to the Internet from the remote client does not go through the Zyxel Device and is not encrypted.

Figure 35 Network Access Mode: Split Tunnel Mode



SSL Access Policy Objects

The SSL access policies reference the following objects. If you update this information, in response to changes, the Zyxel Device automatically propagates the changes through the SSL policies that use the object(s). When you delete an SSL policy, the objects are not removed.

Table 40 Objects

OBJECT TYPE	OBJECT SCREEN	DESCRIPTION
User Accounts	User Account/ User Group	Sets the user account or user group to which you want to apply this SSL access policy.
Application	SSL Application	Sets an SSL application object for specifying the type of application and the address of the local computer, server, or web site SSL users are to be able to access.
IP Pool	Address	Sets an address object to define a range of private IP addresses to assign to user computers so they can access the internal network through a VPN connection.
Server Addresses	Address	Sets address objects for the IP addresses of the DNS and WINS servers that the Zyxel Device sends to the VPN connection users.
VPN Network	Address	Sets an address object for the network segment users are allowed to access through a VPN connection.

Please note that you cannot delete an object that is referenced by other settings.

14.2 SSL VPN Commands

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

Table 41 Input Values for SSL VPN Commands

LABEL	DESCRIPTION
user-account	The name of a user or 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.

14.2.1 SSL VPN Commands

This table lists the commands for SSL VPN. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 42 SSL VPN Commands

COMMAND	DESCRIPTION
`vrf main sslvpn-server enabled {true| false}`	Enables the SSL VPN policy.
`vrf main sslvpn-server bind-interface <interface>`	Sets the interface or incoming traffic to the Zyxel Device.
`vrf main sslvpn-server listen-port <1...65535>`	Sets the SSL VPN server port of the Zyxel Device for full tunnel mode SLL VPN access. Leave this field to default settings unless it conflicts with another interface.
`vrf main sslvpn-server proto {tcp| udp}`	Sets the SSL VPN server port to use TCP or UDP for communication.
`vrf main sslvpn-server server-subnet <ipv4_cidr>`	Sets IP address pool that is used to assign IP addresses to the VPN clients. Enter an IPv4 address in CIDR format, for example, 10.8.0.0/24.
`vrf main sslvpn-server {keepalive-interval| keepalive-timeout} <1...65535>`	`keepalive-interval`: Sets the interval between each keep alive message sent by the Zyxel Device. The default value is 10. `keepalive-timeout`: Sets the maximum time the Zyxel Device waits to receive a keep alive message from the remote SSL VPN router before it declares that the remote SSL VPN router is dead. The default value is 120. The interval should be less than the wait time.
`vrf main sslvpn-server auth {rsa-sha224| rsa-sha256| rsa-sha384| rsa-sha512}`	Sets the authentication algorithm used to authenticate SSL VPN clients. `rsa-sha224` is less secure but more compatible with different clients and applications. `rsa-sha512` is more secure but less compatible.
`vrf main sslvpn-server auth-server <1...2> <auth-server>`	Sets a specified RADIUS server for the Zyxel Device to use for authentication.
`vrf main sslvpn-server cipher {aes-128-cbc| aes-192-cbc| aes-256-cbc}`	Sets the encryption algorithm used to encrypt SSL VPN clients.
`vrf main sslvpn-server full-tunnel {true| false}`	Enables `full-tunnel` to encrypt all traffic through the VPN.
`vrf main sslvpn-server full-tunnel-through-wan {true| false}`	Enables `full-tunnel-through-wan` to allow only traffic encrypted by the Zyxel Device from the remote client to the Internet.
`vrf main sslvpn-server dns-servers {ZyWALL| ipv4}`	Specifies the IP address of the DNS server whose information the Zyxel Device sends to the remote users. This allows them to access devices on the local network using domain names instead of IP addresses. `ZyWALL`: the PVN clients use the IP address of the interface you specified and the Zyxel Device works as a DNS relay. `ipv4`: enter a static IPv4 address.

Table 42 SSL VPN Commands

COMMAND	DESCRIPTION
`vrf main sslvpn-server split-tunnel <ipv4_cidr>`	Enables `split-tunnel` to only encrypt traffic going to networks behind the Zyxel Device. Enter an IPv4 address in CIDR notation, for example, 10.8.0.0/24. Traffic going to the Internet from this IP address is encrypted. Traffic going to the Internet from the remote client does not go through the Zyxel Device is not encrypted.
`vrf main sslvpn-server allowed-user <user-account>`	Specifies a user or user group to associate the user or user group to the SSL VPN policy.

CHAPTER 15
Bandwidth Management

15.1 Bandwidth Management Overview

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

15.1.1 BWM Type

The Zyxel Device supports **shared** bandwidth management. All users to which the rule is applied need to share the bandwidth configured in the rule.

15.2 Bandwidth Management Commands

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

Table 43 BWM Commands

COMMAND	DESCRIPTION
`vrf main bwm enabled {true| false}`	Enables bandwidth management on the Zyxel Device.
`vrf main bwm rule <profile-name> enable {true| false}`	Enables the BWM policy profile.
`vrf main bwm rule <profile-name> user <user-name>`	Enter a user or user group object name of the rule.
`vrf main bwm rule <profile-name> description <description>`	Enter a description of this policy. It is not used elsewhere. You can use alphanumeric and ()+/:+?!*#@$_%- characters, and it can be up to 60 characters long.
`vrf main bwm rule <profile-name> incoming <interface-name>`	Specifies the source interface of the traffic to which this policy applies.
`vrf main bwm rule <profile-name> outgoing <interface-name>`	Specifies the destination interface of the traffic to which this policy applies.
`vrf main bwm rule <profile-name> source <address-name>`	Sets a source address or address group, including geographic address, for whom this policy applies. Enter any if the policy is effective for every source.
`vrf main bwm rule <profile-name> destination <address-name>`	Sets a destination address or address group, including geographic address, for whom this policy applies. Enter any if the policy is effective for every destination.

Table 43 BWM Commands (continued)

COMMAND	DESCRIPTION
vrf main bwm rule <*profile-name*> service <*service-name*>	Sets a service or service group to identify the type of traffic to which this policy applies. any means all services.
vrf main bwm rule <*profile-name*> application <*application-name*>	Sets an application to identify the specific traffic to which this policy applies. If you enter BitTorrent, it includes the services listed below at the time of writing: • BitTorrent • BitTorrent_FileTransfer • BitTorrent_Application • BitTorrent_Bundle
vrf main bwm rule <*profile-name*> logging to {no| log| log-alert}	Sets whether to have the Zyxel Device generate a log (log), log and alert (log-alert) or neither (no) when any traffic matches this policy.
vrf main bwm rule <*profile-name*> download <*0...10000*>	Sets how much inbound bandwidth, in megabits per second, this policy allows the traffic to use when there are other services or applications using the interface's bandwidth. Inbound refers to the traffic the Zyxel Device sends to a connection's initiator. Enter 0 to apply bandwidth management for the matching traffic which is the maximum amount your Zyxel Device can transmit. Enter 1-10000 to apply bandwidth management for matching traffic from 1 to 10,000 Mbps. If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
vrf main bwm rule <*profile-name*> *download-maximum* <*0...10000*>	Sets how much inbound bandwidth, in megabits per second, this policy allows the traffic to use when there are no other services or applications using the interface's bandwidth. Inbound refers to the traffic the Zyxel Device sends to a connection's initiator. Enter 0 to apply bandwidth management for the matching traffic which is the maximum amount your Zyxel Device can transmit. Enter 1-10000 to apply bandwidth management for matching traffic from 1 to 10,000 Mbps. Note: Traffic matching a Limited policy may "borrow" all unused bandwidth on the inbound interface. If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
vrf main bwm rule <*profile-name*> upload <*0...10000*>	Sets how much outbound bandwidth, in megabits per second, this policy allows the traffic to use when there are other services or applications using the interface's bandwidth. Inbound refers to the traffic the Zyxel Device sends to a connection's initiator. Enter 0 to apply bandwidth management for the matching traffic which is the maximum amount your Zyxel Device can transmit. Enter 1-10000 to apply bandwidth management for matching traffic from 1 to 10,000 Mbps. If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.

Table 43 BWM Commands (continued)

COMMAND	DESCRIPTION
vrf main bwm rule *<profile-name> upload-maximum <0...10000>*	Sets how much outbound bandwidth, in megabits per second, this policy allows the traffic to use when there are no other services or applications using the interface's bandwidth. Outbound refers to the traffic the Zyxel Device sends to a connection's initiator. Enter `0` to apply bandwidth management for the matching traffic which is the maximum amount your Zyxel Device can transmit. Enter `1-10000` to apply bandwidth management for matching traffic from 1 to 10,000 Mbps. Note: Traffic matching a Limited policy may "borrow" all unused bandwidth on the inbound interface. If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
vrf main bwm rule *<profile-name> priority <0...7>*	Enter a number between 0 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority. 0 is for real-time traffic such as video, and 7 is for lowest priority traffic such as background traffic. Traffic with a higher priority is given bandwidth before traffic with a lower priority. When traffic with higher priority has reached the full bandwidth, the traffic with lower priority can use the remaining bandwidth. The Zyxel Device uses priority queueing scheduler to divide bandwidth between traffic flows with the same priority. The number in this field is ignored if the download and upload limits are both set to Unlimited.
show bwm-applications	Shows the applications the Zyxel Device can apply the bandwidth management policy.

CHAPTER 16
Application Patrol

16.1 Application Patrol Overview

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

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

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

The following sections list the application patrol commands.

16.2 Application Patrol General Commands

The following table describes the application patrol general commands.

Table 44 app Commands: Application Patrol

COMMAND	DESCRIPTION
`show app-patrol-{categories| applications| signature-version}`	`categories`: Displays all the category IDs, names and numbers of applications that belong to each category. `applications`: Displays all the application IDs and names. `signature-version`: Displays the application patrol signature version, signature number and released date.
`show config vrf main app-patrol rule`	Displays the settings of the application patrol rules you configured.
`cmd app-patrol-query {name| category} <app-name| category-id>`	Sets an application name to display all related applications. Sets an application category ID to display all applications that belong to the specified category.
`cmd app-patrol-statistics-flush`	Clears all application patrol statistics.

16.3 Application Patrol Commands

The following table describes the application patrol commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 45 app Commands: Application Patrol

COMMAND	DESCRIPTION
`vrf main app-patrol statistics enabled {true| false}`	Enables application patrol statistics gathering. The `false` command disables it.
`vrf main app-patrol rule <rule-name>`	Creates an application patrol rule with the specified name. You may use 1-30 alphanumeric characters and also underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`description <description>`	Write a description for the application patrol rule.
`multiple-application <0...4294967295>`	Creates a profile of application patrol settings. You can create multiple profiles with different settings under the same rule.
`sid <sid>`	Enters an application ID to add it to the application patrol profile you are configuring.
`action {forward| drop| reject}`	Sets the action when traffic matches the settings you configured in this profile. Actions are: • `forward` - routes packets that matches these signatures. • `drop` - silently drops packets that matches these signatures without notification. • `reject` - drops packets that matches these signatures and sends notification.
`logging {no| log| log-alert}`	Generates a log, log and alert or neither (no) when traffic matches the settings you configured in this profile.

16.4 Application Patrol Statistics

The following table describes the commands for displaying application patrol statistics.

Table 46 Commands for Application Patrol Statistics

COMMAND	DESCRIPTION
`show config vrf main app-patrol statistics enabled`	Displays if the application patrol statistics collection is enabled.
`show state vrf main app-patrol statistics top-entry usage entry {app-name| category| usage-byte| usage-percent}`	Queries the top five application patrol statistics by application names, categories, usage by bytes and usage by percent.

16.4.0.1 Application Patrol Command Examples

This command shows details of an application patrol rule created.

```
usgflex200hp> show config vrf main app-patrol rule
rule 1
    multiple-application 4294967295
        sid 15728640
        action drop
        logging log-alert
```

The example below shows you how to create and configure an application patrol rule.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main app-patrol rule config1
usgflex200hp running rule config1# multiple-application 1
usgflex200hp running multiple-application 1# sid 32964608
usgflex200hp running multiple-application 1# sid 15728640
usgflex200hp running multiple-application 1# action drop
usgflex200hp running multiple-application 1# logging log-alert
usgflex200hp running multiple-application 1# commit
Configuration committed.
```

CHAPTER 17
Anti-Malware

17.1 Anti-Malware Overview

Malware is short for malicious software, such as computer viruses, worms and spyware. The Zyxel Device anti-malware feature protects your connected network from malware by scanning traffic coming in from the WAN and going out from the WAN for malware signature matches.

The traffic scanned by the Zyxel Device may include HTTP traffic, FTP traffic and email with attachments. The traffic is scanned for signature patterns found in the Defend Center database.

Viruses, Worms, and Spyware

A computer virus is a type of malicious software designed to corrupt and/or alter the operation of other legitimate programs. A worm is a self-replicating virus. Spyware infiltrates your device to secretly gather information, such as your network activity, passwords, bank details, and so on.

Types of Malware

The following table describes some of the common malware.

Table 47 Common Malware Types

TYPE	DESCRIPTION
File Infector	This is a small program that embeds itself in a legitimate program. A file infector is able to copy and attach itself to other programs that are executed on an infected computer.
Boot Sector Virus	This type of virus infects the area of a hard drive that a computer reads and executes during startup. The virus causes computer crashes and to some extend renders the infected computer inoperable.
Macro Virus	Macro viruses or Macros are small programs that are created to perform repetitive actions. Macros run automatically when a file to which they are attached is opened. Macros spread more rapidly than other types of viruses as data files are often shared on a network.
Email Virus	Email viruses are malicious programs that spread through email.
Polymorphic Virus	A polymorphic virus (also known as a mutation virus) tries to evade detection by changing a portion of its code structure after each execution or self replication. This makes it harder for an anti-malware scanner to detect or intercept it. A polymorphic virus can also belong to any of the virus types discussed above.

Hash Value

A hash function is an algorithm that maps data of arbitrary size to data of fixed size. The value returned by a hash function is a hash value. Hash values can be used to identify if the contents of a file have changed. At the time of writing, the MD5 (Message Digest 5) hash algorithm is supported.

Cloud Query

The Zyxel Device queries the **Defend Center** database by sending the file's hash value and receiving the scan results through the Defend Center.

17.2 Anti-Malware Commands

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

Table 48 Input Values for General Anti-Malware Commands

LABEL	DESCRIPTION
md5-pattern *file-pattern*	Use up to 80 single-byte characters to specify a file pattern. Single-byte characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed. A question mark (?) represents a single character wildcard. For example, use "a?.zip" (without the quotation marks) to specify aa.zip, ab.zip and so on. An asterisk (*) represents a multiple character wildcard. For example, use "*a.zip" (without the quotation marks) to specify any file that ends with "a.zip". A file named "testa.zip" would match. There could be any number (of any type) of characters in front of the "a.zip" at the end and the file name would still match. A file named "test.zipa" for example would not match. A * in the middle of a pattern has the Zyxel Device check the beginning and end of the file name and ignore the middle. For example, with "abc*.zip", any file starting with "abc" and ending in ".zip" matches, no matter how many characters are in between. The whole file name has to match if you do not use a question mark or asterisk. If you do not use a wildcard, the Zyxel Device checks up to the first 80 characters of a file name.

17.2.1 General Anti-Malware Commands

The following table describes general anti-malware commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Note: You must register for the anti-malware service in order to use it.

Table 49 General Anti-Malware Commands

COMMAND	DESCRIPTION
`vrf main anti-malware enabled {true| false}`	Enable the anti-malware service. The anti-malware service depends on anti-malware service registration.
`vrf main anti-malware scan-mode express enabled {true| false}`	Enable or disable the anti-malware scan mode. Express mode is a scan mode in which Zyxel Device scans files that match the list of user-defined file types using cloud query.
`vrf main anti-malware file-size-limit <1...10>`	Sets the limit of the file size in megabyte (MB) the Zyxel Device anti-malware will scan. A file that exceeds the file size you set here will pass without been scanned by the Zyxel Device anti-malware.

Table 49 General Anti-Malware Commands (continued)

COMMAND	DESCRIPTION
`vrf main anti-malware cloud-query file-type`	Adds or removes a file type from the list of user-defined file types that cloud query will scan. Allowed values: 7z, AVI, BMP, BZ2, EXE, Flash, GIF, Gz, JPG, MOV, MP3, MPG, "MS Office", PDF, PNG, RAR, RM, RTF, TIFF, WAV, ZIP.
`vrf main anti-malware eicar-detection enabled {true| false}`	Turns detection of the EICAR test file on or off. The EICAR test file is a standardized test file for signature based anti-malware scanners. When the scanner detects the EICAR file, it responds in the same way as if it found real malware. The EICAR file can also be compressed to test whether the anti-malware software can detect it in a compressed file. The test string consists of the following human-readable ASCII characters.
`vrf main anti-malware default-port enabled {true| false}`	Has the Zyxel Device only scan traffic going through the specified ports. The default specified ports are 21, 25, 80, 110, 143, 443, 465, 990, 993, 995, 3128 and 8080. You can remove or add a port to this list by using the `extra-port` or the `exception-port` commands. Disables this to have the Zyxel Device scan traffic going through all ports.
`vrf main anti-malware default-port {extra-port| exception-port}` *`port number`*	`extra-port`: Adds a port to the default specified port list. `exception-port`: Removes a port from the default specified port list.
`show state vrf main anti-malware default-port-state`	Displays the ports the Zyxel Device will scan when you set `vrf main anti-malware default- port enabled` to `true`.
`vrf main anti-malware default-profile infected-action {none| destroy}`	Sets the action to take when the Zyxel Device detects a malware in a file. The file can be "destroyed" by overwriting a portion of the file with zeros before forwarding to the user.
`vrf main anti-malware default-profile logging {no| log| log-alert}`	Sets whether the Zyxel Device should create a log message and an optional alert if it finds a malware in a file.
`vrf main anti-malware statistics enabled {true| false}`	Has the Zyxel Device collect the anti-malware statistics.
`show config vrf main anti-malware {default-profile| statistics| eicar-detection| cloud-query| allow-list| block-list| default-port| enabled| scan-mode}`	Displays: • default profile, cloud query, scan mode, allow list and block list settings. • if EICAR detection, statistics collection, default port and anti-malware are enabled.

17.2.2 Allow and Block Lists

The following table describes the commands for configuring the allow list and block list. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 50 Commands for the Anti-Malware Allow/Block Lists

COMMAND	DESCRIPTION
`vrf main anti-malware allow-list enabled {true| false}`	Enable or disable the allow list. When activated, the Zyxel Device does not perform anti-malware checks on files that match any of the allow list file patterns.
`vrf main anti-malware allow-list {md5-hash` *`md5-pattern`* `| file-name-pattern` *`file-pattern`*`} enabled {true| false}`	Adds an MD5 hash pattern or file name pattern to the allow list if it did not already exist, and then activates or deactivates the pattern. A file name pattern listed in the allow list allows incoming files with names that match the pattern.
`vrf main anti-malware allow-list logging {no| log}`	Sets whether the Zyxel Device should create a log message when a packet matches the allow list file patterns.
`show config vrf main anti-malware allow list {md5-hash| file-name-pattern| enabled| logging}`	Displays the anti-malware allow list settings.
`vrf main anti-malware block-list enabled {true| false}`	Enable or disable the block list. When activated, the Zyxel Device logs and deletes files with names that match any of the block list file patterns.
`anti-malware block-list {md5-hash` *`md5-pattern`* `| file-name-pattern` *`file-pattern`*`} enabled {true| false}`	Adds an MD5 hash pattern or file pattern to the block list if it did not already exist, and then activates or deactivates the pattern. A file name pattern listed in the block list blocks incoming files with names that match the pattern.
`vrf main anti-malware block-list logging {no| log}`	Sets whether the Zyxel Device should create a log message when a packet matches the block list file patterns.
`show config vrf main anti-malware block list {md5-hash| file-name-pattern| enabled| logging}`	Displays the anti-malware block list settings.

17.2.2.1 Allow List Example

This example shows how to enable the allow list and configure an active allow list entry.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main anti-malware allow-list enabled true
usgflex200hp running config# vrf main anti-malware allow-list logging log
usgflex200hp running config# vrf main anti-malware allow-list md5-hash
BB1372E462191A9C955906A152C59E89
usgflex200hp running md5-hash BB1372E462191A9C955906A152C59E89# enabled true
usgflex200hp running md5-hash BB1372E462191A9C955906A152C59E89# save
usgflex200hp running md5-hash BB1372E462191A9C955906A152C59E89# exit
```

17.3 Anti-Malware Statistics

The following table describes the commands for collecting and displaying anti-malware statistics.

Table 51 Commands for Anti-Malware Statistics

COMMAND	DESCRIPTION
show state vrf main anti-malware statistics summary malware-detected-count	Displays the number of times the Zyxel Device detects malware that matches the signatures.
show state vrf main anti-malware statistics event entry {timestamp| source-ip| destination-ip| hash| virus-name}	Displays anti-malware statistics entries by time, destination IP address, source IP address, virus name or hash value.
show state vrf main anti-malware statistics top-entry {virus-name| source-ip| destination-ip}	Displays the top five anti-malware statistics entries by destination IP address, source IP address or virus name.
cmd anti-malware-statistics-flush	Clears the collected statistics.

17.3.1 Anti-Malware Statistics Example

This example shows how to collect and display anti-malware statistics.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main anti-malware statistics enabled true
usgflex200hp running config# show config vrf main anti-malware statistics enabled
enabled true
usgflex200hp running config# show state vrf main anti-malware statistics summary
summary
malware-detected-count 0
```

17.4 Anti-Malware Debug Commands

The following table describes the commands for collecting and displaying anti-malware statistics.

Table 52 Debug Commands for Anti-Malware

COMMAND	DESCRIPTION
cmd debug anti-malware cloud-query cache {enable | disable | flush}	Enables or disables saving of results of anti-malware queries to the cloud on the Zyxel Device. Use flush to clear all previously saved anti-malware queries on the Zyxel Device. You may want to do this if there are false positive query results.
cmd debug anti-malware local-loop-mode	Displays anti-malware connection status from the Zyxel Device to the cloud query server.
cmd debug anti-malware clean-log enabled {true | false}	Enables or disables removing anti-malware logs saved on the Zyxel Device.

17.4.1 Anti-Malware Debug Commands Examples

This example shows some example anti-malware debug cloud query commands.

Figure 36 Debug Cloud Query Commands

```
usgflex500h> edit running
usgflex500h running config# cmd debug anti-malware cloud-query cache enable
anti-malware-debug-cloud-query-cache
    ok
        status "change cloud-query-cache Ok.
"
        ..
 cmd debug anti-malware cloud-query cache disable
anti-malware-debug-cloud-query-cache
    ok
        status "change cloud-query-cache Ok.
"
        ..
cmd debug anti-malware cloud-query cache flush
anti-malware-debug-cloud-query-cache
    ok
        status "change cloud-query-cache Ok.
"
        ..
```

This example shows an example of the anti-malware debug local loop command.

Figure 37 Debug Local Loop Command

```
usgflex500h> edit running
usgflex500h running config# cmd debug anti-malware local-loop-mode
anti-malware-debug-cloud-query-am-local-loop-mode
    ok
        status "change local-loop-mode Ok.
"
        ..
```

This example shows an example of removing the anti-malware logs from the Zyxel Device.

Figure 38 Debug Remove Anti-Malware Logs Command

```
usgflex500h> edit running
usgflex500h running config#  cmd debug anti-malware clean-log enabled true
anti-malware-debug-cloud-query-clean-log
    ok
        status "change clean-log Ok.
"
        ..
```

CHAPTER 18
Reputation Filter

18.1 Overview

Use the **Reputation Filter** commands to configure settings for IP Reputation, DNS Threat Filter and URL Threat filtering.

IP Reputation

IP reputation checks the reputation of an IPv4 address from a database. An IP is considered to have a bad reputation if suspicious activities, such as spam, virus, and/or phishing have come from it. The Zyxel Device will respond when there are packets coming from an IPv4 address with a bad reputation.

URL Threat Filter

URL filtering compares access to specific URLs against a database of blocked or allowed sites. Sites on the database are sorted into categories such as:

Anonymizers	Browser Exploits
Malicious Downloads	Malicious Sites
Phishing	Spam URLs
Spyware Adware Keyloggers	

DNS Threat Filter

DNS threat filtering inspects DNS queries made by clients on your network and compares the queries against a database of blocked or allowed Fully Qualified Domain Names (FQDNs). The Zyxel Device DNS Threat Filter will either drop the DNS query or reply to the user with a fake DNS response.

The following types of DNS queries are inspected by the Zyxel Device:
- Type "A" ...
- Type "AAAA" ...
- Type "NS" ...
- Type "MX" ...
- Type "CNAME" ...
- Type "PTR" ...
- Type "SOA" ...

The Zyxel Device replies with a DNS reply packet containing a fake IP address for type "A", and replies with a DNS reply packet with server failure code for remaining types.

18.1.1 Threat Checking Priority

IP Reputation

The priority for IP Reputation checking is as follows:

1. Allow List
2. SecuReporter Allow List
3. Block List
4. External Block List
5. Local Zyxel Device Signatures

URL Threats

The priority for URL Threat checking is as follows:

1. Allow List
2. SecuReporter Allow List
3. Block List
4. External Block List
5. Cloud Query Cache
6. Cloud Query

DNS Threats

The priority for DNS Threat Filter checking is as follows:

1. Allow List
2. SecuReporter Allow List
3. Block List
4. External Block List
5. Cloud Query Cache
6. Cloud Query

18.2 IP Reputation Commands

The following table describes general IP reputation commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 53 IP Reputation Commands

COMMAND	DESCRIPTION
`vrf main ip-reputation allow-list enabled {true| false}`	Enables the IP reputation allow list to allow: • Incoming packets that come from the listed IPv4 addresses. • Outgoing packets that go to the listed IPv4 addresses.
`vrf main ip-reputation allow-list logging {no| log}`	Sets whether the Zyxel Device generates a log when: • Incoming packets come from the IPv4 addresses listed in the allow list. • Outgoing packets going to the IPv4 addresses listed in the allow list. The Zyxel Device will not generate a log if you use the no command.
`vrf main ip-reputation allow-list ip-list <IPv4 address> enabled {true| false} [description <description>]`	Adds the specified IPv4 address on the IP reputation allow list. You can also add an IP address block using CIDR notation, for example 192.168.0.1/24. A description is optional.
`vrf main ip-reputation block-list enabled {true| false}`	Enables the IP reputation allow list to block: • Incoming packets that come from the listed IPv4 addresses. • Outgoing packets that go to the listed IPv4 addresses.
`vrf main ip-reputation block-list logging {no| log| log-alert}`	Sets whether the Zyxel Device generates a log or a log and an alert when: • Incoming packets come from the IPv4 addresses listed in the block list. • Outgoing packets going to the IPv4 addresses listed in the block list. The Zyxel Device will not generate a log if you use the no command.
`vrf main ip-reputation block-list ip-list <IPv4 address> enabled {true| false} [description <description>]`	Adds the specified IPv4 address on the IP reputation block list. You can also add an IP address block using CIDR notation, for example 192.168.0.1/24. A description is optional.
`vrf main ip-reputation enabled {true| false}`	Enables the IP reputation filtering service on the Zyxel Device. The `false` command disables the IP reputation filtering service.
`vrf main ip-reputation action {allow| block}`	Sets what action the Zyxel Device takes when a packet arrives from or goes to an IPv4 address with a bad reputation. `allow`: The Zyxel Device allows the packet to go through. `block`: The Zyxel Device denies the packet, and then sends a TCP RST to both the packet sender and receiver.
`vrf main ip-reputation system-protect enabled {true | false}`	Blocks packets with a bad reputation going to or arriving from the Zyxel Device.
`vrf main ip-reputation logging {no| log| log-alert}`	Sets whether the Zyxel Device generates a log or a log and an alert when: • Incoming packets come from an IPv4 address with a bad reputation. • Outgoing packets go to an IPv4 address with a bad reputation. The Zyxel Device will not generate a log if you use the no command.

Table 53 IP Reputation Commands (continued)

COMMAND	DESCRIPTION
vrf main ip-reputation priority {high| medium| low}	Sets the threshold threat level to which the Zyxel Device will take action (**high**, **medium**, and **low**). The threat level is determined by the IP reputation engine, which grades IPv4 addresses as follows: • **high**: An IPv4 address that scores 0 to 20 points. • **medium**: An IPv4 address that scores 0-60 points. • **low**: An IPv4 address that scores 0-80 points.
vrf main ip-reputation outgoing-category botnets	Sets the category of packets coming from the Internet or local networks that the Zyxel Device applies IP reputation filtering to.
vrf main ip-reputation incoming-category {spam-sources| exploits| web-attacks| botnets| scanners| denial-of-service| negative-reputation| phishing| anonymous-proxies}	Select the categories of packets coming from the Internet that the Zyxel Device applies IP reputation filtering to.
show config vrf main ip-reputation enabled	Displays if IP reputation is enabled.
show config vrf main ip-reputation statistics enabled	Displays if the collection of IP reputation statistics is enabled.
show config vrf main ip-reputation statistics allow-list	Displays the IP reputation allow list settings. An allow list is a list of entries that will bypass the related feature filtering, and are permitted to pass through the Zyxel Device.
show state vrf main ip-reputation secureporter-allow-list	Displays allow lists in the Zyxel Device that were created in SecuReporter.
show config vrf main ip-reputation statistics block-list	Displays the IP reputation block list settings
show config vrf main ip-reputation action	Displays the action the Zyxel Device takes when a packet arrives from an IPv4 address with a bad reputation.
show config vrf main ip-reputation logging	Displays the Zyxel Device log settings when: • Incoming packets come from an IPv4 address with a bad reputation. • Outgoing packets go to an IPv4 address with a bad reputation.

18.2.1 IP Reputation Statistics

The following table describes the commands for collecting and displaying IP reputation statistics.

Table 54 IP Reputation Statistics Commands

COMMAND	DESCRIPTION
vrf main ip-reputation statistics enabled {true| false}	Enables the collection of IP reputation statistics.
show state vrf main ip-reputation summary	Displays the collected IP reputation statistics.

Table 54 IP Reputation Statistics (continued)Commands

COMMAND	DESCRIPTION
`show state vrf main ip-reputation top-entry {malicious-ip| victim-host| category}`	Displays the top five IP reputation statistics entries by malicious IP, victim host or threat category.
`show state vrf main ip-reputation event entry {timestamp| malicious-ip| victim-host| threat-category| threat-level| count}`	Displays the IP reputation statistics entries by time, malicious IP victim host, threat category, threat level, or numbers of times threats are detected.
`show system protection signature version`	Displays the system protection signature version, such as "version 2.1.10.20230606.0".
`show system protection signature update status`	Displays when system protection was last updated, for example, "last update time: 2024-02-19 08:24:01".

18.3 DNS Threat Filter Commands

The following table describes general DNS Threat Filter commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 55 DNS Threat Filter Commands

COMMAND	DESCRIPTION
`vrf main dns-threat-filter enabled {true| false}`	Enables DNS threat filter on the Zyxel Device.
`vrf main dns-threat-filter allow-list fqdn-list <FQDN> enabled {true| false} [description <description>]`	Adds a specified Fully Qualified Domain Name (FQDN) to the DNS threat filter allow list. A description is optional.
`vrf main dns-threat-filter allow-list enabled {true| false}`	Enables the DNS threat filter allow list.
`vrf main dns-threat-filter allow-list logging {no| log}`	Sets whether the Zyxel Device generates a log when a packet contains an FQDN you configured in the allow list. The Zyxel Device will not generate a log if you use the no command.
`vrf main dns-threat-filter block-list fqdn-list <FQDN> enabled {true| false} [description <description>]`	Adds a specified Fully Qualified Domain Name (FQDN) to the DNS threat filter block list. A description is optional.
`vrf main dns-threat-filter block-list enabled {true| false}`	Enables the DNS threat filter block list.
`vrf main dns-threat-filter block-list logging {no| log| log-alert}`	Sets whether the Zyxel Device generates a log or a log and an alert when a packet contains an FQDN you configured in the block list. The Zyxel Device will not generate a log if you use the no command.

Table 55 DNS Threat Filter Commands (continued)

COMMAND	DESCRIPTION
vrf main dns-threat-filter default_profile action {redirect| pass}	Sets what the Zyxel Device does when it detects a malicious DNS query packet. pass: Have the Zyxel Device allow the DNS query packet and not reply a DNS reply packet with a fake IP for it. redirect: Have the Zyxel Device reply with a DNS reply packet containing a default or custom-defined IP address. The default redirect IP is the IP address of the DNS Threat Filter server (dnsft.cloud.zyxel.com).
vrf main dns-threat-filter default_profile logging {no| log| log-alert}	Sets whether the Zyxel Device generates a log or a log and an alert when it detects a malicious DNS query packet. The Zyxel Device will not generate a log if you use the no command.
vrf main dns-threat-filter default_profile security-threat-category {anonymizers| malicious-sites| spyware-adware-keyloggers| phishing| spam-urls| browser-exploits| malicious-downloads}	The Zyxel Device considers DNS queries that match the specified category to be malicious.
vrf main dns-threat-filter redirect {default| custom-defined}	Sets whether the Zyxel Device uses the default redirect settings or the custom defined redirect settings when there is a DNS query packet containing an FQDN with a bad reputation.
vrf main dns-threat-filter custom-redirect-ip *<IPv4 address>*	Sets the redirect IP address for malicious DNS queries to the specified IPv4 address.
vrf main dns-threat-filter malform-detected-action {drop| pass}	drop: Sets the Zyxel Device to drop a DNS query packet if the DNS query is invalid, or if the Zyxel Device cannot read the packet. A DNS query is invalid under any of the following conditions: • The number of entries in the DNS header question count field is 0 • An error occurs while parsing the domain name in the question field • The length of the domain name exceeds 255 characters pass: Sets the Zyxel Device to allow malformed DNS packets to pass through.
vrf main dns-threat-filter malform-detected-logging {no| log}	Have the Zyxel Device log a DNS query if the DNS query packet is not a standard DNS query, or if the device cannot read the packet. The Zyxel Device will not generate a log if you use the no command.
vrf main dns-threat-filter fake-response-ttl <300...86400>	Sets the time period in seconds for redirecting clients to a default or custom-defined IP address when the clients try to access a blocked FQDN. The default value is 3600. If you remove an FQDN from the block list before the response time-to-live (TTL) time is up, the clients will still be redirected to a default or custom-defined IP address when they try to access the FQDN.
show config vrf main dns-threat-filer statistics enabled	Displays if the collection of DNS threat filter statistics is enabled.
show config vrf main dns-threat-filter allow-list	Displays the DNS threat filter allow list settings. An allow list is a list of entries that will bypass the related feature filtering, and are permitted to pass through the Zyxel Device.

Table 55 DNS Threat Filter Commands (continued)

COMMAND	DESCRIPTION
show state vrf main dns-threat-filter secureporter-allow-list	Displays allow lists in the Zyxel Device that were created in SecuReporter.
show config vrf main dns-threat-filter block-list	Displays the DNS threat filter block list settings.
show config vrf main dns-threat-filter default_profile	Displays the DSN threat filter default profile settings.
show config vrf main dns-threat-filter enabled	Displays if the DNS threat filter is enabled.
show config vrf main dns-threat-filter redirect	Displays the DNS threat filter redirect settings when there is a DNS query packet containing an FQDN with a bad reputation.
show config vrf main dns-threat-filter malform-detected-action.	Displays the action set when the DNS query is invalid.
show config vrf main dns-threat-filter malform-detected-logging	Displays if the Zyxel Device logs a DNS query when the DNS query is invalid.
show config vrf main dns-threat-filter fake-response-ttl	Displays the time period in second you set for redirecting clients to a default or custom-defined IP address when the clients try to access a blocked FQDN.

18.3.1 Redirecting DNS Query Packets Command Examples

You want to:

- Have the Zyxel Device rely with a DNS replay packet containing a custome-defined IP address when there is a DNS query packet containing an FQDN with a bad reputation.
- Have the Zyxel Device generate logs when there is a DNS query packet containing an FQDN with a bad reputation.

The DNS threat filter general settings use the parameters in the table below. General settings are for all traffic in the Zyxel Device network.

Table 56 DNS Threat General Settings Example

LOG	ACTION	CUSTOM-DEFINED REDIRECT IP ADDRESS
Log	redirect	10.10.10.10

1 Configure the DNS threat filter general settings.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main dns-threat-filter default_profile action
redirect
usgflex200hp running config# vrf main dns-threat-filter default_profile logging
log
usgflex200hp running config# vrf main dns-threat-filter custom-redirect-ip
10.10.10.10
usgflex200hp running config# commit
Configuration committed.
```

18.3.2 DNS Threat Filter Statistics

The following table describes the commands for collecting and displaying DNS Threat Filter statistics.

Table 57 DNS Threat Filter Statistics Commands

COMMAND	DESCRIPTION
`vrf main dns-threat-filter statistics enabled {true| false}`	Enables the collection of DNS threat filter statistics.
`show state vrf main dns-threat-filter statistics summary`	Displays the collected DNS Threat Filter domain blocking statistics.
`show state vrf main url-threat-filter statistics event entry {timestamp| threat-category| source-ip| dns-name}`	Queries the DNS threat filter statistics entries by time, FQDN, threat category, or source IP.
`show state vrf main dns-threat-filter statistics top-entry {category| dns-name| source-ip}`	Queries the top five DNS threat filter statistics entries by threat category, FQDN or source IP.

18.4 URL Threat Filter Commands

The following table describes general URL Threat Filter commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 58 URL Threat Filter Commands

COMMAND	DESCRIPTION
`vrf main url-threat-filter enabled {true| false}`	Enables URL threat filter on the Zyxel Device.
`vrf main url-threat-filter block redirect-url <url>`	Sets the URL of the web page to which you want to send users when their web access is blocked by the URL Threat Filter. The web page you specify here opens in a new frame below the denied access message. Use "http://" or "https://" followed by up to 262 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/blocked access.

Table 58 URL Threat Filter Commands (continued)

COMMAND	DESCRIPTION
vrf main url-threat-filter block message <*message*>	Sets a message to be displayed when the URL Threat Filter blocks access to a web page. Use up to 127 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator".
vrf main url-threat-filter default_profile action {block| pass}	Sets what action the Zyxel Device takes when a packet contains a malicious URL. block: The Zyxel Device blocks access to the web pages that match the categories you selected. pass: The Zyxel Device allows access to the web pages that match the categories you selected.
vrf main url-threat-filter default_profile logging {no| log| log-alert}	Sets whether the Zyxel Device generates a log or a log and an alert when a packet contains a malicious URL. The Zyxel Device will not generate a log if you use the no command.
vrf main url-threat-filter default_profile security-threat-category {anonymizers| malicious-sites| spyware-adware-keyloggers| phishing| spam-urls| browser-exploits| malicious-downloads}	The Zyxel Device blocks the specified web page categories.
vrf main url-threat-filter allow-list enabled {true| false}	Enables URL threat filter allow list.
vrf main url-threat-filter allow-list logging {no| log}	Sets whether the Zyxel Device generates a log when a packet contains a URL you configured in the allow list. The Zyxel Device will not generate a log if you use the no command.
vrf main url-threat-filter allow-list site-list <*URL*> [description <*description*>]	Adds a web site to the allow list using the following formats: • IPv4 address <W.X.Y.Z> • IPv4 subnet in CIDR format, i.e. 192.168.1.0/32<W.X.Y.Z>/<1...32> • Range of IPv4 addresses. <W.X.Y.Z>-<W.X.Y.Z> • Wildcard domain name, in the format *String1.String2*. For example: zyxel*.co*. String 1 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), . (period), * (wildcard character). String 2 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), * (wildcard character). • Top level domain. for example: zyxel.com. A description is optional.
vrf main url-threat-filter block-list enabled {true| false}	Enables URL threat filter block list.
vrf main url-threat-filter block-list logging {no| log| log-alert}	Sets whether the Zyxel Device generates a log or a log and an alert when a packet contains a URL you configured in the block list. The Zyxel Device will not generate a log if you use the no command.

Table 58 URL Threat Filter Commands (continued)

COMMAND	DESCRIPTION
vrf main url-threat-filter block-list site-list *<URL>* [description *<description>*]	Adds a web site to the block list using the following formats: • IPv4 address <W.X.Y.Z> • IPv4 subnet in CIDR format, i.e. 192.168.1.0/32<W.X.Y.Z>/<1...32> • Range of IPv4 addresses. <W.X.Y.Z>-<W.X.Y.Z> • Wildcard domain name, in the format *String1.String2*. For example: zyxel*.co*. String 1 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), . (period), * (wildcard character). String 2 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), * (wildcard character). • Top level domain. for example: zyxel.com. A description is optional.
vrf main url-threat-filter default-port enabled {true|false}	Enables this to have the Zyxel Device only scan traffic going through the specified ports. The default specified ports are 80, 443, 3128 and 8080. You can remove or add a port to this list by using the extra-port or the exception-port commands. Disables this to have the Zyxel Device scan traffic going through all ports.
vrf main url-threat-filter default-port {extra-port|exception-port} *port number*	Uses the extra-port command to add a port to the default specified port list. Uses the exception-port command to remove a port from the default specified port list.
show config vrf main url-threat-filter statistics enabled	Displays if the collection of URL threat filter statistics is enabled.
show config vrf main url-threat-filter block message	Displays the message to be displayed when the URL Threat Filter blocks access to a web page.
show config vrf main url-threat-filter default_profile	Displays the URL threat filter default profile settings.
show config vrf main url-threat-filter allow-list	Displays the URL threat filter allow list settings. An allow list is a list of entries that will bypass the related feature filtering, and are permitted to pass through the Zyxel Device.
show state vrf main url-threat-filter secureporter-allow-list	Displays allow lists in the Zyxel Device that were created in SecuReporter.
show config vrf main url-threat-filter block-list	Displays the URL threat filter block list settings.
show config vrf main url-threat-filter default-port enabled	Displays if the default port is enabled.
show config vrf main url-threat filter enabled	Displays if URL threat filter is enabled.

18.4.1 URL Threat Filter Command Examples

Use these commands to block users in your network from accessing URLs that are categorized as browser exploits, malicious downloads, malicious sites, phishing or spam URLs. Use these commands if you also want to create a trusted list of URLs to make sure the Zyxel Device will allow incoming packets from these URLs and outgoing packets to these URLs even if they are categorized as URL threats.

The example uses the parameters given below.

Table 59 URL Threat Filter Example

ACTION	LOG	THREAT CATEGORIES	TRUST LIST
block	log-alert	• Browser Exploits • Malicious Downloads • Malicious Sites • Phishing • Spam URLs	• www.google.com • www.yahoo.com

1 Configure the URL threat filer settings as the parameters given above.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main url-threat-filter default_profile action
block
usgflex200hp running config# vrf main url-threat-filter default_profile logging
log-alert
usgflex200hp running config# vrf main url-threat-filter default_profile security-
threat-category browser-exploits
usgflex200hp running config# vrf main url-threat-filter default_profile security-
threat-category malicious-downloads
usgflex200hp running config# vrf main url-threat-filter default_profile security-
threat-category malicious-sites
usgflex200hp running config# vrf main url-threat-filter default_profile security-
threat-category phishing
usgflex200hp running config# vrf main url-threat-filter default_profile security-
threat-category spam-urls
```

2 Enable URL threat filter allow list.

```
usgflex200hp running config# vrf main url-threat-filter allow-list enabled true
```

3 Configure the URL threat filter allow list as the parameters given above.

```
usgflex200hp running config# vrf main url-threat-filter allow-list site-list
www.google.com
usgflex200hp running config# vrf main url-threat-filter allow-list site-list
www.yahoo.com
```

4 Save the current configuration to the Zyxel Device.

```
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# exit
```

18.4.2 URL Threat Filter Statistics

The following table describes the commands for collecting and displaying URL Threat Filter statistics.

Table 60 URL Threat Filter Statistics Commands

COMMAND	DESCRIPTION
vrf main url-threat-filter statistics enabled {true| false}	Enables the collection of URL threat filter statistics.
show state vrf main url-threat-filter statistics summary	Displays the collected URL Threat Filter IP blocking statistics.
show state vrf main url-threat-filter statistics event entry {timestamp| url| threat-category| source-ip| destination-ip}	Displays the URL threat filter statistics entries by time, URL, threat category, source IP or destination IP.
show state vrf main url-threat-filter statistics top-entry {category| url| source-ip}	Displays the top five URL threat filter statistics entries by threat category, URL or source IP.

18.4.3 URL Threat Filter Statistics Example

This example shows how to display URL Threat Filter statistics.

```
usgflex200hp> show state vrf main url-threat-filter statistics summary summary
    scanned-count 0
    hit-count 0
```

18.4.3.1 Security Threat Category Definitions

The following table contains a list of URL Threat Filter categories.

Table 61 Current Category Descriptions

CATEGORY	DESCRIPTION
Anonymizers	Sites and proxies that act as an intermediary for surfing to other Web sites in an anonymous fashion, whether to circumvent web filtering or for other reasons.
Browser Exploits	Sites that contain browser exploits. A browser exploit is any content that forces a web browser to perform operations that you do not explicitly intend.
Malicious Downloads	Sites that host files containing malicious content, such as viruses, spyware, rootkits, and ransomware.
Malicious Sites	Sites that install unwanted software on a user's computer with the intent to enable third-party monitoring or make system changes without the user's consent.
Phishing	Sites that are used for deceptive or fraudulent purposes (e.g. phishing), such as stealing financial or other user account information. These sites are most often designed to appear as legitimate sites in order to mislead users into entering their credentials.

Table 61 Current Category Descriptions (continued)

Spam URLs	Sites that have been promoted through spam techniques.
Spyware Adware Keyloggers	Sites that contain spyware, adware, or keyloggers. Spyware is a program installed on your computer, usually without your explicit knowledge, that captures and transmits personal information or Internet browsing habits and details to companies. Companies use this information to analyze browsing habits, to gather marketing data, and to sell your information to others. Key logger programs try to capture and steal your passwords and watch and record everything you do on your computer. Adware programs typically display blinking advertisements or pop-up windows when you perform a certain action. Adware programs are often installed in exchange for another service, such as the right to use a program without paying for it.

18.5 External Block Lists

Use these commands to use block IP, FQDN or URL list entries stored in a file on a web server that supports HTTP or HTTPS and is reachable from the Zyxel Device. The Zyxel Device will bypass checking by this feature (if enabled) and block incoming and outgoing packets from the block list entries in this file. In this way, different Zyxel Devices can use the same block list.

The external block list file must be in text format (*.txt) with each entry separated by a new line.

Entries stored in a file on a web server allow the Zyxel Device to use longer lists than the Zyxel Device itself can contain and also allows an admin to use the same block lists across different Zyxel Devices.

List types are:

- IP Reputation
- URL / DNS Threat

18.5.1 IP Reputation External Block List

The following table describes the commands for enabling and configuring an external list of IP addresses to be blocked. The Zyxel Device blocks incoming and outgoing packets from the addresses in this file.

- The external block list file must be in text format (*.txt) with each entry separated by a new line.
- The external block list file must be stored on a web server that supports HTTP or HTTPS, and that is reachable from the Zyxel Device.
- Each entry consists of a single IPv4 address, a IPv4 subnet in CIDR (Classless Inter-Domain Routing) format, or an IPv4 IP address range. These are examples:
  - 104.244.79.43
  - 188.68.0.255/31
  - 1.1.1.1-1.1.1.3
- The external block list file can contain a maximum of 50,000 entries.

- If the external block list file contains any invalid entries, the Zyxel Device will skip the invalid entries but still block the valid entries.

Table 62 Commands for IP Reputation Statistics

COMMAND	DESCRIPTION
vrf main external-block-list ip-reputation enabled {true | false}	Enables or disables the IP Reputation external block list. When enabled, the Zyxel Device blocks incoming packets that come from the listed addresses in the block list file.
vrf main external-block-list ip-reputation profile <*profile-name*> description <*description*> source <*source*>	Creates an external block list profile. You must give the profile a name, a description consisting of 1–60 characters, and may include letters, numbers, and the following special characters: ()+/:=?!*#@$_%- The source must contain the exact file name, path and IP address of the server containing the external block list file.
show state vrf main external-block-list ip-reputation all	Shows all external block list profile details, such as name, count, last-update-time.
del / vrf main external-block-list ip-reputation profile <*profile name*>	Deletes the specified external block list profile.
cmd external-block-list-update ip-reputation	Sets the Zyxel Device to check for updates to the external block list immediately
show state vrf main external-block-list-update-check ip-reputation	Shows if the update check has completed. Check the log page for the update results.
vrf main external-block-list ip-reputation auto-update enabled {true | false}	Sets the Zyxel Device to automatically check for updates to the external block list.
vrf main external-block-list ip-reputation auto-update schedule-type {every-n-hours | daily | weekly}	Sets the hourly, daily or weekly frequency for Zyxel Device to check for updates to the external block list every n hours at the time and day specified. You should select a time when your network is not busy for minimal interruption.
vrf main external-block-list ip-reputation auto-update schedule every-n-hours <1..23>	Sets the Zyxel Device to check for updates to the external block list every n hours at the time and day specified. You should select a time when your network is not busy for minimal interruption.
vrf main external-block-list ip-reputation auto-update schedule daily meridiem {am | pm} oclock <*1..12*>	Sets the Zyxel Device to check for updates to the external block list once per day, at the specified hour. For example, the time format is the 24 hour clock, so '23' means 11 PM.
vrf main external-block-list ip-reputation auto-update schedule weekly day {sun | mon | tue | wed | thu | fri | sat} meridiem {am | pm} oclock <*1..12*>	Sets the Zyxel Device to check for updates to the external block list once per week, on the specified day at the specified hour.

18.5.2 URL /DNS Threat Filter External block List

The following table describes the commands for enabling and configuring an external database of URLs

to be blocked. The Zyxel Device blocks incoming and outgoing packets from the addresses in this file.

- The external block list file must be in text format (*.txt) with each entry separated by a new line.
- The external block list file must be stored on a web server that supports HTTP or HTTPS, and that is reachable from the Zyxel Device.
- Each entry consists of a URL or domain name. These are examples:
  - https://www.zyxel.com/products_services/smb.shtml?t=s
  - www.zyxel.com
- The external block list file can contain a maximum of 50,000 entries.
- If the external block list file contains any invalid entries, the Zyxel Device will not use the file.

Table 63 Commands for URL / DNS Threat Filter External Block List

COMMAND	DESCRIPTION
`vrf main external-block-list dns-url-threat-filter enabled {true | false}`	Enables or disables the URL / DNS Threat external block list. When enabled, the Zyxel Device blocks incoming packets that come from the listed addresses in the block list file.
`vrf main external-block-list dns-url-threat-filter profile <profile-name> description <description> source <source>`	Creates an external block list profile. You must give the profile a name, a description consisting of 1–60 characters, and may include letters, numbers, and the following special characters: ()+/:=?!*#@$_%- The source must contain the exact file name, path and IP address of the server containing the external block list file.
`show state vrf main external-block-list dns-url-threat-filter all`	Shows all external block list profile details, such as name, count, last-update-time.
`del / vrf main external-block-list dns-url-threat-filter profile <profile name>`	Deletes the specified external block list profile.
`cmd external-block-list-update dns-url-threat-filter`	Sets the Zyxel Device to check for updates to the external block list immediately
`show state vrf main external-block-list-update-check dns-url`	Shows if the update check has completed. Check the log page for the update results.
`vrf main external-block-list dns-url-threat-filter auto-update enabled {true | false}`	Sets the Zyxel Device to automatically check for updates to the external block list.
`vrf main external-block-list dns-url-threat-filter auto-update schedule-type {every-n-hours | daily | weekly}`	Sets the hourly, daily or weekly frequency for Zyxel Device to check for updates to the external block list every n hours at the time and day specified. You should select a time when your network is not busy for minimal interruption.

Table 63 Commands for URL / DNS Threat Filter External Block List (continued)

COMMAND	DESCRIPTION
`vrf main external-block-list dns-url-threat-filter auto-update schedule every-n-hours <1..23>`	Sets the Zyxel Device to check for updates to the external block list every n hours at the time and day specified. You should select a time when your network is not busy for minimal interruption.
`vrf main external-block-list dns-url-threat-filter auto-update schedule daily meridiem {am | pm} oclock <1..12>`	Sets the Zyxel Device to check for updates to the external block list once per day, at the specified hour. For example, the time format is the 24 hour clock, so '23' means 11 PM.

CHAPTER 19
IPS Commands

19.1 Overview

IPS (Intrusion Prevention System) protects against network-based intrusions, by detecting malicious or suspicious packets and responding instantaneously.
The IPS commands mostly mirror web configurator features. It is recommended you use the web configurator for IPS features such as searching for web signatures or editing an IPS profile. Some web configurator terms may differ from the command-line equivalent.

Packet Inspection Signatures

A signature is a pattern of malicious or suspicious packet activity. You can specify an action to be taken if the system matches a stream of data to a malicious signature. You can change the action in the profile screens. Packet inspection examine OSI (Open System Interconnection) layer-4 to layer-7 packet contents for malicious data. Generally, packet inspection signatures are created for known attacks while anomaly detection looks for abnormal behavior.

Rate Based Signatures

While IPS signatures have the Zyxel Device respond instantaneously, **Rate Based Signatures** are IPS signatures that allow the Zyxel Device to just respond after a number of occurrences (**Count**) within a certain time period (**Period**) you set.

Figure 39 IPS Signatures Example

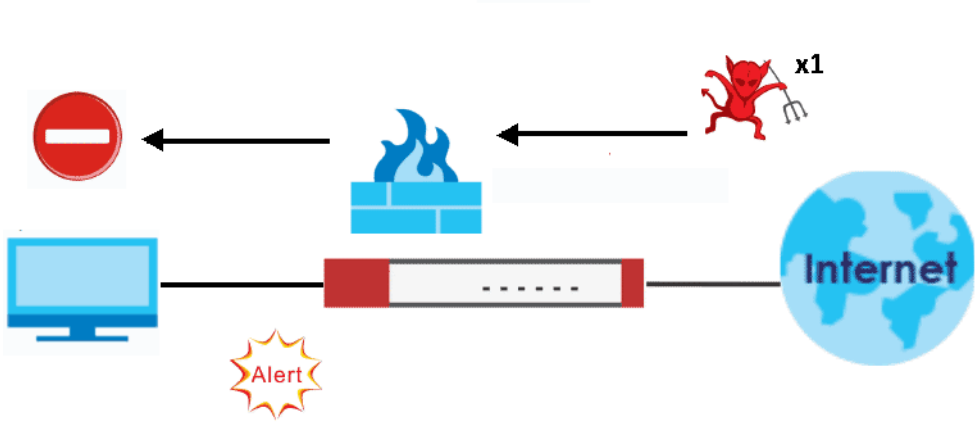
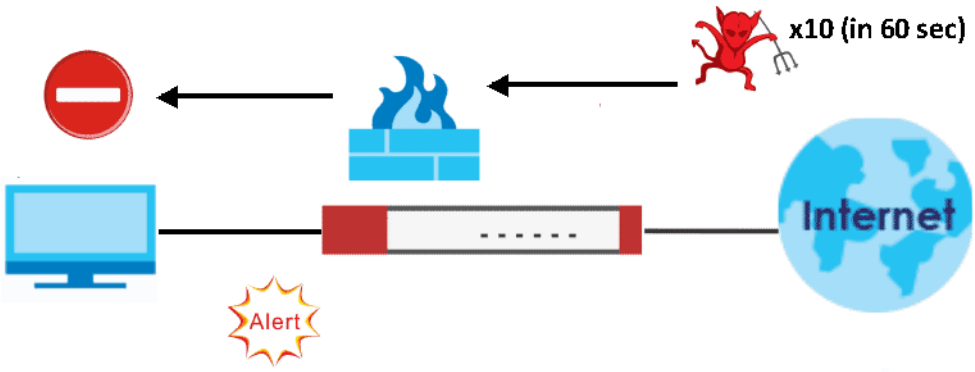


Figure 40 Rate Based Signatures Example



19.2 General IPS Commands

Note: You must register for the IPS signature service (at least the trial) before you can use it.

This table shows the general IPS commands. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 64 IPS General Commands

COMMAND	DESCRIPTION
`vrf main ips enabled {true| false}`	Enable IPS on the Zyxel Device. The `false` command disables IPS.
`vrf main ips all-traffic-scan-mode {prevention-mode| detection-mode}`	Sets what the Zyxel Device does when a stream of data matches a malicious signature. • `detection-mode`: The Zyxel Device only creates a log message. • `prevention-mode`: The Zyxel Device performs a user-specified action.
`vrf main ips system-protect enabled {true| false}`	Enables IDP system-protect to scan the packets that are destined for or sent out by the Zyxel Device for malicious or suspicious activities.
`vrf main ips system-protect bypass {tcp-port| udp-port} <1...65536>`	Sets a specified TCP or UDP port to bypass IPS system protection.
`show config vrf main ips {statistics| allow-list| default_profile| default_detect_only| enabled| all-traffic-scan-mode}`	Displays: • if statistics collection and IPS are enabled. • allow list, prevention mode profile and detection mode profile settings. • traffic scan mode.
`show ips-rate-based-signature {default_profile| default_detect_only}`	Displays rate based signatures settings.

19.2.0.1 General IPS Commands Example

This example shows how to activate signature-based IPS and set it to prevention mode on the Zyxel Device.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main ips enabled true
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config vrf main ips enabled
enabled true
usgflex200hp running config# vrf main ips all-traffic-scan-mode prevention-mode
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config vrf main ips all-traffic-scan-mode
all-traffic-scan-mode prevention-mode
```

19.3 IPS Profile Commands

Use the commands listed below to configure the IPS profiles.

19.3.1 Prevention Mode Profile

Use these commands to configure the IPS profile when the Zyxel Device is in **Prevention Mode**.

Table 65 Prevention Mode Profile Commands

COMMAND	DESCRIPTION
`vrf main ips default_profile`	Enters the sub-command mode to configure the IPS prevention mode profile.
`signature <0...4294967295> enabled {true| false} logging {no| log| log-alert} action {none| drop| reject}`	Sets the action and log for the specified signature.
`signature <0...4294967295> counts <1...300> seconds <1...300> block-period <0...86400>`	counts: Sets the number of security events that need to occur within the defined seconds to trigger an action. seconds: Sets the length of time in seconds the event should occur from a client the counts number of times to trigger an action. For example, counts is set to 5, and seconds is set to 60. If the Zyxel Device detects 5 or more occurrences of malicious traffic in less than 60 seconds, then action is triggered. block-period: Sets the time period the attacker's IP will be blocked.

19.3.2 Detection Mode Profile

Use these commands to configure the IPS profile when the Zyxel Device is in **Detection Mode**.

Table 66 Detection Mode Profile Commands

COMMAND	DESCRIPTION
`vrf main ips default_detect_only`	Enters the sub-command mode to configure the IPS detection mode profile.
`signature <signature-id> enabled {true| false} logging {no| log| log-alert}`	Sets the log for the specified signature.

19.3.2.1 Profile Commands Example

The example below shows you how to:

- configure the prevention mode profile.
- view profile setting.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main ips default_profile
usgflex200hp running default_profile# signature 112012 enabled true logging log
action drop
usgflex200hp running default_profile# signature 112011 enabled true logging log
action reject
usgflex200hp running default_profile# signature 12010 enabled true logging no
action none
usgflex200hp running default_profile# commit
Configuration committed.
usgflex200hp running default_profile# exit
usgflex200hp> show config vrf main ips default_profile signature
signature 112012
    action drop
    enabled true
    logging log
    ..
signature 112011
    action reject
    enabled true
    logging log
    ..
signature 112010
    action drop
    enabled true
    logging log-alert
    ..
signature 112009
    action none
    enabled true
    logging log
    ..
signature 12010
    action none
    enabled true
    logging no
```

19.3.3 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 67 Signature Search Command

COMMAND	DESCRIPTION
`show ips-search-signature profile <profile-name> sid <sid> severity <severity-mask> platform <platform-mask> classtype <classtype-mask> service <service-mask> action <action-mask> enabled {true| false} logging {no| log| log-alert} name <signature-name>`	Searches for signature(s) in a profile by the parameters specified. For example, [show ips-search-signature profile default_profile name worm sid 0 severity 0 platform 0 classtype 0 service 0 action 0] searches for all signatures in the default_profile containing the text "worm" within the signature name.

19.3.3.1 Search Parameter Tables

The following table displays the command line severity, platform and class 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, Linux and Android then type "2060" as the platform parameter.

Table 68 Severity, Platform and Class Type Command Values

SEVERITY	PLATFORM	CLASS TYPE
0 = Any	0 = Any	0 = Any
1 = Very Low	4 = Windows	1 = Misc
2 = Low	8 = Linux	2 = Web-Attacks
4 = Medium	16 = FreeBSD	4 = Buffer-Overflow
8 = High	32 = Solaris	8 = Backdoor/Trojan
16 = Severe	128 = Other-Unix	16 = Access-Control
	256 = Network-Device	32 = P2P
	512 = Mac-OS	64 = IM
	1024 = iOS	128 = Virus-Worm
	2048 = Android	256 = BotNet
	4096 = Windows-Mobile	512 = Dos-DDos
	8192 = Symbian	1024 = Scan
	32768 = Others	2048 = File-Transfer
		4096 = Mail
		8192 = Stream-Media
		16384 = Tunnel
		32768 = ACL

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 and FTP services, then type “640” as the service parameter.

Table 69 Service and Action Command Values

SERVICE	ACTION
0 = Any	0 = Any
1 = Misc	1 = None
2 = Exploit	2 = Drop
4 = Web	4 = Reject
8 = Web Client	
16 = Web ActiveX	
32 = Database	
64 = File Format	
128 = FTP	
256 = ICMP	
512 = DNS	
1024 = RDP	
2048 = DHCP	
4096 = SMTP	
8192 = SNMP	
16384 = POP3	
32768 = IMAP	
65536 = NETBIOS	
131072 = SCADA	
262144 = SIP	
DoS = 524288	

19.4 IPS Statistics

The following table describes the commands for collecting and displaying IPSP statistics. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

Table 70 Commands for IPS Statistics

COMMAND	DESCRIPTION
`vrf main ips statistics enabled {true| false}`	Enables the collection of IPS statistics. The `false` command disables the collection of IPS statistics.
`show state vrf main ips statistics summary {scanned-session-count| packet-drop-count| packet-reset-count}`	Displays the collected statistics.
`show state vrf main ips statistics event entry {timestamp| count| souce-ip| destination-ip| sid| name| type| severity}`	Queries IPS statistics entries by time, numbers of times traffic matches the signatures, destination IP address, source IP address, signature ID, signature name or signature severity level.
`show state vrf main ips statistics top-entry {signature-name| source-ip| destination-ip}`	Queries the top five IPS statistics entries by destination IP address, source IP address or signature name.

19.4.1 IPS Statistics Example

This example shows how to display IPS statistics.

```
usgflex200hp> show state vrf main ips statistics summary
summary
    scanned-session-count 0
    packet-drop-count 0
    packet-reset-count 0
```

19.5 IPS Allow List

The Zyxel Device will exclude the incoming packets of the signature(s) in the IPS allow list. These packets won't be intercepted and will be passed through uninspected.

You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 71 Commands for IPS Allow List

COMMAND	DESCRIPTION
`vrf main ips allow-list`	Enter IPS allow list sub-command mode.
`sid <0...4294967295>`	Adds the specified signature to the IPS allow list.
`logging {no| log}`	Sets whether or not to generate a log when the incoming packets match the signatures you set in the allow list.

19.5.1 IPS Allow List Example

This example shows how to configure allow list settings.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main ips allow-list
usgflex200hp running allow-list# sid 12013 logging no
usgflex200hp running allow-list# sid 12014 logging log
usgfleusgflex200hp running allow-list# commit
Configuration committed.
```

CHAPTER 20
Content Filtering

20.1 Content Filtering Overview

The Zyxel Device content filtering includes HTTP(S) traffic scan and DNS domain scan, see Section 20.1.1 on page 131 and Section 20.1.2 on page 132 for more information.

The Zyxel Device content filtering allows you to block access to specific categories of web site content, and/or block access to specific web sites. You can create different content filtering policies for different addresses, users or groups and content filtering profiles. See Section 20.3.3 on page 140 for an example on how to use the Zyxel Device content filtering.

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.

Content Filtering Profiles

A content filtering profile conveniently stores your custom settings for the following features.

- Category-Based Blocking

  The Zyxel Device can block access to particular categories of web site content, such as pornography or racial intolerance.
- Customize Web Site Access

  You can specify URLs to which the Zyxel Device blocks access. You can alternatively block access to all URLs except ones that you specify. You can also have the Zyxel Device block access to URLs that contain particular keywords.

20.1.1 HTTP(S) Traffic Scan

The HTTP(S) Traffic Scan allows the Zyxel Device to block access to specific websites, by inspecting the URL or Server Name Indication (SNI). SNI lets a client indicate which host name it is attempting to connect to at the start of the handshaking process. This allows a server to present one of many certificates to the same IP address and TCP port number, so that different HTTPS websites can be served by the same IP address without requiring those sites to use the same certificate.

HTTP(S) Traffic Scanning Process

1 The Zyxel Device content filtering detects an HTTP(S) connection, and inspects the website sent.

2 If the website contains prohibited material, the HTTP(S) request is redirected to a block page.

Note: If the user's web browser is using encryption, then you must enable SSL Inspection for HTTP(S) Traffic Scan to work.

HTTP(S) Traffic Scanning Configuration Guidelines

When the Zyxel Device receives an HTTP request, the content filter searches for a policy that matches the source address and time (schedule). The content filter checks the policies in order (based on the policy numbers). When a matching policy is found, the content filter allows or blocks the request depending on the settings of the filtering profile specified by the policy. Some requests may not match any policy. The Zyxel Device allows the request if the default policy is not set to block. The Zyxel Device blocks the request if the default policy is set to block.

HTTPS Domain Filter

HTTPS Domain Filter works with the content filtering category feature to identify HTTPS traffic and take appropriate action. SSL Inspection identifies HTTPS traffic for all Security Service traffic and has higher priority than HTTPS Domain Filter. HTTPS Domain Filter only identifies keywords in the domain name of an URL and matches it to a category. For example, if the keyword is 'picture' and the URL is http://www.google.com/picture/index.htm, then HTTPS Domain Filter cannot identify 'picture' because that keyword in not in the domain name 'www.google.com'. However, SSL Inspection can identify 'picture' in the URL http://www.google.com/picture/index.htm.

Keyword Blocking URL Checking

The Zyxel Device checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

Since the Zyxel Device checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the Zyxel Device would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path (news/pressroom.php) but it would not find "tw/news".

20.1.2 DNS Domain Scan

The DNS Domain Scan allows the Zyxel Device to block access to specific websites by inspecting DNS queries made by users on your network. If the website in the DNS query contains prohibited material, then the Zyxel Device replies to the DNS query with a IP address that points to the block page. Unlike the HTTP(S) Traffic Scan, the DNS Domain Scan works if the user is using TLS 1.3 with ESNI.

DNS Domain Scan Process

1 A user enters a URL into their web browser.

2 The user's computer sends a DNS query for the URL.

3 The DNS Domain Scan inspects the website in the DNS query packet.

4 If the website contains prohibited material, the DNS reply is redirected to a block page.

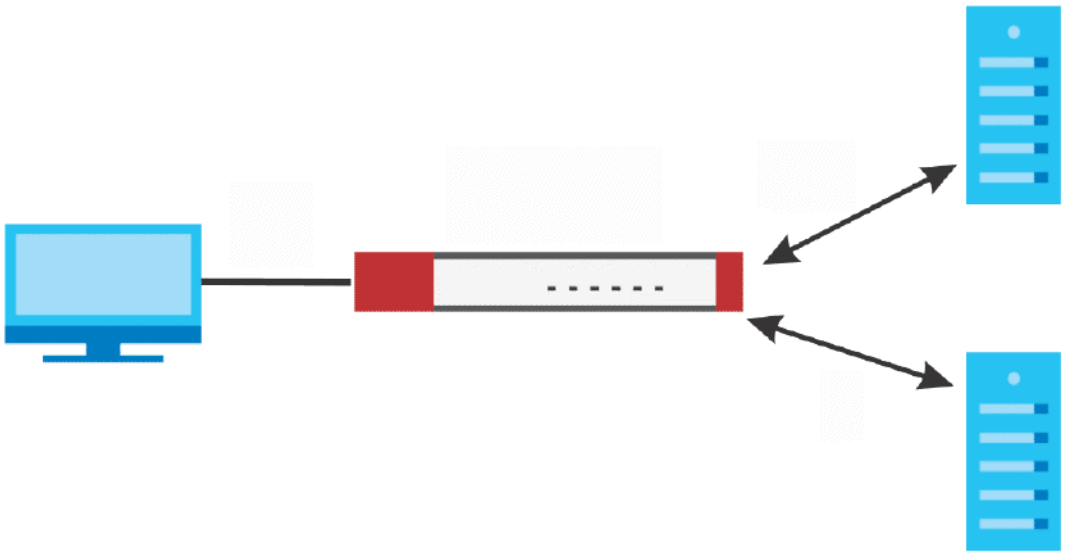
20.1.3 External Content Filtering Service

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

External Content Filtering Server Lookup Procedure

The content filtering lookup process is described below.

Figure 41 Content Filtering Lookup Procedure



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

2 The Zyxel Device 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 Zyxel Device's cache. The Zyxel Device blocks, blocks and logs or just logs the request based on your configuration.

3 If the Zyxel Device has no record of the web site, it queries the external content filtering database.

4 The external content filtering server sends the category information back to the Zyxel Device, 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 Zyxel Device's content filtering cache.

20.2 Content Filtering Command Input Values

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

Table 72 Content Filtering Command Input Values

LABEL	DESCRIPTION
profile-name	The filtering profile defines how to filter web URLs or content. You may use 1-30 alphanumeric characters, and also underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
category	The name of a web category. For a list of category definitions, see Section 20.4 on page 141. {adult-topics | alcohol | anonymizing-utilities | art-culture-heritage | auctions-classifieds | blogs-wiki | business | chat | computing-internet | consumer-protection | content-server | controversial-opinions | cult-occult | dating-personals | dating-social-networking | digital-postcards | discrimination | drugs | education-reference | entertainment | extreme | fashion-beauty | finance-banking | for-kids | forum-bulletin-boards | gambling | gambling-related | game-cartoon-violence | games | general-news | government-military | gruesome-content | health | historical-revisionism | history | humor-comics | illegal-uk | incidental-nudity | information-security | information-security-new | instant-messaging | interactive-web-applications | internet-radio-tv | internet-services | job-search | major-global-religions | marketing-merchandising | media-downloads | media-sharing | messaging | mobile-phone | moderated | motor-vehicles | non-profit-advocacy-ngo | nudity | online-shopping | p2p-file-sharing | parked-domain | personal-network-storage | personal-pages | pharmacy | politics-opinion | pornography | portal-sites | potential-criminal-activities | potential-hacking-computer-crime | potential-illegal-software | private-ip-addresses | profanity | professional-networking | provocative-attire | public-information | pups | real-estate | recreation-hobbies | religion-ideology | remote-access | reserved | residential-ip-addresses | resource-sharing | restaurants | school-cheating-information | search-engines | sexual-materials | shareware-freeware | social-networking | software-hardware | sports | stock-trading | streaming-media | technical-business-forums | technical-information | text-spoken-only | text-translators | tobacco | travel | usenet-news | violence | visual-search-engine | weapons | web-ads | web-mail | web-meetings | web-phone | unrated}
trust-hosts	The IP address or domain name of a trusted web site. Use a host name such as www.good-site.com. Do not use the complete URL of the site – that is, do not include “http://”. All subdomains are allowed. For example, entering “zyxel.com” also allows “www.zyxel.com”, “partner.zyxel.com”, “press.zyxel.com”, etc. Use up to 63 case-insensitive characters (0-9a-z-). You can enter a single IP address in dotted decimal notation like 192.168.2.5. You can enter a subnet by entering an IP address in dotted decimal notation followed by a slash and the bit number of the subnet mask of an IP address. The range is 0 to 32. To find the bit number, convert the subnet mask to binary and add all of the 1’s together. Take “255.255.255.0” for example. 255 converts to eight 1’s in binary. There are three 255’s, so add three eights together and you get the bit number (24). An example is 192.168.2.1/24 You can enter an IP address range by entering the start and end IP addresses separated by a hyphen, for example 192.168.2.5-192.168.2.23.

Table 72 Content Filtering Command Input Values (continued)

LABEL	DESCRIPTION
forbid-hosts	The IP address or domain name of a forbidden web site. Use a host name such as www.bad-site.com into this text field. Do not use the complete URL of the site – that is, do not include "http://". All subdomains are also blocked. For example, entering "bad-site.com" also blocks "www.bad-site.com", "partner.bad-site.com", "press.bad-site.com", etc. Use up to 63 case-insensitive alphanumeric characters (0-9a-zA-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".

20.3 Content Filtering Commands

The following table lists the commands that you can use for content filtering configuration, such as creating a denial of access message or specifying a redirect URL. Use the `edit running` command to

enter the configuration mode to be able to use these commands. See Table 72 on page 134 for details about the values you can input with these commands.

Table 73 Content Filtering General Commands

COMMAND	DESCRIPTION
`vrf main content-filter https-domain-filter enabled {true| false]`	Enable HTTPS domain filter which lets the Zyxel Device take action on HTTPS web pages using the category service. In an HTTPS connection, the Zyxel Device can extract the Server Name Indication (SNI) from a client request, check if it matches a category in the Content Filter and then take appropriate action. The keyword match is for the domain name only. The `false` command disables the HTTPS domain filter.
`vrf main content-filter https-domain-filter block-page-enabled {true| false}`	Enable HTTPS domain filter block page to have the Zyxel Device display a warning page instead of a black page when an HTTPS connection is redirected.
`vrf main content-filter default-port enabled {true| false}`	Has the Zyxel Device only scan traffic going through the specified ports. The default specified ports are 21, 25, 80, 110, 143, 443, 465, 990, 993, 995, 3128 and 8080. You can remove or add a port to this list by using the `extra-port` or the `exception-port` commands. Disables this to have the Zyxel Device scan traffic going through all ports.
`vrf main content-filter default-port {exception-port| extra-port} <0...65535>`	`extra-port`: Adds a port to the default specified port list. `exception-port`: Removes a port from the default specified port list.
`vrf main content-filter block redirect-url <redirect-url>`	Sets the URL of the web page to which to send users when their web access is blocked by the Content Filter.
`vrf main content-filter block message <message>`	Sets the message to display when the Content Filter blocks access to a web page.
`vrf main content-filter offline action {pass| block}`	Sets the action for attempted access to web pages if the external web filtering database is unavailable.
`vrf main content-filter offline logging {no| log}`	Sets whether to generate logs for attempted access to web pages if the external web filtering database is unavailable.
`vrf main content-filter dns-scan enabled {true| false}`	Lets the Zyxel Device inspect DNS queries made by users on your network.
`vrf main content-filter dns-scan custom-redirect-ip <IPv4 address>`	Sets the redirect IP address for prohibited DNS queries to the specified IPv4 address. The default redirect IP address is the IP address of the DNS domain scan server (dnsft.cloud.zyxel.com).
`vrf main content-filter dns-scan fake-response-ttl <300...86400>`	Sets the time period in seconds for redirecting clients to a default or custom-defined IP address when the clients try to access a blocked FQDN. The default value is 3600. If you remove an FQDN from the block list before the response time-to-live (TTL) time is up, the clients will still be redirected to a default or custom-defined IP address when they try to access the FQDN.
`vrf main content-filter dns-scan redirect {default| custom-defined}`	Sets whether the Zyxel Device uses the default redirect settings or the custom defined redirect settings when users on your network try to access blocked FQDNs.

Table 73 Content Filtering General Commands (continued)

COMMAND	DESCRIPTION
show config vrf main content-filter https-domain-filter {enabled| block-page-enabled}	Displays if the HTTPS domain filter and the HTTPS domain filter blocked page is enabled.
show config vrf main content-filter default-port {enabled| exception-port| extra-port}	Displays: • if the default port is enabled. • exception port and extra port settings.
show config vrf main content-filter statistics enabled	Displays if the content filter statistics collection is enabled.
show config vrf main content-filter blocked {redirect-url| message}	Displays the redirect URL and blocked message settings when the Content Filter blocks access to a web page.
show config vrf main content-filter offline {action| logging}	Displays the action and log settings when there are attempts to access web pages if the external web filtering database is unavailable.
show config vrf main content-filter dns-scan {enabled| redirect| custom-redirect-ip| fake-response-ttl}	Displays the DNS domain scan settings.
cmd content-filter-cache-flush	Clears the history of the websites the Zyxel Device content filter has scanned. Use this command when you think the content filter categories stored on the Zyxel Device is not up to date.
cmd content-filter-statistic-flush	Clears the collected statistics.

20.3.1 Content Filtering Profile Commands

The following table lists the commands that you can use to configure a content filtering profile. Use the edit running command to enter the configuration mode to be able to use these commands. See Table 72 on page 134 for details about the values you can input with these commands.

Table 74 Content Filtering Profile Commands Summary

COMMAND	DESCRIPTION
show config vrf main content-filter profile	Displays the content filtering profiles settings.
vrf main content-filter profile *<profile-name>*	Creates a content filtering profile and enters the sub-command mode.
sslv3 drop {true| false}	Blocks HTTPS web sites using SSL V3 or a previous version.
sslv3 logging {no| log| log-alert}	Sets whether the Zyxel Device generates a log or a log and an alert when the user on your network tries to access an HTTPS web site that is using SSL V3 or a previous version. The Zyxel Device will not generate a log if you use the no command.
match action {pass| block}	Sets the action for attempted access to web sites that match the profile's selected managed categories.

Table 74 Content Filtering Profile Commands Summary (continued)

COMMAND	DESCRIPTION
`match logging {no| log| log-alert}`	Sets whether the Zyxel Device generates a log or a log and an alert when the user on your network tries to access a web site that matches the profile's selected managed categories. The Zyxel Device will not generate a log if you use the no command.
`allow-list logging {no| log}`	Sets whether the Zyxel Device generates a log when the user on your network accesses a web site listed in the allow list you configured. The Zyxel Device will not generate a log if you use the no command.
`allow-list site-list <trust-hosts>`	Adds a trusted web site entry in the following formats: • IPv4 address <W.X.Y.Z> • IPv4 subnet in CIDR format, i.e. 192.168.1.0/32<W.X.Y.Z>/<1..32> • Range of IPv4 addresses. <W.X.Y.Z>-<W.X.Y.Z> • Wildcard domain name, in the format *String1.String2*. For example: zyxel*.co*. String 1 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), . (period), * (wildcard character). String 2 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), * (wildcard character). • Top level domain
`block-list logging {no| log| log-alert}`	Sets whether the Zyxel Device generates a log or a log and an alert when the user on your network tries to access a web site listed in the block list you configured. The Zyxel Device will not generate a log if you use the no command.
`block-list site-list <forbid-hosts>`	Adds a forbidden web site entry in the following formats: • IPv4 address <W.X.Y.Z> • IPv4 subnet in CIDR format, i.e. 192.168.1.0/32<W.X.Y.Z>/<1..32> • Range of IPv4 addresses. <W.X.Y.Z>-<W.X.Y.Z> • Wildcard domain name, in the format *String1.String2*. For example: zyxel*.co*. String 1 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), . (period), * (wildcard character). String 2 must consist of 1–63 characters, and may include letters, numbers, and the following special characters: - (hyphen), * (wildcard character). • Top level domain
`url-keyword logging {no| log| log-alert}`	Sets whether the Zyxel Device generates a log or a log and an alert when the user on your network tries to access a web site with an URL that contains certain keywords in the domain name or IP address. The Zyxel Device will not generate a log if you use the no command.

Table 74 Content Filtering Profile Commands Summary (continued)

COMMAND	DESCRIPTION
`url-keyword keyword-list <keyword>`	Adds a forbidden keyword or IP address to the profile's list. Please note the Zyxel Device checks the URL's domain name (or IP address) and file path separately when performing keyword blocking. When the Zyxel Device inspects the URL queries made by users on your network, the Zyxel Device will check both the URL domain name and file path for keywords that are blocked. When the Zyxel Device inspects the DNS queries made by users on your network, the Zyxel Device will only check the URL domain name for keywords that are bocked, but not the file path.
`description <description>`	Sets a description for the content filtering profile to help identify the purpose of the profile.
`allow-only-enabled {true| false}`	Has the Zyxel Device only allow access to the web sites listed in the allow list.
`log-allowed-traffic {true| false}`	Has the Zyxel Device generate logs for all allowed traffic.
`category <category>`	Adds a managed category to the profile list.

20.3.2 Content Filtering Statistics

The following table describes the commands for collecting and displaying content filtering statistics.

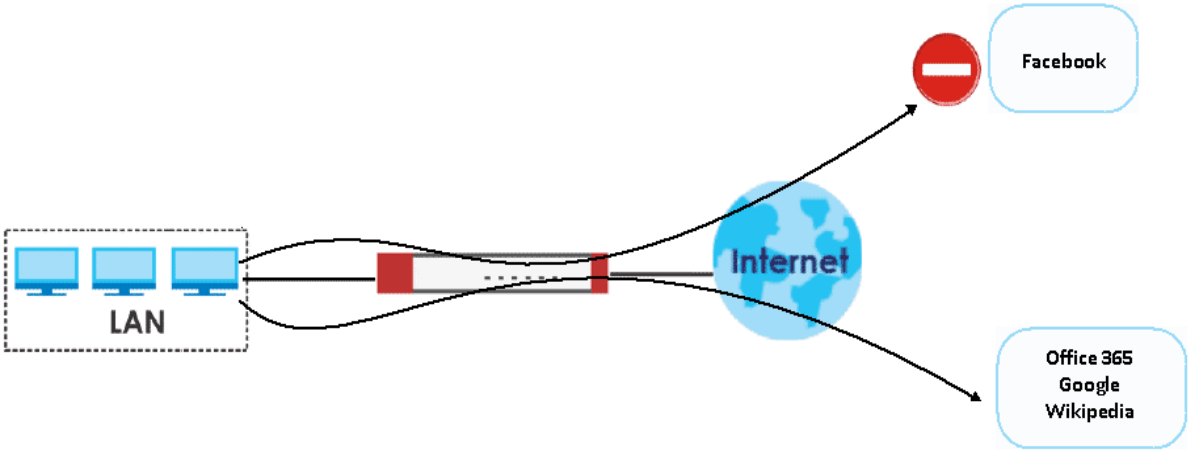
Table 75 Content Filtering Statistics Commands

COMMAND	DESCRIPTION
`vrf main content-filter statistics enabled {true| false}`	Enable the collection of content filtering statistics. The `false` command disables the collection of content filtering statistics.
`vrf main content-filter statistics summary`	Displays the collected Content Filter statistics.
`vrf main content-filter statistics blocked-event entry {timestamp| source-ip| destination-ip| url| category| profile-name| action}`	Displays the traffic Content Filter has blocked by time, destination IP address, source IP address, URL, category, profile name and action.
`vrf main content-filter statistics allowed-event entry {timestamp| source-ip| destination-ip| url| category| profile-name| action}`	Displays the traffic Content Filter has allowed to pass by time, destination IP address, source IP address, URL, category, profile name and action.
`vrf main content-filter statistics event entry {timestamp| source-ip| destination-ip| url| category| profile-name| action}`	Displays content filtering statistics entries by time, destination IP address, source IP address, URL, category, profile name and action.
`vrf main content-filter statistics top-entry {blocked-source-ip| blocked-category| blocked-url| allowed-source-ip| allowed-category| allowed-url}`	Displays the top five content filtering statistics entries by blocked source IP address, blocked category, blocked URL, allowed source IP address, allowed category and allowed URL.

20.3.3 Content Filtering Example

This is an example of using the Zyxel Device to block access to a specific network service. A company wants to prevent its employees from using Facebook during their time in the office, but still allows access to other web pages, such as Office 365, Google, Wikipedia... The company wants to make sure any traffic going from the LAN to the Internet cannot access Facebook whether the traffic goes through the Zyxel Device or not.

Figure 42 Content Filtering Example



Follow the steps below to block the Zyxel Device LAN users from accessing Facebook.

1 Create a content filtering profile named **facebook_block**.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main content-filter profile
facebook_block
```

2 You then enter sub-command mode for the **facebook_block** profile to configure the content filtering profile's list of forbidden keywords.

```
usgflex200hp running profile facebook_block#
```

3 Enter ***.facebook*.com** to block access to websites with URLs that contain **facebook**. Use asterisks (*) as a wildcard to match any string in trusted and forbidden websites. Exit sub-command mode.

```
usgflex200hp running profile facebook_block# url-keyword keyword-list
*.facebook*.com
usgflex200hp running profile facebook_block# commit
Configuration committed.
usgflex200hp running profile facebook_block# exit
```

4 To block traffic that goes through the Zyxel Device from the LAN to the Internet, you need to apply the content filtering profile **facebook_block** to the security policies **LAN1_Outgoing** and **LAN2_Outgoing**. Enter sub-command mode for configuring the security policy **LAN1_Outgoing**.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main secure-policy rule 1
usgflex200hp running rule 1#
```

5 Apply the content filter profile **facebook_block** to the security policies' content filtering profile. Set the log to **log by-profile** to generate a log for all traffic that matches criteria in the profile. Exit sub-command mode.

```
usgflex200hp running rule 1# content-filter-profile profile name
facebook_block enabled true log by-profile
usgflex200hp running rule 1# commit
Configuration committed.
```

6 Repeat step 7 and step 8 to apply the content filtering profile **facebook_block** to the security policy **LAN2_Outgoing**.

20.3.4 Content Filtering Statistics Example

This example shows how to display content filtering statistics.

```
usgflex200hp> show state vrf main content-filter statistics summary
summary
    total-inspected 0
    blocked 0
    passed 0
    allow-list-hit 0
    block-list-hit 0
    url-keyword-hit 0
    service-unavailable-passed 0
    service-unavailable-blocked 0
    sslv3-block-hit 0
```

20.4 Content Filtering Category Definitions

The following table listed the managed categories available.

Table 76 Managed Category Descriptions

CATEGORY	DESCRIPTION
Adult Topics	Web pages that contain content or themes that are generally considered unsuitable for children.
Alcohol	Web pages that mainly sell, promote, or advocate the use of alcohol, such as beer, wine, and liquor. This category also includes cocktail recipes and home-brewing instructions.

Table 76 Managed Category Descriptions (continued)

Anonymizing Utilities	Web pages that result in anonymous web browsing without the explicit intent to provide such a service. This category includes URL translators, web-page caching, and other utilities that might function as anonymizers, but without the express purpose of bypassing filtering software. This category does not include text translation.
Art Culture Heritage	Web pages that contain virtual art galleries, artist sites (including sculpture and photography), museums, ethnic customs, and country customs. This category does not include online photograph albums.
Auctions Classifieds	Web pages that provide online bidding and selling of items or services. This category includes web pages that focus on bidding and sales. This category does not include classified advertisements such as real estate postings, personal ads, or companies marketing their auctions.
Blogs Wiki	Web pages containing dynamic content, which often changes because users can post or edit content at any time. This category covers the risks with dynamic content that might range from harmless to offensive.
Business	Web pages that provide business-related information, such as corporate overviews or business planning and strategies. This category also includes information, services, or products that help other businesses plan, manage, and market their enterprises, and multi-level marketing. This category does not include personal pages and web-hosting web pages.
Chat	Web pages that provide web-based, real-time social messaging in public and private chat rooms. This category includes IRC. This category does not include instant messaging.
Computing Internet	Web pages containing reviews, information, buyer's guides of computers, computer parts and accessories, computer software and Internet companies, industry news and magazines, and pay-to-surf sites.
Consumer Protection	Websites that try to rob or cheat consumers. Some examples of their activities include selling counterfeit products, selling products that were originally provided for free, or improperly using the brand of another company. This category also includes sites where many consumers reported being cheated or not receiving services. This category does not include phishing, which tries to perpetrate fraud or theft by stealing account information.
Content Server	URLs for servers that host images, media files, or JavaScript for one or more sites and are intended to speed up content retrieval for existing web servers, such as Apache. This category includes domain-level and sub-domain-level URLs that function as content servers. This category does not include: • Web pages for businesses that provide the content servers • Web pages that allow users to browse photographs. See the Media Sharing category. • URLs for servers that serve only advertisements. See the Web Ads category.

Table 76 Managed Category Descriptions (continued)

Controversial Opinions	Web pages that contain opinions that are likely to offend political or social sensibilities and incite controversy. Much of this content is at the extremes of public opinion. This category does not include opinion or language clearly intended to promote hate or discrimination.
Cult Occult	Sites relating to non-traditional religious practices considered to be false, unorthodox, extremist, or coercive.
Dating Personals	Web pages that provide networking for online dating, matchmaking, escort services, or introductions to potential spouses. This category does not include sites that provide social networking that might include dating, but are not specific to dating.
Dating Social Networking	Web pages that focus on social interaction such as online dating, friendship, school reunions, pen-pals, escort services, or introductions to potential spouses. This category does not include wedding-related content, dating tips, or related marketing.
Digital Postcards	Web pages that allow people to send and receive digital postcards and greeting cards via the Internet.
Discrimination	Web pages, which provide information that explicitly encourages the oppression or discrimination of a specific group of individuals. This category does not include jokes and humor, unless the focus of the entire site is considered discriminatory.
Drugs	Websites that provide information on the purchase, manufacture, and use of illegal or recreational drugs. This category does not include sites with exclusive health or political themes.
Education Reference	Web pages devoted to academic-related content such as academic subjects (mathematics, history), school or university web pages, and education administration pages (school boards, teacher curriculum).
Entertainment	Web pages that provide information about cinema, theater, music, television, infotainment, entertainment industry gossip-news, and sites about celebrities such as actors and musicians. This category also includes sites where the content is devoted to providing entertainment on the web, such as horoscopes or fan clubs.
Extreme	Web pages that provide content considered gory, perverse, or horrific.
Fashion Beauty	Web pages that market clothing, cosmetics, jewelry, and other fashion-oriented products, accessories, or services. This category also includes product reviews, comparisons, and general consumer information, and services such as hair salons, tanning salons, tattoo studios, and body-piercing studios. This category does not include fashion-related content such as modeling or celebrity fashion unless the site focuses on marketing the product line.
Finance Banking	Web pages that provide financial information or access to online financial accounts. This category includes stock information (but not stock trading), home finance, and government-related financial information.
For Kids	Web pages that are family-safe, specifically for children of approximate ages ten and under. This category can also be used as an exception to allow web pages that do not pose a risk to children, or to access sites that have a primary educational or recreational focus for children, but are in other categories such as Games, Humor/Comics, Recreation/Hobbies, or Entertainment.

Table 76 Managed Category Descriptions (continued)

Forum Bulletin Boards	Web pages that provide access (http://) to Usenet newsgroups or hold discussions and post user-generated content, such as real-time message posting for an interest group. This category also includes archives of files uploaded to newsgroups. This category does not include message forums with a business or technical support focus.
Gambling	Web pages that allow users to wager or place bets online, or provide gambling software that allows online betting, such as casino games, betting pools, sports betting, and lotteries. This category does not include web pages related to gambling that do not allow betting online.
Gambling Related	Web pages that offer information about gambling, without providing the means to gamble. This category includes casino-related web pages that do not offer online gambling, gambling links, tips, sports picks, lottery results, and horse, car, or boat racing.
Game Cartoon Violence	Web pages that provide fantasy or fictitious representations of violence within the context of games, comics, cartoons, or graphic novels. This category includes images and textual descriptions of physical assaults or hand-to-hand combat, and grave injury and destruction caused by weapons or explosives.
Games	Web pages that offer online games and related information such as cheats, codes, demos, emulators, online contests or role-playing games, gaming clans, game manufacturer sites, fantasy or virtual sports leagues, and other gaming sites without chances of profit. This category includes gaming consoles.
General News	Web pages that provide online news media, such as international or regional news broadcasting and publication. This category includes portal sites that provide news content.
Government Military	Web pages that contain content maintained by governmental or military organizations, such as government branches or agencies, police departments, fire departments, civil defense, counter-terrorism organizations, or supranational organizations, such as the United Nations or the European Union. This category includes military and veterans' medical facilities.
Gruesome Content	Web pages with content that can be considered tasteless, gross, shocking, or gruesome. This category does not include web pages with content pertaining to physical assault.
Health	Web pages that cover all health-related information and health care services. This category does not include cosmetic surgery, marketing/selling pharmaceuticals, or animal-related medical services.
Historical Revisionism	Web pages that denounce, or offer different interpretations of, significant historical facts, such as holocaust denial. This category does not include all re-examination of historical facts, only historical events that are highly sensitive.
History	Web pages that provide content about historical facts. This category includes content suitable for higher education, but the Education category includes content for primary education. For example, a site with Holocaust photographs might be offensive, but have academic value.

Table 76 Managed Category Descriptions (continued)

Humor Comics	Web pages that provide comical or funny content. This category includes sites with jokes, sketches, comics, and satire pages. This category might also include graphic novel content, which is often associated with comics.
Illegal UK	Web pages that contain child sexual abuse content hosted anywhere in the world, and criminally obscene and incitement to racial hatred content hosted in the UK.
Incidental Nudity	Web pages that contain non-pornographic images of the bare human body like those in classic sculpture and paintings, or medical images. This category enables you to allow or block sites in order to address cultural or geographic differences in opinion about nudity. For example, you can use this category to block access to nudity, but allow access when nudity is not the primary focus of a site, such as news sites or major portals.
Information Security	Web pages that legitimately provide information about data protection. This category includes detailed information for safeguarding business or personal data, intellectual property, privacy, and infrastructure on the Internet, private networks, or in other bandwidth services such as telecommunications. This category does not include: • Legitimate information security companies and security software providers, such as virus protection companies. • Sites that intend to exploit security or teach how to bypass security.
Information Security New	Web pages that legitimately provide information about data protection. This category includes detailed information for safeguarding business or personal data, intellectual property, privacy, and infrastructure on the Internet, private networks, or in other bandwidth services such as telecommunications. This category does not include: • Legitimate information security companies and security software providers, such as virus protection companies. • Sites that intend to exploit security or teach how to bypass security.
Instant Messaging	Web pages that provide software for real-time communication over a network exclusively for users who joined a member's contact list or an instant-messaging session. Most instant-messaging software includes features such as file transfer, PC-to-PC phone calls, and can track when other people log on and off.
Interactive Web Applications	Web pages that provide access to live or interactive web applications, such as browser-based office suites and groupware. This category includes sites with business, academic, or individual focus. This category does not include sites providing access to interactive web applications that do not take critical user data or offer security risks, such as Google Maps.
Internet Radio TV	Web pages that provide software or access to continuous audio or video broadcasting, such as Internet radio, TV programming, or podcasting. Quick downloads and shorter streams that consume less bandwidth are in the Streaming Media or Media Downloads categories.
Internet Services	Web pages that provide services for publication and maintenance of Internet sites such as web design, domain registration, Internet Service Providers, and broadband and telecommunications companies that provide web services. This category includes web utilities such as statistics and access logs, and web graphics like clip art.

Table 76 Managed Category Descriptions (continued)

Job Search	Web pages related to a job search including sites concerned with resume writing, interviewing, changing careers, classified advertising, and large job databases. This category also includes corporate web pages that list job openings, salary comparison sites, temporary employment, and company job-posting sites. This category does not include make-money-at-home sites.
Major Global Religions	Web pages with content about religious topics and information related to major religions. This category includes sites that cover religious content such as discussion, beliefs, non-controversial commentary, articles, and information for local congregations such as a church or synagogue homepage. The religions in this category are Baha'i, Buddhism, Chinese Traditional, Christianity, Hinduism, Islam, Jainism, Judaism, Shinto, Sikhism, Tenrikyo, Zoroastrianism.
Marketing Merchandising	Web pages that promote individual or business products or services on the web, but do not sell their products or services online. This category includes websites that are generally a company overview, describing services or products that cannot be purchased directly from these sites. Examples include automobile manufacturer sites, wedding photography services, or graphic design services. This category does not include: • Other categories that imply marketing such as Alcohol, Auctions/Classifieds, Drugs, Finance/Banking, Mobile Phone, Online Shopping, Real Estate, School Cheating Information, Software/Hardware, Stock Trading, Tobacco, Travel, and Weapons. • Sites that market their services only to other businesses. See the Business category. • Sites that rob or cheat consumers. See the Consumer Protection category.
Media Downloads	Web pages that provide audio or video files for download such as MP3, WAV, AVI, and MPEG formats. The files are saved to, and played from, the user's computer. This category does not include audio or video files that are played directly through a browser window. See the Streaming Media category.
Media Sharing	Web pages that allow users to upload, search for, and share media files and photographs, such as online photograph albums.
Messaging	Examples include text messaging to mobile phones, PDAs, fax machines, and internal website user-to-user messaging or site-to-site messaging. This category does not include real-time chat or instant messaging, or message posts that can be viewed by anyone but the intended recipient.
Mobile Phone	Web pages that sell media, software, or utilities for mobile phones that can be downloaded and delivered to mobile phones. Examples include ringtones, logos/skins, games, screen-savers, text-based tunes, and software for SMS, MMS, WAP, and other mobile phone protocols.
Moderated	Bulletin boards, chat rooms, search engines, or web mail sites that are monitored by an individual or group who has the authority to block messages or content considered inappropriate. This category does not include sites with posted rules against offensive content. See the Forum/Bulletin Boards category.

Table 76 Managed Category Descriptions (continued)

Motor Vehicles	Websites for manufacturers and dealerships of consumer transportation vehicles, such as cars, vans, trucks, SUVs, motorcycles, and scooters. This category also includes sites that provide product marketing, reviews, comparisons, pricing information, auto fairs, auto expos, and general consumer information about motor vehicles. This category does not include automotive accessories, mechanics, auto-body shops, and recreational hobby pages. This category does not include sites that provide business-to-business-only content regarding motor vehicles.
Non Profit Advocacy NGO	Web pages from charitable or educational groups that fulfill a stated mission, benefiting the larger community, such as clubs, lobbies, communities, non-profit organizations, labor unions, and advocacy groups. Examples are Masons, Elks, Boy and Girl Scouts, or Big Brothers.
Nudity	Web pages that have non-pornographic images of the bare human body. This category includes classic sculpture and paintings, artistic nude photographs, some naturism pictures, and detailed medical illustrations. This category does not include high-profile sites where nudity is not a concern for visitors. See the Incidental Nudity category.
Online Shopping	Web pages that sell products or services online. Web pages selling a broad range of products might pose a risk to users by offering access to items that are normally in other categories such as Pornography, Weapons, Nudity, or Violence. Web pages selling such content exclusively are in their respective categories.
P2P File Sharing	Web pages that allow the exchange of files between computers and users for business or personal use, such as downloadable music. P2P clients allow users to search for and exchange files from a peer-user network. They often include spyware or real-time chat capabilities. This category includes BitTorrent web pages.
Parked Domain	Web pages that once served content, but their domains have been sold or abandoned and are no longer registered. Parked domains do not host their own content, but usually redirect users to a generic page that states the domain name is for sale, or redirect users to a generic search engine and portal page, some of which provide valid search engine results.
Personal Network Storage	Web pages that allow users to upload folders and files to an online network server in order to backup, share, edit, or retrieve files or folders from any web browser.
Personal Pages	Personal home pages that share a common domain such as those hosted by ISPs, university/education servers, or free web page hosts. This category also includes unique domains that contain personal information, such as a personal home page. This category does not include home pages of public figures.
Pharmacy	Web pages that provide reviews, descriptions, and market or sell prescription-based drugs, over-the-counter drugs, birth control, or dietary supplements.
Politics Opinion	Web pages covering political parties, individuals in political life, and opinion on various topics. This category might also cover laws and political opinion about drugs. This category includes URLs for political parties, political campaigning, and opinions on various topics, including political debates.
Pornography	Web pages, which provide materials intended to be sexually arousing or erotic. This category includes fetish pages, animation, cartoons, stories, and illegal pornography.

Table 76 Managed Category Descriptions (continued)

Portal Sites	Web pages that serve as major gateways or directories to content on the web. Many portal sites also provide a variety of internal site features or services such as search engines, email, news, and entertainment. Mailing list sites with a variety of content are in this category. This category does not include sites with topic-specific content.
Potential Criminal Activities	Web pages, which provide instructions to commit illegal or criminal activities. Instructions include committing murder or suicide, sabotage, bomb-making, lock-picking, service theft, evading law enforcement, or spoofing drug tests. This category might also include information on how to distribute illegal content, perpetrate fraud, or consumer scams. This category does not include computer-related fraud.
Potential Hacking Computer Crime	Web pages, which provide instructions, or otherwise enable, fraud, crime, or malicious activity that is computer-oriented. This category includes web pages related to computer crime include malicious hacking information or tools that help individuals gain unauthorized access to computers and networks (root kits, kiddy scripts). This category also includes other areas of electronic fraud such as dialer scams and illegal manipulation of electronic devices. This category does not include illegal software.
Potential Illegal Software	Web pages, which the filter believes offer information to potentially 'pirated' or illegally distribute software or electronic media, such as copyrighted music or film, distribution of illegal license key generators, software cracks, and serial numbers. This category does not include peer-to-peer web pages.
Private IP Addresses	Sites that are private IP addresses as defined in RFC 1918, that is, hosts that do not require access to hosts in other enterprises (or require just limited access) and whose IP address may be ambiguous between enterprises but are well defined within a certain enterprise.
Profanity	Web pages that contain crude, vulgar, or obscene language or gestures.
Professional Networking	Web pages that provide social networking exclusively for professional or business purposes. This category includes sites that provide personal or group profiles, and enable their members to interact through real-time communication, message posting, public bulletins, and media sharing. This category also contains alumni sites that have a networking function. This category does not include social networking sites where the focus might vary, but include friendship, dating, or professional focuses.
Provocative Attire	Web pages with pictures that include alluring or revealing attire, lingerie and swimsuits, or supermodel or celebrity photograph collections, but do not involve nudity. This category does not include sites with swimwear or similar attire that is not intended to be provocative. For example, Olympic swimming sites are not in this category.
Public Information	Web pages that provide general reference information such as public service providers, regional information, transportation schedules, maps, or weather reports.
PUPs	Web pages that contain Potentially Unwanted Programs (PUPs). PUPs are often made for a beneficial purpose but they alter the security of a computer or the computer user's privacy. Computer users who are concerned about security or privacy might want to be informed about this software, and in some cases, they might want to remove this software from their computers.

Table 76 Managed Category Descriptions (continued)

Real Estate	Web pages that provide commercial or residential real estate services and information. Service and information includes sales and rental of living space or retail space and guides for apartments, housing, and property, and information on appraisal and brokerage. This category includes sites that allow you to browse model homes. This category does not include content related to personal finance, such as credit applications.
Recreation Hobbies	Web pages for recreational organizations and facilities that include content devoted to recreational activities and hobbies. This category includes information about public swimming pools, zoos, fairs, festivals, amusement parks, recreation guides, hiking, fishing, bird watching, or stamp collecting. This category does not include activities that need no active participation, such as watching a movie or reading celebrity gossip.
Religion Ideology	Web pages with content related to religious topics and beliefs in human spirituality that are not within the major religions. This category includes religious discussion, beliefs, articles, and information for local congregations or groups such as a church homepage, unless the site is already in the Major Global Religions category. This category also includes comparative religion, or sites that include religions and ideologies. This category does not include astrology and horoscope sites
Remote Access	Web pages that provide remote access to a program, online service, or an entire computer system. Although remote access is often used legitimately to run a computer from a remote location, it creates a security risk, such as backdoor access. Backdoor access, written by the original programmer, allows the system to be controlled by another party without the user's knowledge.
Reserved	This category is reserved for future use.
Residential IP Addresses	IP addresses (and any domains associated with them) that access the Internet by DSL modems or cable modems. Because this content is not generally intended for Internet access via HTTP, access to the Internet through these IP addresses can indicate suspicious behavior. This behavior might be related to malware located on the home computer or homegrown gateways set up to allow anonymous Internet access.
Resource Sharing	Web pages that harness idle or unused computer resources to focus on a common task. The task can be on a company or an international basis. Well known examples are the SETI program and the Human Genome Project, which use the idle time of thousands of volunteered computers to analyze data.
Restaurants	Web pages that provide information about restaurants, bars, catering, take-out and delivery, including online ordering. This category includes sites that provide information about location, hours, prices, menus and related dietary information. This category also includes restaurant guides and reviews, and cafes and coffee shops. This category does not include groceries, wholesale food, non-profit and charitable food organizations, or bars that do not focus on serving food.
School Cheating Information	Web pages that promote plagiarism or cheating by providing free or fee-based term papers, written essays, or exam answers. This category does not include sites that offer student help, discuss literature, films, or books, or other content that is often the subject of research papers.

Table 76 Managed Category Descriptions (continued)

Search Engines	Web pages that provide search results that enable users to find information on the Internet based on key words. This category does not include site-specific search engines.
Sexual Materials	Web pages that describe or depict sexual acts, but are not intended to be arousing or erotic. Examples of sexual materials include sex education, sexual innuendo, humor, or sex related merchandise. This category does not include web pages with content intended to arouse.
Shareware Freeware	Web pages that are repositories of downloadable copies of shareware and freeware. This category does not include subscription-based software.
Social Networking	Web pages that enable social networking for a variety of purposes, such as friendship, dating, professional, or topics of interest. These sites provide personal or group profiles and enable interaction among their members through real-time communication, message posting, public bulletins, and media sharing. This category does not include sites that are exclusive to dating, matchmaking, or a specific professional networking focus.
Software Hardware	Web pages related to computing software and hardware, including vendors, product marketing and reviews, deployment and maintenance of software and hardware, and software updates and add-ons such as scripts, plug-ins, or drivers. Hardware includes computer parts, accessories, and electronic equipment used with computers and networks. This category includes the marketing of software and hardware, and magazines focused on software or hardware product reviews or industry trends.
Sports	Web pages related to professional or organized recreational sports. This category includes sporting news, events, and information such as playing tips, strategies, game scores, or player trades. This category does not include fantasy leagues, sports centers, athletic clubs, fitness or martial arts clubs, and non-league billiards, darts, or other such activities.
Stock Trading	Web pages that offer purchasing, selling, or trading of shares online. This category also includes ticker-tape information that enables viewing of real-time stock prices and financial spread betting in the stock market. Other betting is in the Gambling category. This category does not include sites that offer information about stocks, but do not offer purchasing, selling, or trading of shares.
Streaming Media	Web pages that provide streaming media, or contain software plug-ins for displaying audio and visual data before the entire file has been transmitted. This category does not include audio or video files that are downloaded to a user's computer before being played.
Technical Business Forums	Web pages with a technical or business focus that provide online message posting or real-time chatting, such as technical support or interactive business communication. Although users can post any type of content, these forums tend to present less risk of containing offensive content. Sites that offer a variety of forums with themes, including technical and business content, are only in the categories of Forum/Bulletin Boards or Chat.

Table 76 Managed Category Descriptions (continued)

Technical Information	Web pages that provide computing information with an educational focus in areas such as Information Technology, computer programming, and certification. Examples include Linux user groups, UNIX commands, software tutorials, or dictionaries of technical terms. Most sites in this category might be subdirectories of larger domains. For example, a software site with a tutorial page is in this category only at the tutorial page URL. This category does not include content about information security.
Text Spoken Only	Content that is text or audio only, and does not contain pictures. This category can be used as an exception to allow explicit text and recorded material to be accessed when you want pictures blocked using the Pornography, Violence, or Sexual Materials categories. Libraries or universities can use this category to prevent the display of offensive graphics in their public facilities.
Text Translators	Web pages that allow users to type phrases or a block of text to translate it from one language into another. This category also includes language identifier web pages. URL translation is in the Anonymizing Utilities category.
Tobacco	Web pages that sell, promote, or advocate the use of tobacco products, tobacco paraphernalia, including cigarettes, cigars, pipes, snuff and chewing tobacco.
Travel	Web pages that promote personal or business travel, such as hotels, resorts, airlines, ground transportation, car rentals, travel agencies, and general tourist and travel information. This category also includes sites for buying tickets or accommodation. This category does not include personal vacation photographs.
Usenet News	Web pages that provide access (http://) to Usenet newsgroups and archives of files uploaded to newsgroups. This category also includes online groups that offer similar community-oriented content posting.
Violence	Web pages that contain real or lifelike images or text that portray, describe, or advocate physical assaults against people, animals, or institutions, such as depictions of war, suicide, mutilation, or dismemberment.
Visual Search Engine	Web pages that provide image-specific search results such as thumbnail pictures. This category does not include sites that offer site-specific visual search engines.
Weapons	Web pages that provide information about buying, making, modifying, or using weapons, such as guns, knives, swords, paintball guns, and ammunition, explosives, and weapon accessories. This category also includes sites that contain content for: weapons for personal or military use, homemade weapons, non-lethal weapons such as mace, pepper spray, or Taser guns, weapons facilities, such as shooting ranges, and government or military oriented weapons. This category does not include political action groups, such as the NRA.

Table 76 Managed Category Descriptions (continued)

Web Ads	Web pages that provide advertisement-hosting or programs that create advertisements. Examples include links, source code or applets for banners, popups, and other kinds of static or dynamically generated advertisements that appear on web pages. This category is intended to block advertisements on web pages, not the companies that provide the advertisements or advertising services. This category does not include aggressive advertising adware. See the Spyware/Adware category.
Web Mail	Web pages that enable users to send or receive email through the Internet.
Web Meetings	Web pages that host live meetings, video conferences, and interactive presentations mainly for businesses. Web meetings generally include streaming audio and video, and allow data transfer or office-oriented application sharing, such as online presentations.
Web Phone	Web pages that enable users to make telephone calls via the Internet or obtain information or software for this purpose. Web Phone service is also called Internet Telephony, or VoIP. Web phone service includes PC-to-PC, PC-to-phone, and phone-to-phone services connecting via TCP/IP networks.
Unrated	Web pages that cannot be categorized into any of the categories listed above.

CHAPTER 21
Sandboxing

21.1 Sandboxing Overview

Zyxel sandbox is a security mechanism which provides a safe environment to separate running programs from your network and host devices. Files with unknown or untrusted programs and codes are uploaded to the cloud. These files are executed within an isolated virtual machine (VM) to monitor and analyze the zero-day malware and advanced persistent threats (APTs). The zero-day malware refers to malware that is unknown to any software vendor or developer. It is dangerous because there is no available defenses against it at the time of discovery.

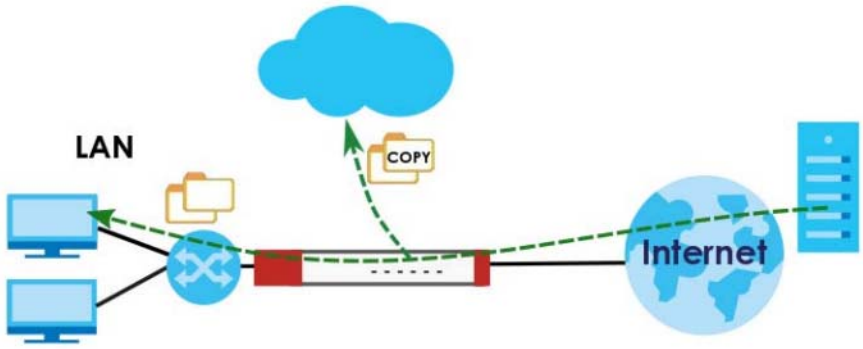
The zero-day malware and APTs may evade the Zyxel Device's detection, such as anti-malware. Results of cloud sandbox are sent from the server to the Zyxel Device.

After checking the received files against its local cache, the Zyxel Device sandbox uploads a copy of the files for inspection if the files are not recorded in the local cache. The scan result from the cloud is added to the Zyxel Device cache and used for future inspection. When a file with malicious or suspicious code is detected, the Zyxel Device takes specific actions on the threats.

By default, the Zyxel Device sandbox forwards all files that have not been checked before to the clients behind the Zyxel Device.

Note: The scan results will be removed from the Zyxel Device cache after the Zyxel Device restarts. When the scan results stored reach the limit, new scan results automatically overwrite existing scan results, starting with the oldest scan result first.

Figure 43 Zyxel Sandbox Inspection



The Zyxel Device forwards files that are not recorded in the local cache to the client behind the Zyxel Device before sandbox has completed checking. The scan result will display in the logs. We suggest you to inform your client not to open the file until sandbox has completed checking. If the client already opened it, then please urge the client to run an up-to-date anti-malware scanner.

If the receiver of a suspect file cannot open a file, sandbox may have already modified the file by deleting the infected portion. Please check the logs and let the receiver know if this is so.

21.2 Sandbox Commands

The following table describes the sandbox commands. You must use the edit running command to enter the configuration mode before you can use these commands.

Table 77 Sandbox Commands

COMMAND	DESCRIPTION
vrf main sandbox enabled {true| false}	Turns on sandbox on the Zyxel Device. The false command disables sandbox.
vrf main sandbox statistics enabled {true| false}	Enable to have the Zyxel Device collect sandbox statistics, such as the time, type and name of the files scanned.
vrf main sandbox malicious action {allow| destroy} logging {no| log| log-alert}	Sets whether the Zyxel Device deletes (destroy) or forwards (allow) malicious files. This also sets the Zyxel Device to generate a log, log and alert or neither (no) when a malicious file is detected. Malicious files are files given a high score for malware characteristics by the cloud. You can check the medium score for malware characteristics given by the cloud in the logs.
vrf main sandbox suspicious action {allow| destroy} logging {no| log| log-alert}	Sets whether the Zyxel Device deletes (destroy) or forwards (allow) suspicious files. This also sets the Zyxel Device to generate a log, log and alert or neither (no) when a suspicious file is detected. Suspicious files are files given a medium score for malware characteristics by the cloud. You can check the medium score for malware characteristics given by the cloud in the logs.
vrf main sandbox file-type {archives| executables| ms-office-document| macromedia-flash-data| pdf| rtf}	Specifies the type of files to be sent for sandbox inspection. • archives: A zip file is a file used to compress multiple files together into a single file. A zip file can reduce the overall size of a collection of files. • executables: An executable file is a file that contains a program or application which your computer can run • ms-office-document: This category includes Microsoft Word files, Microsoft Excel files and Microsoft PowerPoint files. MS Office Document are files that are created using software developed by Microsoft. • macromedia-flash-data: A flash file (.swf) is a file that contains animations, multimedia elements or games. A flash file is often embedded into a web page. • pdf: A Portable Document Format (PDF) file is a file that maintains the presentation and formatting of documents across different platform and devices. • rft: A Rich Text Format (RTF) file is a file that allows you to create text with different formats, such as bold or italics.
show state vrf main sandbox statistics {summary| top-entry| event}	Displays: • a summary of the collected sandbox statistics. • top log entries by destination IP, source IP and type. • the time, type, file name, hash, destination IP and source IP of the files scanned.

21.2.1 Sandbox Command Examples

This command shows how to enable sandbox on the Zyxel Device and displays the status of security services.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main sandbox enabled true
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show state vrf main sandbox statistics summary
summary
    scanning 0
    scanned 0
    destroyed-files 0
    malicious-files 0
    suspicious-files 0
    safe-files 0
    other 0
```

This command sets the Zyxel Device to delete malicious files and generate a log when a malicious file is detected.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main sandbox malicious action destroy logging log
usgflex200hp running config# commit
Configuration committed.
```

CHAPTER 22
SSL Inspection

22.1 SSL Inspection Overview

Secure Socket Layer (SSL) traffic, such as HTTPS, POP3+SSL, and SMTPS, is encrypted and therefore cannot be inspected using Unified Threat Management (UTM) profiles such as App Patrol, Content Filter, Intrusion Prevention System (IPS), or Anti-Malware. The Zyxel Device uses SSL Inspection to decrypt SSL traffic, sends it to the Security Service engines for inspection, then encrypts traffic that passes inspection and forwards it to the destination server, such as Google.

The Zyxel Device supports the following SSL/TLS versions and cipher suites:

- TLS1.0 AES-CBC
- TLS1.2 AES-CBC/AES-GCM
- TLS1.3

SSL inspection does not support the following:

- Compression
- Client Authentication
- SSLv3 AES-CBC

22.2 SSL Inspection Command Input Values

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

Table 78 SSL Inspection Command Input Values

LABEL	DESCRIPTION
profile-name	This is the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
description	This is additional information about this SSL Inspection profile. You can enter up to 60 characters ("0-9", "a-z", "A-Z", "-" and "_").
cert-name	This is a name of a certificate.

22.3 SSL Inspection General Commands

The table lists the SSL inspection general commands.

Table 79 SSL Inspection General Commands

COMMAND	DESCRIPTION
`vrf main ssl-inspection server-sign-cert mode {rsa-1024| rsa-2048| ecdsa-rsa-1024| ecdsa-rsa-2048}`	Select how to validate a client accessing an HTTPS website using RSA or ECDSA encryption through the Zyxel Device. ECDSA is required by certain clients such as iOS 13. The Zyxel Device must check that the client's certificate and public key are valid and were issued by a Certificate Authority (CA) listed in the Zyxel Device's list of trusted CAs. The default value is 1024. • `ecdsa-rsa-1024` means the Zyxel Device uses ECDSA-256 if the client supports ECDSA-256, or RSA-1024 if the client does not support ECDSA-256. • `ecdsa-rsa-2048` means the Zyxel Device uses ECDSA-256 if the client supports ECDSA-256, or RSA-2048 if the client does not support ECDSA-256. Note: You should flush the SSL inspection certificate cache after changing the server signing mode.
`vrf main ssl-inspection default-port enabled {true| false}`	Sets the Zyxel Device only scan traffic going through the specified ports. The default specified ports are 443 (HTTPS), 465 (SMTP), 993 (IMAP) and 995 (POP3). You can remove or add a port to this list by using the `extra-port` or the `exception-port` commands. Disables this to have the Zyxel Device scan traffic going through all ports.
`vrf main ssl-inspection default-port {extra-port| exception-port}` *port number*	Uses the `extra-port` command to add a port to the default specified port list. Uses the `exception-port` command to remove a port from the default specified port list.
`show config vrf main ssl-inspection server-sign-cert mode`	Displays the type of encryption used to validate a client accessing an HTTPS website through the Zyxel Device.
`show config vrf main ssl-inspection default-port enabled`	Displays if the default port is enabled.
`show state vrf main ssl-inspection default-cert-version`	Displays: • The current certificate set version. • The date and time the current certificate set was released.
`show state vrf main ssl-inspection default-port-state`	Displays the Zyxel Device default ports.
`show state vrf main ssl-inspection cert-list`	Displays certificates used in SSL Inspection.

22.4 SSL Inspection Exclusion Commands

There may be privacy and legality issues regarding inspecting a user's encrypted session. The legal issues may vary by locale, so it's important to check with your legal department to make sure that it's OK to intercept SSL traffic from your Zyxel Device users.

To ensure individual privacy and meet legal requirements, you can configure an exclusion list to exclude matching sessions to destination servers. This traffic is not intercepted and passes through the Zyxel Device uninspected.

This table lists the SSL inspection exclusion-related commands.

Table 80 SSL Inspection Exclusion Commands

COMMAND	DESCRIPTION
`vrf main ssl-inspection exclude-list-settings log-enabled {true| false}`	Create a log for traffic that bypasses SSL inspection. The `false` command disables SSL exclusion list logging.
`vrf main ssl-inspection exclude-list <exclude-list entry>`	Create an entry in one of the following ways: • Type an IPv4. For example, type 192.168.1.35 • Type an IPv4 block in CIDR notation. For example, type 192.168.1.1/24 • Type an IPv4 address range by entering the start and end addresses separated by a hyphen (-). For example, type 192.168.1.1-192.168.1.35 • Type a DNS name. For example, type www.zyxel.com.tw. • Type a common name (wildcard char: '*', escape char: '\'). Use up to 127 case-insensitive characters (0-9a-zA-Z`~!@#$%^&*()-_=+[]{}\ | ;:',.<>/?). '*' can be used as a wildcard to match any string. Use '*' to indicate a single wildcard character. • Type an email address. For example, type abc@zyxel.com.tw
`show config vrf main ssl-inspection exclude-list-settings log-enabled`	Displays whether the Zyxel Device will create a log for traffic that bypasses SSL inspection.
`show config vrf main ssl-inspection exclude-list`	Displays the SSL inspection exclude list settings.

22.5 SSL Inspection Profile Settings

This table lists the SSL inspection profile setting commands.

Table 81 SSL Inspection Profile Commands

COMMAND	DESCRIPTION
`vrf main ssl-inspection profile <profile-name>`	Creates an SSL inspection profile, and then enters the SSL inspection profile sub-command mode. The profile name may consist of 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`description <description>`	Enter additional information about this SSL inspection entry. You can enter up to 60 characters (0-9az-A-Z'()+:=?;!*#@$_%-").
`support-version-min version {tls1_0| tls1_1| tls1_2}`	The Zyxel Device only inspects SSL traffic if the SSL version is equal to this value or higher.

Table 81 SSL Inspection Profile Commands

COMMAND	DESCRIPTION
support-version-min logging {no| log| log-alert}	Sets whether the Zyxel Device generates a log or a log and an alert for unsupported traffic that matches traffic bound to this profile. The Zyxel Device will not generate a log if you use the no command.
unsupported-suite action {pass| block}	Select to pass or block unsupported traffic, such as traffic using unsupported cipher suites, compression, or client authentication.
unsupported-suite logging {no| log| log-alert}	Sets whether the Zyxel Device generates a log or a log and an alert for unsupported traffic tat matches traffic bound to this profile. The Zyxel Device will not generate a log if you use the no command.
untrusted-cert-chain action {pass| block| inspect}	Sets whether to pass, inspect, or block an untrusted certification chain. A certificate chain is a certification process that involves the following certificates between the SSL/TLS server and a client. A certificate chain will fail if one of the following certificates is not correct. • A certificate owned by a user • The certificate signed by a certification authority • A root certificate
untrusted-cert-chain logging {no| log| log-alert}	Sets whether the Zyxel Device generates a log or a log and an alert for unsupported traffic tat matches traffic bound to this profile. The Zyxel Device will not generate a log if you use the no command.
certificate *<cert-name>*	Sets the certificate for this profile.
show config vrf main ssl-inspection profile	Displays the SSL inspection profiles settings.

22.6 SSL Inspection Certificate Update

Use these commands to update the latest certificates of servers using SSL connections to the Zyxel Device network. You must have Internet access and have activated SSL Inspection on the Zyxel Device at myZyxel.com.

This table lists the SSL inspection certificate cache commands.

Table 82 SSL Inspection Certificate Update Commands

COMMAND	DESCRIPTION
cmd ssl-inspection cert-update now	Download the latest certificate set from the myZyxel.com and update it on the Zyxel Device.
vrf main ssl-inspection cert-update auto {true| false}	The Zyxel Device automatically updates the certificate set when a new one becomes available on myZyxel.com.
show config vrf main ssl-inspection cert-update auto	Displays if automatically updating the certificate set is configured on the Zyxel Device.

22.7 SSL Inspection Statistics

This table lists the SSL inspection statistics commands.

Table 83 SSL Inspection Statistics Commands

COMMAND	DESCRIPTION
`vrf main ssl-inspection statistics enabled {true| false}`	Enables SSL inspection statistics collection. The `false` command disables SSL exclusion statistics collection.
`show state vrf main ssl-inspection statistics summary`	Displays SSL inspection statistics such as concurrent sessions, total SSL sessions, sessions inspected, decrypted Kilobytes, encrypted Kbytes, sessions blocked, and sessions passed.
`show config vrf main ssl-inspection statistics enabled`	Displays if SSL inspection statistics collection is enabled.

22.8 SSL Inspection Debug Command

This table lists the SSL inspection debug commands.

Table 84 SSL Inspection Debug Commands

COMMAND	DESCRIPTION
`cmd debug ssl-inspection console enabled {true | false}`	Enables SSL inspection debug logs regarding data encryption and decryption on the Command Line Interface (CLI). The `false` command disables SSL inspection debug logs on the CLI.
`cmd debug ssl-inspection daemon console enabled {true | false}`	Enables daemon debug logs regarding certificate queries on the CLI. The `false` command disables daemon debug logs on the CLI.

22.9 SSL Inspection Command Examples

These are some other example SSL Inspection usage commands.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main ssl-inspection statistics enabled true
usgflex200hp running config# vrf main ssl-inspection exclude-list 1.1.1.1
usgflex200hp running config# vrf main ssl-inspection exclude-list 2.2.2.2
usgflex200hp running config# vrf main ssl-inspection profile Config1
usgflex200hp running profile Config1# support-version-min version tls1_1
usgflex200hp running profile Config1# support-version-min logging log
usgflex200hp running profile Config1# unsupported-suite action block
usgflex200hp running profile Config1# unsupported-suite logging log-alert
usgflex200hp running profile Config1# untrusted-cert-chain action block
usgflex200hp running profile Config1# untrusted-cert-chain logging log-alert
usgflex200hp running profile Config1# certificate default
usgflex200hp running profile Config1# commit
Configuration committed.
usgflex200hp running profile Config1# exit
usgflex200hp> edit running
usgflex200hp running config# show config vrf main ssl-inspection profile
profile Config1
    certificate default
    support-version-min
        version tls1_1
        logging log
        ..
    unsupported-suite
        action block
        logging log-alert
        ..
    untrusted-cert-chain
        action block
        logging log-alert
        ..
usgflex200hp running config# show config vrf main ssl-inspection exclude-list
exclude-list 1.1.1.1
exclude-list 2.2.2.2
```

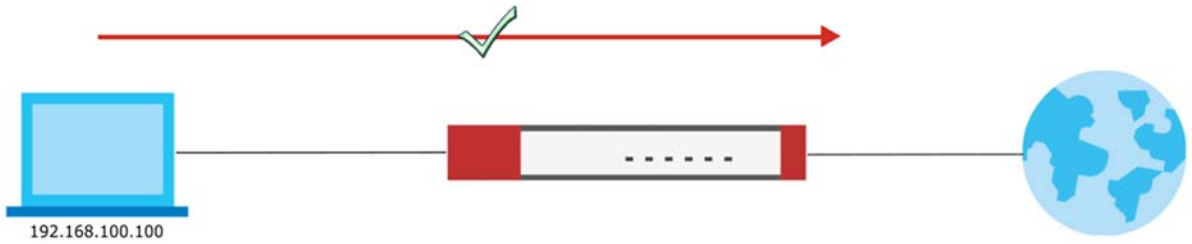
CHAPTER 23
IP Exception

23.1 IP Exception Overview

IP Exception allows incoming IP packets to bypass specific security services based on the packet's source or destination address. Bypassing a security service means the security service does not intercept nor inspect the packet.

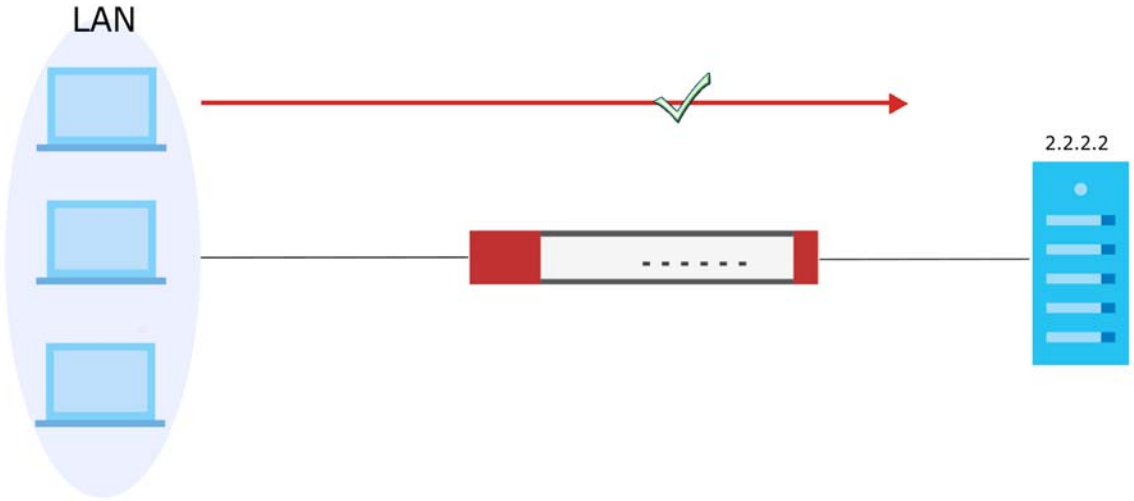
For example, 192.168.100.100 is a trusted LAN computer. Add the IP address of the LAN computer to **Source** in **IP Exception** so the Zyxel Device will not perform security checking on traffic coming from this computer.

Figure 44 IP Exception Bypass Source Example



You can also add a trusted destination to bypass security checking. For example, 2.2.2.2 is a trusted web site. Add the IP address of the trusted web site to **Destination** in **IP Exception** so the Zyxel Device will not perform security checking when you access the web site to save resources.

Figure 45 IP Exception Bypass Destination Example



IP Exception supports bypassing the following security services:

- Anti-Malware
- URL Threat Filter
- IPS (Intrusion Prevention System)
- IP Reputation.
- DNS Threat Filter

23.2 IP Exception Command Input Values

The following table identifies the values required for many IP Exception commands.

Table 85 IP Exception Command Input Values

LABEL	DESCRIPTION
profile-name	The name of an IP Exception rule. You may use 2-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
address-name	The source or destination address of an IP packet. The address name can be any of the following: • Address object name • Address group object name • FQDN object name For details on addresses, see Chapter 25 on page 171.

23.3 IP Exception Commands

The Zyxel Device excludes incoming packets that match any IP Exception rule. Each IP Exception rule contains a source address, destination address, and a list of bypassed services.

The following table lists the IP Exception commands.

Table 86 IP Exception Commnands

COMMAND	DESCRIPTION
`vrf main ip-exception profile <profile-name>`	Creates an IP exception profile, and then enters the IP exception profile sub-command mode. The profile name may consist of 2-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
`source address-object {ipv4-address address-name| ipv4-group address-name| any}`	Sets an address object of the source IP address for this profile. Uses the any command to have no restriction on the source IP address.
`destination address-object {ipv4-address address-name| ipv4-group address-name| any}`	Sets an address object of the destination IP address for this profile. Uses the any command to have no restriction on the destination IP address.

Table 86 IP Exception Commnands

COMMAND	DESCRIPTION
logging {no| log}	Sets whether the Zyxel Device creates a log when the incoming traffic matches the settings you configured in the profile.
{anti-malware| url-threat-filter| ips| ip-reputation| dns-threat-filter} {pass| bypass}	Sets the service that IPv4 packets will bypass. To bypass multiple services, run the command multiple times.
show config vrf main ip-exception profile	Displays the IP exception profiles settings.

CHAPTER 24
User/Group

24.1 User Account Overview

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

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

24.1.1 User Types

These are the types of user accounts the Zyxel Device uses.

Table 87 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
Admin	Change Zyxel Device configuration (web, CLI)	WWW, SSH, FTP, Console
Viewer	Look at the Zyxel Device settings (web) Perform basic diagnostics (CLI)	WWW, SSH, Console
Access Users		
User	Access network services	WWW
Ext-User	External user account	WWW

24.2 User/Group Command Input Values

The following table identifies the values required for the user/group commands. Other input values are discussed with the corresponding commands.

Table 88 User/Group 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.

24.3 User Commands

The first table lists the commands for users. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 89 User/Group Commands: Users

COMMAND	DESCRIPTION
`object user-object admin <username> role {admin| viewer}`	Creates an admin account and sets the user type to admin or viewer. Presses enter to enter the sub-command mode.
`object user-object user <username> role {user| ext-user}`	Creates a user account and sets the user type to user or ext-user. Presses enter to enter the sub-command mode.
`object user-object user {radius-users| ldap-users| ad-users} role {user| ext-user}`	Sets the user type of the default user account for AD users, LDAP users or RADIUS users. Presses enter to enter the sub-command mode.
`enabled {true| false}`	Enables or disables the user account. All user accounts are enabled by default. Make sure to notify the account owner before you disable a user account. Be careful not to disable your own account.
`{password| password-shadow} <password>`	Sets the password for the user account. Uses the `password` command to enter the sub-command mode to set the password then retype to confirm the password. Uses the `password-shadow` command to set the password in plain text without having to retype to confirm the password.
`description <description>`	Sets the description for the specified user. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are not allowed.
`mobile <mobile-number>`	Sets the mobile phone number for the account. You can use up to 20 character length, including numbers 1~9 and characters +*#()-
`email <email-address>`	Specifies up to two email addresses for a user account.
`logon-lease-time {default| 0...7200}`	Sets the lease time for the specified user. Set it to zero to set unlimited lease time. The default value is 1440 (minutes).
`logon-reauth-time {default| 0...7200}`	Sets the reauthorization time for the specified user. The default value is 1440 (minutes).

Table 89 User/Group Commands: Users

COMMAND	DESCRIPTION
`show config object user-object {admin| user}`	Displays general information of admin accounts and user accounts, such as: • The account role. • If the account is enabled. • Authentication timeout settings.
`show state object user-object {admin| user}`	Displays detailed information of admin accounts and user accounts, such as: • Account password in cipher text. • Account email and mobile number. • The date the account is created. • The password is modified.

24.4 Group Commands

This table lists the commands for groups of users. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 90 User/Group Commands: Groups

COMMAND	DESCRIPTION
`object user-object group <groupname>`	Creates the specified user group and enters sub-command mode.
`description <description>`	Sets the description for the specified user group. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are not allowed.
`user-list <username>`	Adds the specified user to the specified user group.
`group-list <groupname>`	Adds the specified user group to the user group you're configuring.
`show config object user-object group`	Displays general information of the group settings, such as group names and users included in each group.
`show state object user-object group`	Displays detailed information of the group settings, such as group names, users included in each group and the number of times a group is used in other settings.

24.5 User Setting Commands

This table lists the commands for user settings, except for forcing user authentication. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 91 User/Group Commands: Setting

COMMAND	DESCRIPTION
`system user-setting default-logon-lease-time {admin| user| ext-user} <0...7200>`	Sets the default lease time (in minutes) for each new user. Set it to zero to set unlimited lease time.
`system user-setting default-logon-reauth-time {admin| user| ext-user} <0...7200>`	Sets the default reauthorization time (in minutes) for each new user. Set it to zero to set unlimited reauthorization time.
`system user-setting pwd-expiry force-change-pwd {true| false}`	Forces users to change their password after a certain period of time.
`system user-setting pwd-expiry expiration-days <1...365>`	Sets how often users must change their password.
`system user-setting pwd-expiry link-to-device <IP/FQDN>`	Enters an IP address or FQDN to associate the password expiration settings to a specific Zyxel Device.
`system user-setting simultaneous-logon administration-enforce {true| false}`	Sets a limit on the number of simultaneous logins by admin users. Disables this to allow admin users to log in as many times as they want at the same time using the same or different IP addresses.
`system user-setting simultaneous-logon administration-limit <1...300>`	Sets the maximum number of simultaneous logins by each admin user.
`system user-setting simultaneous-logon access-enforce {true| false}`	Enables this to set a limit on the number of simultaneous logins by non-admin users. Disables this to allow non-admin users to log in as many times as they want as long as they use different IP addresses.
`system user-setting simultaneous-logon access-enforce <1...300>`	Sets the maximum number of simultaneous logins by each non-admin user.
`system user-setting simultaneous-logon kick-previous {true| false}`	Sets the action the Zyxel Device will take when the limit you set for the numbers of simultaneous logins by admin users or non-admin users has exceeded. Enables this to have the Zyxel Device remove the earliest login account. Disables this to have the Zyxel Device block any accounts that try to log in.
`system user-setting retry-limit enabled {true| false}`	Enables the retry limit for users.
`system user-setting retry-limit 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 default value is five.
`system user-setting retry-limit lockout-period <1...6553>`	Sets the amount of time, in minutes, a user or IP address is locked out after retry-count number of failed login attempts. The default value is 30.

Table 91 User/Group Commands: Setting

COMMAND	DESCRIPTION
system user-setting update-lease-auto {true| false}	Enables this to let users automatically renew their lease time. Disables this to prevent them from automatically renewing it.
show config system user-setting	Displays the user settings you configured on the Zyxel Device.
show state system user-setting	Displays the status of user settings on the Zyxel Device.

24.5.1 User Setting Command Examples

The following commands show the current settings for the number of simultaneous logins.

```
usgflex200hp> edit running
usgflex200hp running config# system user-setting simultaneous-logon
administration-enforce true
usgflex200hp running config# system user-setting simultaneous-logon
administration-limit 50
usgflex200hp running config# system user-setting simultaneous-logon access-enforce
true
usgflex200hp running config# system user-setting simultaneous-logon access-limit 50
usgflex200hp running config# system user-setting simultaneous-logon kick-previous
true
usgflex200hp running config# commit
Configuration committed.
```

24.5.2 Create User Accounts Command Examples

Lease time is the idle timeout for a specific user. A logged in user must use the web configurator or CLI before he is logged out.

Reauthentication time is the number of minutes the user can be logged into the Zyxel Device in one session before the user has to log in again.

For example, suppose you've set the lease time to 30 minutes and the reauthentication time to 60 minutes. See the comparison table below for more information on the differences between lease time and reauthentication time.

Table 92 Lease Time and Reauthentication Time Comparison Table

	USER ACTION	RESULT
Lease Time	The user has used the Zyxel Device web configurator or CLI within 30 minutes.	The user will not be logged out.
	The user has not used the Zyxel Device web configurator or CLI for over 30 minutes.	The user will be logged out.

Table 92 Lease Time and Reauthentication Time Comparison Table

	USER ACTION	RESULT
Reauthentication Time	The user has used the Zyxel Device web configurator or CLI within 60 minutes.	After 60 minutes, the user will be logged out. He must log in again.
	The user has not used the Zyxel Device web configurator or CLI for over 60 minutes.	

You want to log the admin account **Max** out if 60 minutes of idle time have passed, that is, he has not been using the Zyxel Device web configurator or CLI.

You want to make the number of minutes unlimited so the admin account **Max** will not have to log in again after a certain time period.

Table 93 Create User Account Example

USER NAME	PASSWORD	USER TYPE
Max	1234	admin

1 Create an admin account using the parameters given above.

```
usgflex200hp> edit running
usgflex200hp running config# object user-object user Max role user
usgflex200hp running config# object user-object user Max
usgflex200hp running user Max# password
Enter value for password>
Confirm value for password>
usgflex200hp running user Max# logon-lease-time 60
usgflex200hp running user Max# logon-reauth-time 0
```

2 Save the current configuration to the Zyxel Device.

```
usgflex200hp running user Max# commit
Configuration committed.
```

24.5.3 User/Group Additional Commands

This table lists additional commands for users.

Table 94 User/Group Additional Commands

COMMAND	DESCRIPTION
`show users`	Displays information about the users logged onto the system.
`show lockout-users`	Displays users who are currently locked out.
`cmd lockout-users unlock ip <IP-Address>`	Unlocks the specified IP address.
`cmd users force-logout {user | ip | service}`	Logs out the specified login.

CHAPTER 25 Addresses

25.1 Address Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

You can create IP address objects based on an interface's IP address, subnet, or gateway. The Zyxel Device automatically updates these objects whenever the interface's IP address settings change. This way every rule or setting that uses the object uses the updated IP address settings. For example, if you change the LAN1 interface's IP address, the Zyxel Device automatically updates the corresponding interface-based, LAN1 subnet address object. So any configuration that uses the LAN1 subnet address object is also updated.

Address objects and address groups are used in dynamic routes, firewall rules, application patrol, content filtering, and VPN connection policies. For example, addresses are used to specify where content restrictions apply in content filtering. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

25.2 Address Command Input Values

The following table describes the values required for many address object and address group commands. Other values are discussed with the corresponding commands.

Table 95 Address Commands Input Values

LABEL	DESCRIPTION
object-name	The name of the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
group-name	The name of the address group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
interface	The name of the interface. This depends on the Zyxel Device model. Use ge*x*, *x* = 1 ~ N, where N equals the highest numbered Ethernet interface for your Zyxel Device model.

25.2.1 Address Object Commands

There are the types of address objects:

- **HOST** - the object uses an IP address to define a host address
- **RANGE** - the object uses a range address defined by a **Starting IP Address** and an **Ending IP Address**
- **SUBNET** - the object uses a network address defined by a **CIDR** (Classless Inter-Domain Routing)
- **INTERFACE IP** - the object uses the IP address of one of the Zyxel Device's interfaces
- **INTERFACE SUBNET** - the object uses the subnet mask of one of the Zyxel Device's interfaces
- **INTERFACE GATEWAY** - the object uses the gateway IP address of one of the Zyxel Device's interfaces
- **GEOGRAPHY** - the object uses the IP addresses of a country to represent a country

This table lists the commands for address objects. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 96 Address Object Commands: Addresses

COMMAND	DESCRIPTION
`object address-object address <object-name> description <description>`	Enters the description associated with the zone. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/ :=?;!*#@$_%-" Spaces are note allowed.
`object address-object address <object-name> type {host IP| cidr cidr| range IP-range| geography country-code| interface-ip interface| interface-subnet interface| interface-gateway interface}`	Creates or edits the specified IPv4 address object using the specified parameters. • IP: Enter an IPv4 address. • IP Range: Enter an IPv4 address range. • CIDR: Enter an IPv4 subnet in CIDR format. For example, 192.168.1.0/32. • Country Code: Enter a country or continent code (represents an IP address for that country/continent). • Interface IP/Interface Subnet/ Interface Gateway: Enter an interface name or virtual interface name.
`show state object address-object address`	Displays the status of the address object settings, such as the address object type, interface, IP address and the number of times an address object is used in other settings.
`show config object address-object address`	Displays the address object settings you configured, such as the address object description, type, interface and IP address.

25.2.1.1 Address Object Command Examples

The following example creates IPv4 address objects.

```
usgflex200hp> edit running
usgflex200hp running config# object address-object address Example1 type host
192.168.1.1
usgflex200hp running config# object address-object address Example2 type cidr
192.168.1.0/24
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config object address-object address Example1
address Example1 type host 192.168.1.1
usgflex200hp running config# show config object address-object address Example2
address Example2 type cidr 192.168.1.0/24
```

25.2.2 Address Group Commands

This table lists the commands for address groups. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 97 Address Object Commands: Groups

COMMAND	DESCRIPTION
`object address-object group <group-name>`	Creates the specified address group and enters sub-command mode.
`description <description>`	Sets the description to the specified value. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are not allowed.
`address-list <address-object>`	Adds the specified address to the specified address group.
`group-list <group-name>`	Adds the specified address group to the address group you're configuring.
`show config object address-object group`	Displays the address group settings you configured, such as the address group name and the address included in the address group.
`show state object address-object group`	Displays the status of the address group settings, such as the address group name, the address included in the address group and he number of times an address group is used in other settings.

25.2.2.1 Address Group Command Examples

The following commands create address objects A0, A1, and A2 and add A1 and A2 to address group RD.

```
usgflex200hp> edit running
usgflex200hp running config# object address-object address A0 type host 192.168.1.1
usgflex200hp running config# object address-object address A1 type range
192.168.1.2-192.168.2.20
usgflex200hp running config# object address-object address A2 type cidr
192.168.3.0/24
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# object address-object group RD
usgflex200hp running group RD# address-list A0 address-list A1 address-list A2
usgflex200hp running group RD# commit
Configuration committed.
usgflex200hp running group RD# exit
usgflex200hp> show config object address-object group
group RD
    address-list A0
    address-list A1
    address-list A2
```

25.2.3 Geo IP

Use these commands to update the database of country-to-IP address mappings and manually configure custom country-to-IP address mappings in geographic address objects. You can then use geographic address objects in security policies to forward or deny traffic to whole countries or regions.

25.2.4 Geo IP Commands

Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 98 Geo IP Commands

COMMAND	DESCRIPTION
`geoip database-update auto {true| false}`	Enables the Zyxel Device to automatically check for the latest country-to-IP-address database version on myZyxel.com and allows it to be automatically updated when there is newer version available.
`geoip database-update weekly {mon| tue| wed| thu| fri| sat| sun}`	Specifies the weekly day the Zyxel Device should check for the latest country-to-IP-address database version on myZyxel.com if automatic checking is enabled.
`geoip database-update time`	Specifies the time the Zyxel Device should check for the latest country-to-IP-address database version on myZyxel.com if automatic checking is enabled.
`geoip customize rule <`*`rule-name`*`> ip-type {host `*`IP`*`| range `*`IP-range`*`| cidr `*`cidr`*`} cc-type {continent `*`continent`*`| country `*`country`*`}`	Creates or edits a Geo IP rule using the specified parameters. • IP: Enter an IPv4 address. • IP Range: Enter an IPv4 address range. • CIDR: Enter an IPv4 subnet in CIDR format. For example, 192.168.1.0/32. • Country/Continent: Enter a country or continent code to maps it to the IP address you specified.
`show config geoip database-update {auto | weekly | time}`	Displays if the Zyxel Device is allowed to automatically update to the latest country-to-IP-address database available.
`show config geoip customize rule`	Displays the Geo IP rule settings.

25.2.5 Geo IP Command Examples

The following shows Geo IP command examples.

```
usgflex200hp> edit running
usgflex200hp running config# geoip database-update auto true weekly fri time 22
usgflex200hp running config# geoip customize rule Exmaple1 ip-type host 1.1.1.1
cc-type country AM
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config geoip database-update
database-update auto true weekly fri time 22
usgflex200hp running config# show config geoip customize rule
rule Test cc-type country ZW ip-type host 1.1.1.1
rule Exmaple1 cc-type country AM ip-type host 1.1.1.1
```

CHAPTER 26 Services

26.1 Services Overview

Use service objects to define TCP applications, UDP applications, and ICMP messages that you refer to in features such security policies. You can also create service groups to refer to multiple service objects in other features such as policy routes.

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

26.2 Services Commands Input Values

The following table describes the values required for many service object and service group commands. Other values are discussed with the corresponding commands.

Table 99 Service Command Input Values

LABEL	DESCRIPTION
group-name	The name of the service group. This value is case-sensitive. You may use 1-30 single-byte characters, including 0-9a-zA-Z!"#$%'()+,-/;:=?@_, but the first character cannot be a number. &.<>{|}[\]‘^are not allowed.
object-name	The name of the service. This value is case-sensitive. You may use 1-30 single-byte characters, including 0-9a-zA-Z!"#$%'()+,-/;:=?@_, but the first character cannot be a number. &.<>{|}[\]‘^are not allowed.

26.2.1 Service Object Commands

The first table lists the commands for service objects. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 100 Service Object Commands

COMMAND	DESCRIPTION
`object service-object service <`*`object-name`*`> description <`*`description`*`>`	Enters the description used to refer to the service. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are not allowed.
`object service-object service <object-name> type {tcp| udp} {<`*`1...65535`*`>| <`*`1...65535`*`>-<`*`1...65535`*`>}`	Creates the specified TCP service or UDP service using the specified parameters.

Table 100 Service Object Commands

COMMAND	DESCRIPTION
`object service-object service <object-name> type icmp <icmp-value>`	Creates the specified ICMP message using the specified parameters. `icmp-value`: <0..255> | echo-reply |router-solicitation | time exceeded | parameter problem | timestamp request | timestamp reply | destination unreachable | redirect | echo | router advertisement | any
`object service-object service <object-name> type icmp6 <icmp6-value>`	Creates the specified ICMPv6 message using the specified parameters. `icmp6-value`: <0..255> | destination unreachable | echo request | echo reply | router solicitation | router advertisement | neighbor solicitation | neighbor advertisement | redirect message | packet too big | time exceeded | time exceeded | parameter problem | any
`object service-object service <object-name> type protocol <1...255>`	Creates the specified user-defined service using the specified parameters.
`show config object service-object service`	Displays the service object settings you configured.
`show state object service-object service`	Displays the status of service objects, such as the number of times a service object is used in other settings.

26.2.1.1 Service Object Command Examples

The following commands create four services and displays them.

```
usgflex200hp> edit running
usgflex200hp running config# object service-object service TELNET type tcp
23
usgflex200hp running config# object service-object service FTP type tcp 20-
21
usgflex200hp running config# object service-object service RIP type icmp
any    0      3      5      8      9      10     11     12     13     14
usgflex200hp running config# object service-object service RIP type icmp 5
usgflex200hp running config# object service-object service MULTICAST type
protocol 2
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config object service-object service
TELNET
service TELNET type tcp 23
usgflex200hp running config# show config object service-object service FTP
service FTP type tcp 20-21
usgflex200hp running config# show config object service-object service RIP
service RIP type icmp 5
usgflex200hp running config# show config object service-object service
MULTICAST
service MULTICAST type protocol 2
```

26.2.2 Service Group Commands

The first table lists the commands for service groups. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 101 Service Group Commands

COMMAND	DESCRIPTION
`object service-object group <group-name>`	Creates or edits the specified service group and enters sub-command mode.
`service-list <object-name>`	Adds the specified service to the specified service group.
`group-list <group-name>`	Adds the specified service group to the service group you're configuring.
`description <description>`	Enters the description used to refer to the service.You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are not allowed.
`show config object service-object group`	Displays the service group settings you configured.
`show state object service-object group`	Displays the status of service groups, such as the number of times a service object is used in other settings.

26.2.2.1 Service Group Command Examples

The following commands create service ICMP_ECHO, create service group SG1, and add ICMP_ECHO to SG1.

```
usgflex200hp> edit running
usgflex200hp running config# object service-object group ICMP_ECHO
usgflex200hp running group ICMP_ECHO# commit
Configuration committed.
usgflex200hp running group ICMP_ECHO# exit
usgflex200hp> edit running
usgflex200hp running config# object service-object group SG1
usgflex200hp running group SG1# commit
Configuration committed.
usgflex200hp running group SG1# exit
usgflex200hp> edit running
usgflex200hp running config# object service-object group ICMP_ECHO group-
list SG1
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config object service-object group
ICMP_ECHO
group ICMP_ECHO
    group-list SG1
```

CHAPTER 27 Schedules

27.1 Schedule Overview

The Zyxel Device supports two types of schedules: one-time and recurring. One-time schedules are effective only once, while recurring schedules usually repeat.

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

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.

27.2 Schedule Commands Summary

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

Table 102 Input Values for Schedule Commands

LABEL	DESCRIPTION
object-name	The name of the schedule. You may use 2-30 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
group-name	The name of the schedule group. You may use 2-30 alphanumeric characters underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
hh:mm	24-hour time, hours and minutes; <0..23>:<0..59>.

27.2.1 Schedule Commands

The following table lists the schedule commands. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 103 Schedule Commands

COMMAND	DESCRIPTION
`object schedule-object schedule <object-name> description <description>`	Enters the description used to refer to the schedule. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/ :=?;!*#@$_%-" Spaces are not allowed.
`object schedule-object schedule <object-name> type one-time <yyyy-mm-ddThh:mm>~<yyyy-mm-ddThh:mm>`	Creates or updates a one-time schedule.
`object schedule-object schedule <object-name> type recurring <mon| tue| wed| thu| fri| sat| sun Thh:mm>~<mon| tue| wed| thu| fri| sat| sun Thh:mm>`	Creates or updates a recurring schedule.
`show config object schedule-object schedule`	Displays the schedule settings.
`show state object schedule-object schedule`	Displays the status of the schedule, such as the number of times a schedule is used in other settings.

27.2.2 Schedule Command Examples

The following commands create recurring schedule Schedule1 and one-time schedule Schedule2.

```
usgflex200hp running config# exit
usgflex200hp> edit running
usgflex200hp running config# object schedule-object schedule Schedule1 type
recurring monT08:00~wedT08:00
usgflex200hp running config# object schedule-object schedule Schedule2 type
one-time 2022-11-04T08:00~2022-11-04T15:00
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config object schedule-object schedule
schedule Config1 type one-time 2000-08-10T10:00~2000-08-10T12:00
schedule Schedule1 type recurring monT08:00~wedT08:00
schedule Schedule2 type one-time 2022-11-04T08:00~2022-11-04T15:00
```

27.2.3 Schedule Group Commands

The following table lists the schedule group commands. Use schedule groups when you want to apply several schedules to a rule, such as a security policy.

Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 104 Schedule Group Commands

COMMAND	DESCRIPTION
`object schedule-object group <group-name> description <description>`	Enters a description of the schedule group.You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Space are allowed.
`object schedule-object group <group-name> schedule-list <object-name>`	Adds the specified schedule to the specified schedule group.
`object schedule-object group <group-name> group-list <group-name>`	Adds the specified schedule group to the schedule group you're configuring.
`show config object schedule-object group`	Displays the schedule group settings.
`show state object schedule-object group`	Displays the status of the schedule group, such as the number of times a schedule group is used in other settings.

27.2.4 Schedule Group Command Examples

The following commands create schedule group Group1 and Group2, then add Group 2 to Group1.

```
usgflex200hp> edit running
usgflex200hp running config# show config object schedule-object schedule
schedule Config1 type one-time 2000-08-10T10:00~2000-08-10T12:00
schedule Schedule1 type recurring monT08:00~wedT08:00
schedule Schedule2 type one-time 2022-11-04T08:00~2022-11-04T15:00
usgflex200hp running config# object schedule-object group Group1 schedule-
list Schedule1
usgflex200hp running config# object schedule-object group Group2 schedule-
list Schedule2
usgflex200hp running config# object schedule-object group Group1 group-list
Group2
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config object schedule-object group
group Group1
    schedule-list Schedule1
    group-list Group2
    ..
group Group2
    schedule-list Schedule2
```

CHAPTER 28
AAA Server

28.1 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 AAA servers the Zyxel Device supports.

- Local user database

  The Zyxel Device uses the built-in local user database to authenticate administrative users logging into the Zyxel Device's web configurator or network access users logging into the network through the Zyxel Device. You can also use the local user database to authenticate VPN users.
- Directory Service (LDAP/AD)

  LDAP (Lightweight Directory Access Protocol)/AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.
- RADIUS

  RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

28.2 Authentication Server Command Summary

This section describes the commands for authentication server settings.

28.2.1 AD Server Group Commands

The following table lists the commands you use to configure a group of AD servers

Table 105 AD Server Group Commands

COMMAND	DESCRIPTION
aaa group server ad *<profile-name>*	Sets a descriptive name for identification purposes. It must begin with a letter and may use up to 31 single-byte characters, including 0-9a-zA-Z_-. Spaces are not allowed.
aaa group server ad *<profile-name>* description *<description>*	Enter the description of each server. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are not allowed.

Table 105 AD Server Group Commands (continued)

COMMAND	DESCRIPTION
aaa group server ad <*profile-name*> port <*port*>	Sets the AD port number. Enter a number between 1 and 65535. The default is 389.
aaa group server ad <*profile-name*> ssl {true| false}	Enables the Zyxel Device to establish a secure connection to the AD server. The `false` command disables this feature.
aaa group server ad <*profile-name*> case-sensitive {true| false}	Enables this to have the server checks the case of the usernames. The `false` command disables this feature.
aaa group server ad <*profile-name*> group-attribute <*group-identifier*>	Enter the name of the attribute that the Zyxel Device is to check to determine to which group a user belongs.
aaa group server ad <*profile-name*> password-shadow <*password*>	Sets the bind password. You can use 4-63 single-byte characters, including 0-9a-zA-Z_(){}<>^`+/:!*#@&=$\?.~%,|;-'". This password will be encrypted automatically. When you use the `show config aaa group server ad` command, the encrypted password displays.
aaa group server ad <*profile-name*> cn-identifier <*uid*>	Sets the type of identifier the users are to use to log in. The default is sAMAccountName.
aaa group server ad <*profile-name*> alternative-cn-identifier <*uid*>	Enter a second type of identifier that the users can use to log in if there is one.
aaa group server ad <*profile-name*> search-time-limit <*1...300*>	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The default value is five.
aaa group server ad <*profile-name*> host <*ad-server*>	Sets the AD server address. Enter the IP address (in dotted decimal notation) or the domain name.
aaa group server ad <*profile-name*> domain-name <*domain-name*>	Sets the domain name to which AD server belongs. The Zyxel Device uses this to access the AD server.
aaa group server ad <*profile-name*> username <*user-name*>	Sets the user name that the Zyxel Device uses to access the AD server.
show config aaa group server ad	Displays the AD server profiles settings.
show state aaa group server ad	Displays the status of the AD server profile settings, such as the number of times an AD server profile is used in other settings.
show aaa ad-domain-auth-status	Displays the authentication status of the AD domain.
cmd aaa join-ad-domain	Adds the Zyxel Device to the currently configured AD domain. Note: The Zyxel Device can only join one AD domain at a time. Adding a new AD domain will replace existing domain associations. Note: Ensure that the Domain Zone Forwarder configuration is correct before joining a domain.
cmd aaa leave-ad-domain	Removes the Zyxel Device from the AD server domain.
aaa join-ad-domain ad-profile <*profile-name*>	Adds the Zyxel Device to a specific AD domain. Enter the profile name of the AD domain you want to join. You can only use this command when your user type is admin.

Table 105 AD Server Group Commands (continued)

COMMAND	DESCRIPTION
aaa join-ad-domain ad-netbios-name <*netbios-name*>	Sets the NetBIOS domain name of the AD domain for the Zyxel Device to join. You can only use this command when your user type is admin, but it is required by the AD server.
aaa join-ad-domain ad-admin-name <*user-name*>	Sets the user name for the Zyxel Device to join the AD domain. You can use 1-20 single-byte characters, including 0-9a-zA-Z_(){}<>^`+/:!*#@&=$\?.~%,|;-'". You can only use this command when your user type is admin.
aaa join-ad-domain ad-admin-password-shadow <*password*>	Sets the password associated with the user name. You can use 4-63 single-byte characters, including 0-9a-zA-Z_(){}<>^`+/:!*#@&=$\?.~%,|;-'". This password will be encrypted automatically. When you use the show config aaa join-ad-domain command, the encrypted password displays. You can only use this command when your user type is admin.

28.2.2 LDAP Server Group Commands

The following table lists the commands you use to configure a group of LDAP servers.

Table 106 LDAP Server Group Commands

COMMAND	DESCRIPTION
aaa group server ldap <*profile-name*> description <*description*>	Enters the description of each server. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are not allowed.
aaa group server ldap <*profile-name*> basedn <*basedn*>	Sets a base distinguished name (DN) for the default LDAP server. A base DN identifies a LDAP directory.
aaa group server ad <*profile-name*> port <*port*>	Sets the LDAP port number. Enter a number between 1 and 65535. The default is 389.
aaa group server ldap <*profile-name*> ssl {true| false}	Enables the Zyxel Device to establish a secure connection to the LDAP server. The false command disables this feature.
aaa group server ldap <*profile-name*> case-sensitive {true| false}	Enables this to have the server checks the case of the usernames. The false command disables this feature.
aaa group server ldap <*profile-name*> group-attribute <*group-identifier*>	Enters the name of the attribute that the Zyxel Device is to check to determine to which group a user belongs.
aaa group server ldap <*profile-name*> binddn <*binddn*>	Sets the DN of the user the Zyxel Device uses to log into the default LDAP server.
aaa group server ldap <*profile-name*> password-shadow <*password*>	Sets the bind password. You can use 4-63 single-byte characters, including 0-9a-zA-Z_(){}<>^`+/:!*#@&=$\?.~%,|;-'". This password will be encrypted automatically. When you use the show config aaa group server ldap command, the encrypted password displays.
aaa group server ldap <*profile-name*> cn-identifier <*uid*>	Sets the unique common name (cn) to identify a record.
aaa group server ldap <*profile-name*> alternative-cn-identifier <*uid*>	Enters a second type of identifier that the users can use to log in if there is one.

Table 106 LDAP Server Group Commands (continued)

COMMAND	DESCRIPTION
aaa group server ldap <*profile-name*> search-time-limit <*1...300*>	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The default value is five.
aaa group server ldap <*profile-name*> host <*ldap-server*>	Sets the LDAP server address. Enter the IP address (in dotted decimal notation) or the domain name.
show config aaa group server ldap	Displays the LDAP server profiles settings
show state aaa group server ldap	Displays the status of the LDAP server profile settings, such as the number of times a LDAP server profile is used in other settings.

28.2.3 RADIUS Server Group Commands

The following table lists the commands you use to configure a group of RADIUS servers.

Table 107 RADIUS Server Group Commands

COMMAND	DESCRIPTION
aaa group server radius <*profile-name*> description <*description*>	Sets the description of each server. You can use 1-61 single-byte characters, including 0-9a-zA-Z'()+,/:=?;!*#@$_%-" Spaces are not allowed.
aaa group server radius <*profile-name*> key-shadow <*secret*>	Sets a password (up to 63 alphanumeric characters) as the key to be shared between the external authentication server and the Zyxel Device.
aaa group server radius <*profile-name*> timeout <*1...300*>	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The default value is five.
aaa group server radius <*profile-name*> group-attribute <*group-identifier*>	Sets the name and number of the attribute that the Zyxel Device is to check to determine to which group a user belongs.
aaa group server radius <*profile-name*> case-sensitive {true| false}	Lets the server check the case of the usernames. The false command disables this feature.
aaa group server radius <*profile-name*> host <*radius-server*>	Sets the RADIUS server address. Enter the IP address (in dotted decimal notation) or the domain name.
aaa group server radius <*profile-name*> acct-secret <*secret*>	Sets a password (up to 63 alphanumeric characters) as the key to be shared between the RADIUS accounting server and the Zyxel Device. This key is not sent over the network. This key must be the same on the external authentication server and the Zyxel Device.

Table 107 RADIUS Server Group Commands (continued)

COMMAND	DESCRIPTION
aaa group server radius <*profile-name*> acct-retry-count <*0...10*>	Specifies the number of times the Zyxel Device should reattempt to use the primary RADIUS server before attempting to use the secondary RADIUS server. This also sets how many times the Zyxel Device will attempt to use the secondary RADIUS server. The default value is 3. For example, you set this value to 5. If the Zyxel Device does not get a response from the primary RADIUS server, it tries again up to five times. If there is no response, the Zyxel Device tries the secondary RADIUS server up to five times. If there is also no response from the secondary RADIUS server, the Zyxel Device stops attempting to authenticate the subscriber. The subscriber will see a message that says the RADIUS server was not found.
aaa group server radius <*profile-name*> acct-interim {true| false}	Enables to have the Zyxel Device send subscriber status updates to the RADIUS server at the interval you specify.
aaa group server radius <*profile-name*> acct-interim-interval <*1...1440*>	Specifies the time interval in minutes for how often the Zyxel Device is to send a subscriber status update to the RADIUS server.
aaa group server radius <*profile-name*> nas-ip <*ipv4*>	Sets the IPv4 address of the NAS (Network Access Server). The default IP is 127.0.0.1.
aaa group server radius <*profile-name*> nas-id <*id*>	Specifies the NAS (Network Access Serve) identifier attribute.
show config aaa group server radius	Displays the RADIUS server profiles settings
show state aaa group server radius	Displays the status of the RADIUS server profile settings, such as the number of times a RADIUS server profile is used in other settings.

28.2.4 AAA Group Server Command Examples

The following example shows you how to:

- Set the server host to 172.21.10.100 and authentication port to 1800.
- Set the secret key and timeout period of a RADIUS server group to “876543210” and 80 seconds.

```
usgflex200hp> edit running
usgflex200hp running config# aaa group server radius Profile1 key-shadow
876543210
usgflex200hp running config#! aaa group server radius Profile1 timeout 80
usgflex200hp running config#! aaa group server radius Profile1 host
172.21.10.100 auth-port 1800
usgflex200hp running config# commit
Configuration committed.
```

CHAPTER 29
Authentication Objects

29.1 Admin Two-Factor Authentication

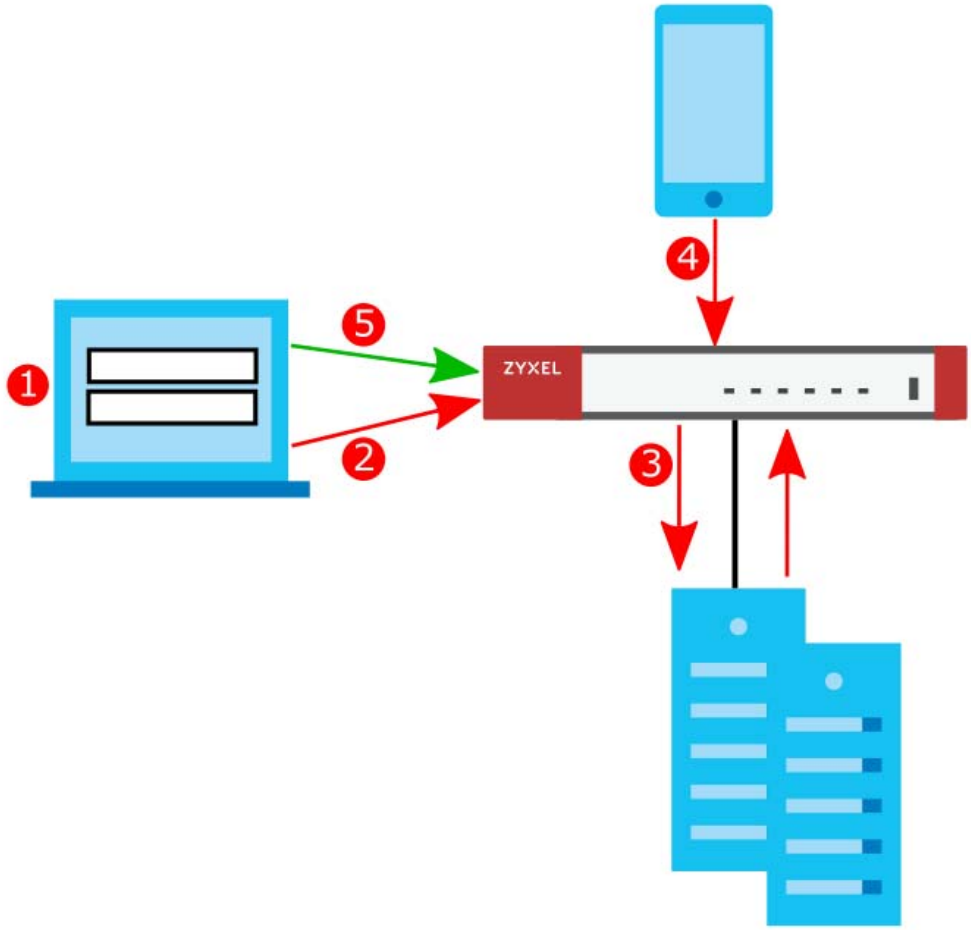
Two-factor authentication adds an extra layer of security for users logging into the Zyxel Device. When two-factor authentication is enabled, a user has to first enter their username and password, and then enter a one-time password when logging in.

You can enable two-factor authentication for administrators who are logging into the Web Configurator or CLI to configure the Zyxel Device.

29.1.1 Two-Factor Authentication with Google Authenticator

This section introduces how Google Authenticator two-factor authentication works.

Figure 46 Google Authenticator Two-Factor Authentication



Admin Access (Web Configurator, SSH)

The following steps explain the procedure when an admin logs into the Zyxel Device.

1. An admin connects to the Zyxel Device through the Web Configurator or SSH.
2. The Zyxel Device requests the admin's username and password.
3. The Zyxel Device authenticates the admin's username and password using a local Zyxel Device database. If this authentication is successful, the Zyxel Device requests the admin's Google Authenticator code.
4. The admin enters the code displayed in the Google Authenticator app.
5. If the Google Authenticator code is correct, the admin can log into the Zyxel Device.

29.2 Two-Factor Authentication Admin Commands

Use the following commands to configure whether **Web** or **SSH** require two-factor authentication for the admin user.

Table 108 Two-Factor Authentication Admin Access Commands

COMMAND	DESCRIPTION
two-factor-auth admin-access enabled {true| false}	True requires two-factor authentication to access a secured network behind the Zyxel Device via the Web Configurator or SSH as an admin. The false command disables two-factor authentication for admin access.
two-factor-auth admin-access user-list user <*username*>	Adds the specified admin user accounts to the two-factor authentication user list to require two-factor authentication when they log in.
two-factor-auth admin-access valid-time <*1...5*>	Sets the maximum time (1-5 minutes) that the admin must enter the code displayed in the Google Authenticator app in order to get authorization for logins via the Web Configurator or SSH.
two-factor-auth admin-access service {web| ssh}	Sets which services require two-factor authentication for the admin.
cmd two-factor-auth google-auth user <*username*> verify-code <*verification-code*>	Verifies whether the code currently displayed in the Google Authenticator app is correct or not to confirm the admin account is binded to the correct Google Authenticator account. The Zyxel Device also creates a temporary secret key file if one does not already exist.
cmd two-factor-auth google-auth user <*username*> backup-code create	Generates new Google Authenticator backup codes. All previously generated backup codes become invalid. You can use Google Authenticator backup codes to log into the Zyxel Device if you are unable to access the Google Authenticator app.
cmd two-factor-auth google-auth user <*username*> revoke	Unbinds the specified admin account in the Google Authenticator app.
show two-factor-auth user <*username*> qrcode	Displays the Google Authenticator QR code for this account. You can link this user account with Google Authenticator by pressing **Enter Provided Key** in the Google Authenticator app.
show two-factor-auth user <username> backup-code	Displays the Google Authenticator backup codes for this user account. You can use Google Authenticator backup codes to log into the Zyxel Device if you are unable to access the Google Authenticator app.
show config two-factor-auth admin-access	Displays the two-factor authentication settings.
show state two-factor-auth admin-access	Displays the two-factor authentication settings and hits.

29.2.1 Admin Access Two-Factor Command Examples

The following example shows how to set up two-factor authentication for an admin.

29.2.1.1 Admin Access Two-Factor Command Example: Email

Follow the steps below to enable two-factor authentication for a Zyxel Device account. The example uses the parameters below.

Table 109 Admin Account Example

USER NAME	PASSWORD	USER TYPE
Mary	1234	admin

Table 110 Two-Factor Authentication Settings Example

AUTHENTICATION METHOD	VALID TIME
Google Authenticator	5 minutes

1 Create an admin account using the parameters given above.

```
usgflex200hp> edit running
usgflex200hp running config# object user-object admin Mary role admin
usgflex200hp running config# object user-object admin Mary password
Enter value for password>
Confirm value for password>
usgflex200hp running config# commit
Configuration committed.
```

2 Enable two-factor authentication for the admin account **Mary**.

```
usgflex200hp running config# two-factor-auth admin-access user-list user Mary
```

3 Configure the two-factor authentication settings using the parameters given above.

```
usgflex200hp running config# two-factor-auth admin-access enabled true
usgflex200hp running config# two-factor-auth admin-access valid-time 5
```

4 Save the current configuration to the Zyxel Device.

```
usgflex200hp running config# commit
Configuration committed.
```

5 Link the account **Mary** with your Google Authenticator account by pressing **Enter Provided Key** in the **Google Authenticator** app.

```
usgflex200hp# cmd two-factor-auth google-auth user Mary verify-code xxxxxx
```

29.3 Two-Factor Authentication VPN Access Commands

Use the following commands to configure whether local users authenticated on the Zyxel Device require two-factor authentication for IPSec / SSL VPN tunnel remote access.

Table 111 Two-Factor Authentication VPN Access Commands

COMMAND	DESCRIPTION
two-factor-auth vpn-access enabled {true | false}	True requires two-factor authentication to remotely access an IPSec / SSL VPN tunnel for local users authenticated on the Zyxel Device. The false command disables two-factor authentication for IPSec / SSL VPN tunnel remote access.
two-factor-auth vpn-access auth-link http-type {http | https}	Specifies whether the two-factor authentication link that the user receives should be http or https.
two-factor-auth vpn-access auth-link auth-interface <*interface*>	Specifies the interface on which to receive two-factor verification from the user.
two-factor-auth vpn-access auth-link auth-url {*domain name* | *ipv4 address* | *ipv6 address*}	Specifies the domain name or IPv4 address in the two-factor authentication link sent to the user. An IPv6 address is not yet supported.
two-factor-auth vpn-access auth-link port <*1...65535*>	Specifies the port to use for the two-factor authentication link sent to the user.
two-factor-auth vpn-access valid-time <*1...5*>	Sets the maximum time (1-5 minutes) that the remote user must enter the code displayed in the Google Authenticator app in order to get authorization for IPSec / SSL VPN tunnel remote access.
two-factor-auth vpn-access service {ike | sslvpn | service} enabled {true | false}	True requires two-factor authentication for IPSec / SSL VPN tunnel remote access for local users authenticated on the Zyxel Device using the selected service.
two-factor-auth vpn-access service {ike | sslvpn | service} valid-time <*1...5*>	Sets the maximum time (1-5 minutes) that the remote user must enter the code displayed in the Google Authenticator app in order to get authorization for IPSec / SSL VPN tunnel remote access.
cmd two-factor-auth google-auth user <*username*> verify-code <*verification-code*>	Verifies whether the code currently displayed in the Google Authenticator app is correct or not to confirm the admin account is binded to the correct Google Authenticator account using the selected service. The Zyxel Device also creates a temporary secret key file if one does not already exist.
cmd two-factor-auth google-auth user <*username*> backup-code create	Generates new Google Authenticator backup codes. All previously generated backup codes become invalid. You can use Google Authenticator backup codes to log into the Zyxel Device if you are unable to access the Google Authenticator app.
cmd two-factor-auth google-auth user <*username*> revoke	Unbinds the specified admin account in the Google Authenticator app.
show two-factor-auth google-auth user <*username*> qrcode	Displays the Google Authenticator QR code for this account. You can link this user account with Google Authenticator by pressing **Enter Provided Key** in the Google Authenticator app.
show two-factor-auth google-auth user <*username*> backup-code	Displays the Google Authenticator backup codes for this user account. You can use Google Authenticator backup codes to log into the Zyxel Device if you are unable to access the Google Authenticator app.

Table 111 Two-Factor Authentication VPN Access Commands (continued)

COMMAND	DESCRIPTION
show two-factor-auth google-auth qrcode backup-code	Displays the Google Authenticator backup codes for this Google Authenticator QR code. You can use Google Authenticator backup codes to log into the Zyxel Device if you are unable to access the Google Authenticator app.
show two-factor-auth google-auth backup-code qrcode	Displays the Google Authenticator QR code for this Google Authenticator backup code.
show config two-factor-auth vpn-access user-list	Displays configured local users that require two-factor authentication to remotely access an IPSec / SSL VPN tunnel.
show config two-factor-auth vpn-access enabled	Displays whether two-factor authentication to remotely access an IPSec / SSL VPN tunnel is configured.
show config two-factor-auth vpn-access valid-time	Displays the configured maximum time (1-5 minutes) that the remote user must enter the code displayed in the Google Authenticator app in order to get authorization to remotely access an IPSec / SSL VPN tunnel.
show state two-factor-auth vpn-access users	Displays the runtime status of local users that require two-factor authentication to remotely access an IPSec / SSL VPN tunnel.
show state two-factor-auth vpn-access enabled	Displays the runtime status of two-factor authentication to remotely access an IPSec / SSL VPN tunnel.
show state two-factor-auth vpn-access valid-time	Displays the runtime status of maximum time (1-5 minutes) that the remote user must enter the code displayed in the Google Authenticator app in order to get authorization to remotely access an IPSec / SSL VPN tunnel.

CHAPTER 30 Certificates

30.1 Certificates Overview

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

30.2 Certificates Commands Input Values

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

Table 112 Certificates Commands Input Values

LABEL	DESCRIPTION
certificate-name	The name of a certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
cn-ipv4-address	A common name IP version 4 address identifies the certificate's owner.
cn-fqdn	A common name domain name identifies the certificate's owner. The domain name is for identification purposes only and can be any string. The domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods.
cn-email	A common name e-mail address identifies the certificate's owner. The e-mail address is for identification purposes only and can be any string. The e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.
organizational-unit	Identifies the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, hyphen (-) and underscore (_).
organization	Identifies 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-code	A two-letter country code, which identifies the nation where the certificate owner is located. For example US, UK, ES, FR.

Table 112 Certificates Commands Input Values (continued)

LABEL	DESCRIPTION
key-type	Encryption algorithms: • **RSA**: Rivest, Shamir and Adleman public-key algorithm. • **DSA**: Digital Signature Algorithm public-key algorithm. • **ECDSA**: Elliptic Curve Digital Signature Algorithm. Signature hash algorithms: • SHA256 • SHA384 • SHA512 RSA and SHA256 are less secure but more compatible with different clients and applications. ECDSA and SHA512 are more secure but less compatible.
extend-key	Extended key usage: • **serverAuth**: Uses this to have the Zyxel Device generate and sore a request for server authentication certificate. • **clientAuth**: Uses this to have the Zyxel Device generate and store a request for client authentication certificate. • **ikeIntermediate**: Uses this to have the Zyxel Device generate and store a request for IKE intermediate authentication certificate.
key-length	Specifies the length of the key, in bits. Allowed values:. • ECDSA: 256, 384 • RSA/DSA: 512, 768, 1024, 1536, 2048, 4096 Typically, the longer the key, the more secure it is. A longer key also uses more PKI storage space. ECDSA keys are significant shorter than RSA and DSA keys, while offering equal or higher security.
city	Identifies the city or town in which the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore. You can add multiple words by enclosing them in double quotes, for example “New York”.
province	Identifies the state, province, or region in which the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore. You can add multiple words by enclosing them in double quotes, for example “New Mexico”.
valid-years	Sets how long the certificate is valid, in years. The value must be between 1 and 10. Note: Software such as web browsers might not trust a certificate that has a long lifetime.

30.3 Certificates Commands

The following table lists the commands that you can use to display and manage the Zyxel Device's summary list of certificates and certification requests. You can also create certificates or certification requests.

Table 113 Certificate Commands

COMMAND	DESCRIPTION
cmd certManager generate self-signed {name *certificate-name*| country *country-code*| state *province*| locality *city*| organization *organization*| organization-unit *organization-unit*| valid-years *1...10*} cn {fqdn *cn-fqdn*| ip *cn-ipv4-address*| email *cn-email*} key-type {ECDSA| RSA| DSA} key-len <*key-length*> extend-key {serverAuth| clientAuth| ikeIntermediate}	Creates a self-signed certificate. key-type: Sets the certificate's encryption algorithm and signature hash algorithm. extend-key: Adds extended use cases for the certificate. The choices are: • serverAuth: Has the Zyxel Device generate and store a request for server authentication certificate. • clientAuth: Has the Zyxel Device generate and store a request for client authentication certificate. • ikeIntermediate: Has the Zyxel Device generate and store a request for IKE Intermediate authentication certificate.
cmd certManager generate signing-request {name *certificate-name*| country *country-code*| state *province*| locality *city*| organization *organization*| organization-unit *organization-unit*} cn {fqdn *cn-fqdn*| ip *cn-ipv4-address*| email *cn-email*} key-type {ECDSA| RSA| DSA} key-len <*key-length*> extend-key {serverAuth| clientAuth| ikeIntermediate}	Generates a certificate request. key-type: Sets the certificate's encryption algorithm and signature hash algorithm. extend-key: Adds extended use cases for the certificate. The choices are: • serverAuth: Has the Zyxel Device generate and store a request for server authentication certificate. • clientAuth: Has the Zyxel Device generate and store a request for client authentication certificate. • ikeIntermediate: Has the Zyxel Device generate and store a request for IKE Intermediate authentication certificate.
cmd certManager delete {certificate| trusted-certificate} name <*certificate-name*>	Deletes the specified certificate. The Zyxel Device keeps all of your certificates unless your specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates.
show certManager {certificate| trusted-certificate} {certpath name *certificate-name*| name| raw name *certificate-name*| base64 name *certificate-name*| json name *certificate-name*}	Displays the certificate in the form you specified. For example, if you enter show certManager base64 name *certificate-name*, you will see the certificate you specified in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters and numerals to convert a binary certificate into a printable form.
show state certManager	Displays the certificate settings and the percentage of the Zyxel Device's PKI storage space that is currently in use.

30.4 Certificates Commands Examples

The following example creates a self-signed certificate with FQDN www.zyxel.com as the common name. It uses the RSA key type with SHA256.

```
usgflex200hp> edit running
usgflex200hp running config# cmd certManager generate self-signed name Example
valid-years 2 cn fqdn www.zyxel.com key-type RSA sha256 key-len 512
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show certManager certificate name Example
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            62:96:ad:db:72:08:ef:fc:de:e1:a2:07:5b:b5:ab:89:a7:84:e0:c7
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.zyxel.com
        Validity
            Not Before: Mar 16 08:58:53 2023 GMT
            Not After : Mar 15 08:58:53 2025 GMT
        Subject: CN = www.zyxel.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (512 bit)
                Modulus:
                    00:b1:05:73:43:83:cb:6e:66:88:c7:2d:83:08:eb:
                    86:35:fd:40:ee:49:01:44:e0:71:91:aa:91:e8:6d:
                    8d:95:0f:40:3d:0e:c7:47:5e:cd:62:85:44:9d:a7:
                    91:00:92:8c:85:cd:02:6d:2e:0a:df:77:b3:31:b1:
                    a1:65:24:36:93
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:1
            X509v3 Subject Key Identifier:
                E6:92:39:DA:71:8D:92:24:02:4E:BF:1B:BE:B4:90:A7:66:3D:16:D4
            X509v3 Key Usage: critical
               Digital Signature, Key Encipherment, Data Encipherment, Certificate
Sign
            X509v3 Subject Alternative Name:
                DNS:www.zyxel.com
    Signature Algorithm: sha256WithRSAEncryption
         6e:47:53:f0:f4:a6:cf:1f:97:39:3c:00:2e:c7:61:ff:6c:03:
         ec:d4:48:b2:4d:12:82:80:2e:c1:40:15:c6:de:da:6f:81:51:
         7e:a2:37:52:cc:21:d1:4c:49:54:b8:71:a7:85:4f:d3:c2:71:
         d6:f1:dc:76:7b:e4:ef:b1:61:f0
```

CHAPTER 31
System

31.1 System Overview

Use these commands to configure general Zyxel Device information, the system time and the console port connection speed for a terminal emulation program. They also allow you to configure DNS settings and determine which services/protocols can access which Zyxel Device zones (if any) from which computers.

31.2 Host Name Commands

The following table describes the commands available for the hostname. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 114 Host Name Commands

COMMAND	DESCRIPTION
`system hostname <hostname>`	Sets a descriptive name to identify your Zyxel Device. You can use up to 30 single-byte characters, dashes (-) and underscores (_). Spaces are not allowed.
`show state system hostname`	Displays the name to identify your Zyxel Device.
`show state system timezone-auto-sync`	Displays the Zyxel Device timezone settings.

31.3 Time and Date

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

31.3.1 Date/Time Commands

The following table describes the commands available for date and time setup.

Table 115 Date/Time General Commands

COMMAND	DESCRIPTION
`cmd datetime 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.
`system timezone-auto-sync {true| false}`	Allows the Zyxel Device to automatically update its time zone from the time server. The `false` command disables the Zyxel Device from automatically updating its time zone from the time server.
`system timezone <timezone>`	Sets the timezone of your location manually. This will set the time difference between your timezone and Greenwich Mean Time (GMT).
`show config system timezone-auto-sync`	Displays if the Zyxel Device is allowed to automatically update its time zone from the cloud server.
`show state system timzone`	Displays the Zyxel Device timezone.

31.3.2 NTP Service Commands

The following table describes the commands available for configuring the NTP service. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 116 NTP Service Commands

COMMAND	DESCRIPTION
`vrf main ntp enabled {true| false}`	Has the Zyxel Device get the time and date from the time server you set. Uses the `false` command to have the Zyxel Device use the time and date settings you configured manually.
`vrf main ntp ntp-source-address <IP address>`	Sets the IP address of the NTP time server for your Zyxel Device to get the time and date. Check that the IP address is available.

Table 116 NTP Service Commands

COMMAND	DESCRIPTION
vrf main ntp time-sources server {IP address| FQDN}{version <*version*>| <*association-type*> <*association-type*>| iburst {true|false}| prefer {true|false}| auth-key-id <id>}	Sets the IP address or Fully-Qualified Domain Name of your NTP time server. version: Enter the version of NTP to be used for time synchronization. association-type: Enter the desired association type between the NTP time server and your Zyxel Device. • PEER: Has both the NTP time server and the Zyxel Device provide time synchronization services to each other. • POOL: Has the ZD get the time and date from a pool of NTP servers determined by a DNS name. The ZD acts as an NTP client, and only gets the time from the NTP server. • SERVER: Has the ZD get the time and date from a single NTP server. The ZD acts as an NTP client, and only gets the time from the NTP server iburst: Has the Zyxel Device send multiple time queries at the beginning of the synchronization to obtain more accurate time information. prefer: Prioritizes synchronization with this time server, when the Zyxel Device synchronizes with multiple NTP servers. auth-key-id: Sets the authentication key ID for authenticating NTP messages between the Zyxel Device and the NTP time server.
vrf main ntp server-subnet <*priority*> {allow| deny}{CIDR subnet| all}	Sets the Zyxel Device as an NTP server and allows or blocks access to specific subnets, or to all subnets. priority: Enter the priority for this rule. The lower the number, the higher the priority. 1 is the highest. CIDR subnet: Enter IP subnet in CIDR format, i.e. 192.168.1.0/32 <W.X.Y.Z>/<1..32> all: Applies the allow or block rule to all subnets.
vrf main server-subnet	Sets the subnet of your NTP time server.
vrf main ntp auth-key	Sets the key used to authenticate between the Zyxel Device and the NTP time server.
show ntp clients	Displays the status of NTP clients synchronizing with the Zyxel Device.
cmd ntp update execute	Gets the time and date from the NTP time server you set.
cmd ntp update get-result	Displays if the Zyxel Device has successfully gotten the time and date from the NTP time server.

31.4 Device Insight Overview

Use Device Insight to collect status and basic information of the clients connected to the Zyxel Device internal interface or IPSec VPN. The clients shown may include clients connected to the Zyxel Device:

- Using wired connections.
- Through access points (APs) using wired connections.
- Through access points (APs) using WiFi connections.
- Through built-in access points using WiFi connections.
- Using SecuExtender (IPSec VPN clients).

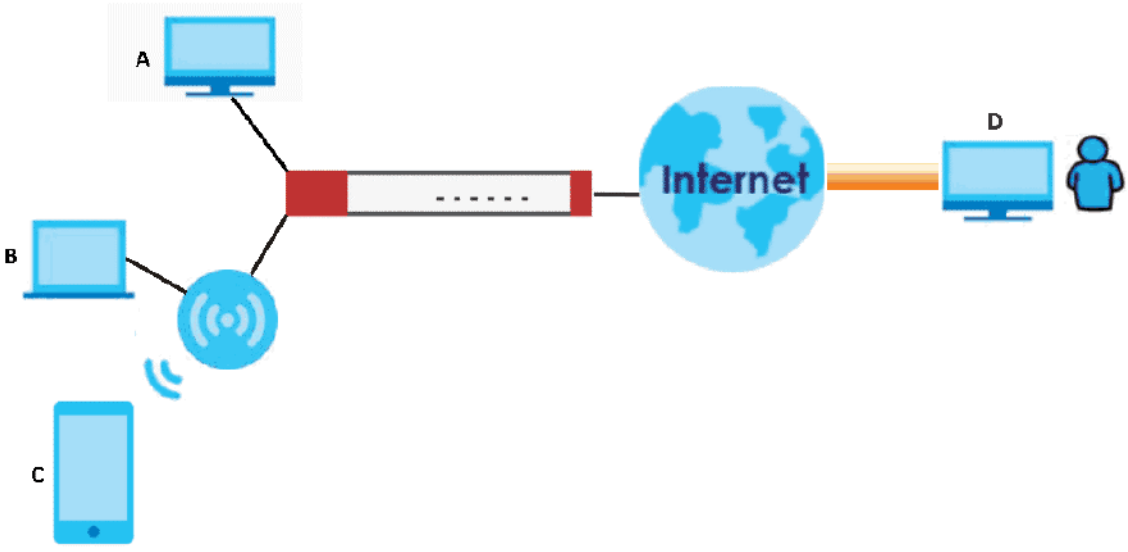
Device Insight collects client information including:

- Hostname
- IP address and MAC address
- Operating system
- Category, such as mobile phones or computers
- Connected interface

Note: To collect clients' information using Device Insight, the clients must be in the same IP subnet in the LAN/VLAN/DMZ networks behind the Zyxel Device. Information from clients that are in different IP subnets in the LAN/VLAN/DMZ networks might not be collected correctly as traffic must pass through another router or a layer-3 switch to the Zyxel Device.

In the graphic below, **A** is a client connected to the Zyxel Device using a wired connection. **B** is a client connected to the Zyxel Device through an AP using a wired connection. **C** is a client connected to the Zyxel Device through an AP using a WiFi connection. **D** is a client connected to the Zyxel Device through an IPSec VPN tunnel using SecuExtender.

Figure 47 Clients' Device Insight Example



31.4.1 Device Insight Commands

The following table describes the commands available for Device Insight. You must use the `edit running` commands to enter the configuration mode before you can use the configuration commands.

Table 117 Device Insight Commands

COMMAND	DESCRIPTION
`vrf main device-insight enabled {true| false}`	Enable Device Insight to collect status and basic information of the clients connected to the Zyxel Device internal interfaces or IPSec VPN.
`vrf main device-insight block-list enabled {true| false} mac <mac-address> logging {no| log| log-alert}`	Enable Device Insight block list to block a client device by the client device's MAC address. This also sets the Zyxel Device to generate a log, log and alert or neither (no) when the blocked client device tries to connect to the Zyxel Device.
`vrf main device-insight mac <mac-address> description <description>`	Creates an entry for the specified client device MAC address. This also sets a description for this entry. You can use up to 63 single-byte characters, including 0-9a-zA-Z\ \-'()+.,\ \/@_
`vrf main device-insight bypass-interface <interface>`	Sets an internal interface that will not be detected by Device Insight. Device Insight detects all clients connected to the Zyxel Device internal interfaces by default.
`cmd device-insight flush all`	Clears all clients status and information Device Insight collected.
`cmd device-insight remove <mac-address>`	Removes a client that's no longer connected to your network. For example, guest A visited your company over a month ago. Guest A used his cellphone to connect to your Zyxel Device networks. His cellphone was identified by Device Insight. Guest A has left for over a month and you're sure he will not return in the near future. You can remove his device using this command. Guest A's device will be identified again if he connects to your Zyxel Device networks in the future. Please note that clients that are blocked cannot be removed. Make sure to unblock clients before you remove them.
`cmd device-insight feedback mac <mac-address> category <category> os <operating-system> type <type>`	Specify a MAC address to report on the client that is wrongly identified regarding its category, operating system or type.

31.5 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.

31.5.1 Domain Zone Forwarder

A domain zone forwarder contains a DNS server's IP address. The Zyxel Device can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. A domain zone is a fully

qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

A name query begins at a client computer and is passed to a resolver, a DNS client service, for resolution. The Zyxel Device can be a DNS client service. The Zyxel Device can resolve a DNS query locally using cached Resource Records (RR) obtained from a previous query (and kept for a period of time). If the Zyxel Device does not have the requested information, it can forward the request to DNS servers. This is known as recursion.

The Zyxel Device can ask a DNS server to use recursion to resolve its DNS client requests. If recursion on the Zyxel Device or a DNS server is disabled, they cannot forward DNS requests for resolution.

A Domain Name Server (DNS) amplification attack is a kind of Distributed Denial of Service (DDoS) attack that uses publicly accessible open DNS servers to flood a victim with DNS response traffic. An open DNS server is a DNS server which is willing to resolve recursive DNS queries from anyone on the Internet.

In a DNS amplification attack, an attacker sends a DNS name lookup request to an open DNS server with the source address spoofed as the victim's address. When the DNS server sends the DNS record response, it is sent to the victim. Attackers can request as much information as possible to maximize the amplification effect.

31.5.2 DNS Commands

The following table describes the commands available for DNS. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 118 DNS Commands

COMMAND	DESCRIPTION
`vrf main dns proxy forward {local| dns-server` *`ip-address`*`}`	Sets a domain zone forwarder record that specifies a fully qualified domain name. You can also use a star (*) if all domain zones are served by the specified DNS server(s).
`vrf main dns zone <`*`domain`*`> ip <`*`ip-address`*`> ttl <`*`0...2147483647`*`>`	Sets how many seconds to keep the record of the mapping between a fully qualified domain name (FQDN) and an IP address.
`vrf main dns zone <`*`domain`*`> a-record`	Sets an A record that specifies the mapping of a fully qualified domain name (FQDN) to an IP address.
`vrf main dns zone <`*`domain`*`> cname-record`	A Canonical Name Record or CNAME record is a type of resource record in the Domain Name System (DNS) that specifies that the domain name is an alias of another, canonical domain name. Type a Fully-Qualified Domain Name (FQDN) of a server. Underscores are not allowed. Use "*." as a prefix in the FQDN for a wildcard domain name (for example, *.example.com).
`vrf main dns zone <`*`domain`*`> mx-record`	Sets a MX record that specifies a mail server that is responsible for handling the mail for a particular domain.

Table 118 DNS Commands (continued)

COMMAND	DESCRIPTION
vrf main dns security-options default recursion {true| false} additional-from-cache {true| false}	Selects to use the default security option. Enables recursion to allow the Zyxel Device to forward DNS client requests to DNS servers for resolution. This can apply to specific open DNS servers using the address objects in a customized rule. Enables additional info from cacher to allow the Zyxel Device to cacher Resource Records (RR) obtained from previous DNS queries.
vrf main dns security-options customize {recursion {true| false} additional-from cache {true| false} address-object-group <*CIDR*>	Configures and selects to use the customize security option. Enables recursion to allow the Zyxel Device to forward DNS client requests to DNS servers for resolution. This can apply to specific open DNS servers using the address objects in a customized rule. Enables additional info from cacher to allow the Zyxel Device to cacher Resource Records (RR) obtained from previous DNS queries. Sets the address object to apply it to the security option.
show config vrf main dns	Displays the DNS settings, such as the DNS server IP address and security options settings.
show state vrf main dns	Displays the DNS settings status, such as the DNS server IP address and if the proxy server is enabled.

31.5.3 DNS Command Examples

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

```
usgflex200hp> edit running
usgflex200hp running config# vrf main dns zone abc.com a-record 1 hostname www
210.17.2.13 ptr true
usgflex200hp running config# commit
Configuration committed.
```

This command displays security options configured for the customized and default rules.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main dns security-options customize recursion true
additional-from-cache true address-object-group 10.0.0.0/8 address-object-group
172.16.0.0/12 address-object-group 192.168.0.0/16
usgflex200hp running config# vrf main dns security-options default recursion true
additional-from-cache true
usgflex200hp running config# commit
Configuration committed.
usgflex200hp running config# show config vrf main dns security-options
security-options customize
    recursion true
    additional-from-cache true
    address-object-group 10.0.0.0/8
    address-object-group 172.16.0.0/12
    address-object-group 192.168.0.0/16
    ..
security-options default
    recursion true
    additional-from-cache true
```

31.6 Notification

The notification commands allow you to configure the Zyxel Device to send you event notifications by email.

You can also configure where to email the alerts when they're generated. Alerts are used for events that require more serious attention, such as system errors and attacks.

31.6.1 Mail Server and Alerts Commands

Use the commands listed below to configure the mail server and mail alerts settings.

Table 119 Mail Server and Alerts Commands

COMMAND	DESCRIPTION
`notification mail tls enabled {true| false}`	Sets the mail server to use or not use (`false` command) Transport Layer Security (TLS) for encrypted communications between the mail server and the Zyxel Device.
`notification mail tls start-tls {true| false}`	The mail server uses SSL or TLS for encrypted communications between the mail server and the Zyxel Device. This command turns off STARTTLS and uses the TLS protocol. The `false` command enables the default STARTTLS protocol (SSL) for encrypted communications between the mail server and the Zyxel Device.
`notification mail tls authenticate-server {true| false}`	Sets the Zyxel Device to authenticates the mail server in the TLS handshake or not (`false` command).
`notification mail server-address <server-address>`	Sets the SMTP mail server IP address or domain name.
`notification mail server-port <1...65535>`	Sets the SMTP port. The default value is 25.

Table 119 Mail Server and Alerts Commands

COMMAND	DESCRIPTION
notification mail smtp-authentication {true| false}	Enables SMTP authentication.
notification mail user <*username*> password <*password*>	Sets the username and password for SMTP authentication. You can use 4 to 63 single-byte characters for the password, including 0-9a-zA-Z'!@#$%^&*()_+={|}\:;"<>'/
notification mailalert <*profile-name*> enabled {true| false}	Sends log messages and alert to the email address you specify.
notification mailalert <*profile-name*> source {all| source-list *source*}	Specifies the types of alerts to be mailed when they're generated.
notification mailalert <*profile-name*> from <*email-address*>	Enters the email address from which the outgoing email is delivered. The address is used in replies.
notification mailalert <*profile-name*> send-alerts-to <*email-address*>	Enters the mail address to which alerts are delivered. You can configure up to 5 email addresses.
notification mailalert <*profile-name*> mail-subject <*subject*>	Sets the email subject.
show config notification mail	Displays mail server settings.
show config notification mailalert	Displays mail alert settings.
show notification status mail	Displays mail server settings.
show notification status mailalert	Displays all mail alert profiles settings.

31.7 Language Commands

Use the language command to set the language the web configurator is using. You must use the edit running command to enter the configuration mode before you can use the command.

Table 120 Command Summary: Language

COMMAND	DESCRIPTION
gui system language <*language*>	Specifies the language used in the web configurator screens.

31.8 ARP Commands

Use the ARP command to enable or disable ARP spoofing prevention.

ARP spoofing prevention verifies the ARP responses from client devices. If the IP and MAC addresses do not match the ARP table on the Zyxel Device, the Zyxel Device will refresh the ARP table to remove the falsified MAC mappings and create a log.

Table 121 Command Summary: ARP

COMMAND	DESCRIPTION
`system network-stack arp-seal enabled {true| false}`	Refreshes the ARP table to remove the falsified MAC mappings and creates a log on the Zyxel Device when there is an ARP message that fails the ARP verification.
`show state system network-stack arp-seal`	Displays if the ARP spoofing prevention feature is enabled.

CHAPTER 32 System Remote Management

32.1 Remote Management Overview

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

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

You may manage your Zyxel Device 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.

32.1.1 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 Zyxel Device will disconnect the session immediately.
3. There is a firewall rule that blocks it.

32.1.2 System Timeout

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

32.2 Common System Command Input Values

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

Table 122 Input Values for General System Commands

LABEL	DESCRIPTION
address_object	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
rule_number	The number of a service control rule. 1 - *X* where *X* is the highest number of rules the Zyxel Device model supports.
zone_object	The name of the zone. Ue up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.

32.3 HTTP/HTTPS Commands

The following table describes the commands available for HTTP/HTTPS. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 123 HTTP/HTTPS Commands

COMMAND	DESCRIPTION
`vrf main http-server server enabled {true| false}`	Enables HTTP access to the Zyxel Device web configurator. The `false` command disables HTTP access to the Zyxel Device web configurator.
`vrf main http-server server port <1...65535>`	Sets the HTTP service port number. The default port is 80.
`vrf main http-server server content-compression {true| false}`	Has the Zyxel Device compress data size before sending data to the clients.
`vrf main http-server server max-connection-per-ip <0...255>`	Sets the numbers of HTTP connections an IP address is allowed to access the Zyxel Device.
`vrf main http-server secure-server enabled {true| false}`	Enables HTTPS access to the Zyxel Device web configurator. The `false` command disables HTTPS access to the Zyxel Device web configurator.
`vrf main http-server secure-server customized exclude-protocol {TLSv1.3| TLSv1.2| TLSv1.1| TLSv1}`	Disables the specified TLS support in the HTTPS server.
`vrf main http-server secure-server customized exclude-ciphers {AES| CHACHA20| 3DES| DES| RC4}`	Has the Zyxel Device not use the specified encryption algorithm for the SSL in HTTPS connections.
`vrf main http-server secure-server port <1...65535>`	Sets the HTTPS service port number. The default port is 443.
`vrf main http-server secure-server force-https {true| false}`	Redirects all HTTP connection requests to a HTTPS URL. The `false` command disables forwarding HTTP connection requests to a HTTPS URL.

Table 123 HTTP/HTTPS Commands

COMMAND	DESCRIPTION
`vrf main http-server secure-server auth-client {true| false}`	Sets the client to authenticate itself to the HTTPS server. The `false` command sets the client not to authenticate itself to the HTTPS server.
`vrf main http-server secure-server certificate <certificate>`	Specifies a certificate used by the HTTPS server. The client will be required to send a certificate to create a secure connection with the Zyxel Device. Use up to 30 single-byte characters for the certificate name, including 0-9a-zA-Z;'~!@#$%^&()_+[]{}',.=-
`vrf main http-server secure-server compatibility {modern| intermediate| old}`	Sets the compatibility level of the HTTPS server. `modern`: This supports the least types of encryption algorithms. Select this to better protect your network. `old`: This supports the most types of encryption algorithms. Select this if your browser version is old.
`vrf main http-server security-options <security-options> {true| false}`	Sets the security methods for HTTP connections.
`vrf main http-server auth-server <1...2>`	Sets the web configurator login authentication using local account or external server according to the index order.
`show config vrf main http-server`	Displays the HTTP and HTTPS settings.
`show state vrf main http-server`	Displays the status of HTTP and HTTPS.

32.3.1 HTTP/HTTPS Command Examples

This following example shows how to:

- Set HTTPS certificate as a certificate named Test.
- Redirect all HTTP connection to use HTTPS connections.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main http-server secure-server certificate Test
usgflex200hp running config# vrf main http-server secure-server force-https true
usgflex200hp running config# commit
Configuration committed.
```

32.4 SSH

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

32.4.1 SSH Implementation on the Zyxel Device

Your Zyxel Device supports SSH using RSA authentication and the following encryption methods: AES, 3DES, Archfour, Blowfish. The SSH server is implemented on the Zyxel Device for remote management on port 22 (by default).

32.4.2 Requirements for Using SSH

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

32.4.3 SSH Commands

The following table describes the commands available for SSH. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 124 SSH Commands

COMMAND	DESCRIPTION
`vrf main ssh-server enabled {true| false}`	Allows access to the Zyxel Device using SSH connections
`vrf main ssh-server address <ip-address>`	Sets the IPv4 address or domain of an SSH client.
`vrf main ssh-server port <1...65535>`	Sets the SSH service port number. The default port is 22.
`vrf main ssh-server certificate <certificate>`	Specifies a certificate whose corresponding private key is to be used to identify the Zyxel Device for SSH connections.
`show config vrf main ssh-server`	Displays the SSH settings.
`show state vrf main ssh-server`	Displays: • If users are allowed to access the Zyxel Device using SSH connections • The SSH service port number • The IPv4 address or domain of the SSH clients.

32.5 FTP

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

32.5.1 FTP Commands

The following table describes the commands available for FTP. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 125 FTP Commands

COMMAND	DESCRIPTION
`vrf main ftp-server enabled {true| false}`	Allows access to the Zyxel Device using FTP connections.
`vrf main ftp-server port <1...65535>`	Sets the FTP service port number. The default port is 21.
`vrf main ftp-server tls-required {true| false}`	Allows FTP over TLS (Transport Layer Security) to encrypt communication. This implements TLS as a security mechanism to secure FTP clients and servers.
`vrf main ftp-server certficate <certificate>`	Specifies a certificate whose corresponding private key is to be used to identify the Zyxel Device for FTP connections.
`show config vrf main ftp-server`	Displays the FTP settings.
`show state vrf main ftp-server`	Displays: • If users are allowed to access the Zyxel Device using FTP connections • The FTP service port number • The IPv4 address or domain of the FTP clients.

32.6 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your Zyxel Device supports SNMP agent functionality, which allows a manager station to manage and monitor the Zyxel Device through the network. The Zyxel Device supports SNMP version one (SNMPv1) version two (SNMPv2c) and version 3 (SNMPv3).

SNMP v3 enhances security for SNMP management using authentication and encryption. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

32.6.1 Supported MIBs

The Zyxel Device supports MIB II that is defined in RFC-1213 and RFC-1215. The Zyxel Device also supports private MIBs (zywall.mib and zyxel-zywall-ZLD-Common.mib) to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the Zyxel Device's MIBs from www.zyxel.com.

32.6.2 SNMP Traps

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

Table 126 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 Zyxel Device is turned on or an agent restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.
vpnTunnelDisconnected	1.3.6.1.4.1.890.1.6.22.2.3	This trap is sent when an IPSec VPN tunnel is disconnected.
vpnTunnelName	1.3.6.1.4.1.890.1.6.22.2.2.1.1	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the disconnected tunnel's IPSec SA name.
vpnIKEName	1.3.6.1.4.1.890.1.6.22.2.2.1.2	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the disconnected tunnel's IKE SA name.
vpnTunnelSPI	1.3.6.1.4.1.890.1.6.22.2.2.1.3	This trap is sent along with the vpnTunnelDisconnected trap. This trap carries the security parameter index (SPI) of the disconnected VPN tunnel.

32.6.3 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 127 Command Summary: SNMP

COMMAND	DESCRIPTION
`vrf main snmp listen protocols <protocol> port <1...65535>`	Sets the SNMP listening port and protocol.
`vrf main snmp static-info location <location>`	Sets the geographic location (of up to 60 characters) for the Zyxel Device.
`vrf main snmp static-info contact <contact>`	Sets the contact information (of up to 60 characters) for the person in charge of the Zyxel Device.
`vrf main snmp static-info name <name>`	Specifies the username of a login account on the Zyxel Device.

CHAPTER 33
File Manager

33.1 Configuration Files Overview

When you apply a configuration file, the Zyxel Device uses the factory default settings for any features that the configuration file does not include.

You can edit configuration files in a text editor and upload them to the Zyxel Device. Configuration files use a .conf extension.

33.1.1 Zyxel Device Configuration File Details

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

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

33.1.2 Configuration File Flow at Restart

You can manually restart the Zyxel Device through a management interface or by physically turning the power off and back on.

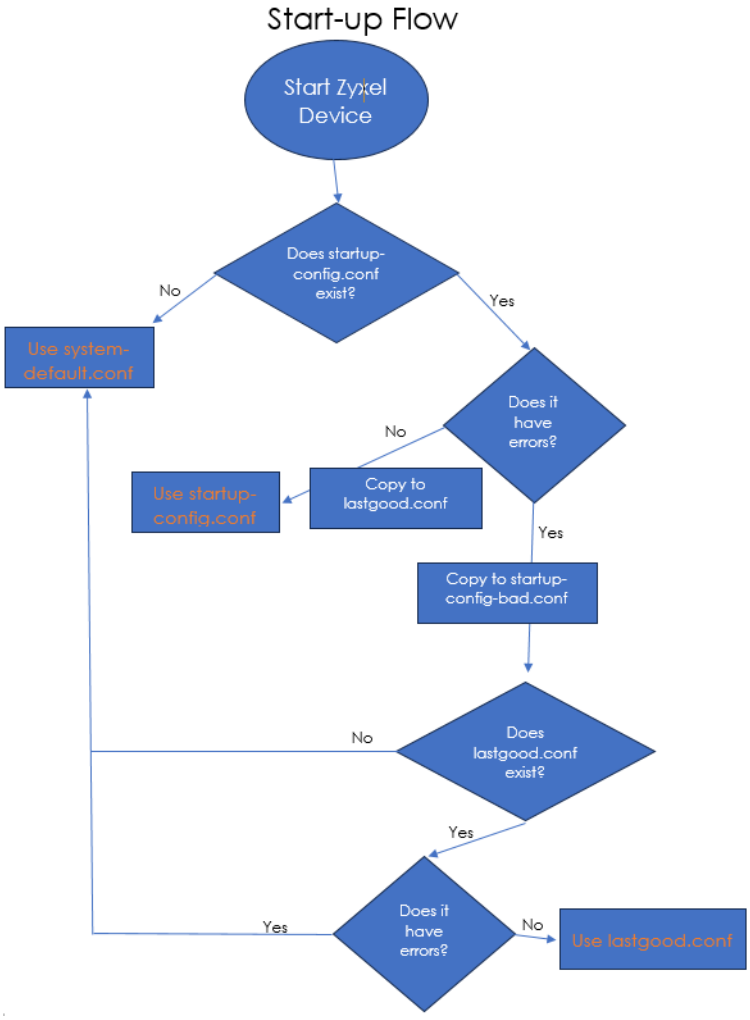
The Zyxel Device restarts automatically when you upload new firmware.

The Zyxel Device always checks for errors in any configuration file when rebooting. The Zyxel Device generates a log for any errors.

- If there is not a **startup-config.conf** when you restart the Zyxel Device, the Zyxel Device uses the **system-default.conf** configuration file with the Zyxel Device's default settings. The Zyxel Device will apply the **system-default.conf** when it boots without a **startup-config.conf**, even if you have a **lastgood.conf**.
- If there is a **startup-config.conf**, the Zyxel Device checks it for errors and applies it if there are no errors. The Zyxel Device also copies it to the **lastgood.conf** configuration file as a back up file.
- If there is an error in **startup-config.conf**, the Zyxel Device generates a log and copies **startup-config.conf** to **startup-config-bad.conf** and then tries the existing **lastgood.conf** configuration file.

- If there isn't a **lastgood.conf** configuration file or it also has an error, the Zyxel Device applies the **system-default.conf** configuration file.

Figure 48 Zyxel Device Start-up Flow



33.2 File Manager Commands Input Values

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

Table 128 File Manager Command Input Values

LABEL	DESCRIPTION
file-name	The name of a file. Use up to 76 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-) and must end with .conf.

33.3 File Manager Commands Summary

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

Table 129 File Manager Commands Summary

COMMAND	DESCRIPTION
`cmd config-copy from <file-name> to <file-name>`	Saves a duplicate of a file on the Zyxel Device from the source file name to the target file name. Specify the file name of the file that you want to copy and the file name to use for the duplicate. The file name uses up to 76 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-) and must end with .conf.
`cmd config-rename from <file-name> to <file-name>`	Changes the name of a file. Specify the file name of the file that you want to rename. The file name uses up to 76 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-) and must end with .conf.
`cmd config-delete <file-name>`	Removes a file. Specify the file name of the file that you want to delete. The file name uses up to 76 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-) and must end with .conf.
`cmd config-mail send-now <file-name>`	Has the Zyxel Device sends the specified configuration file to the configured email addresses. The file name uses up to 76 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-) and must end with .conf.
`cmd config-apply <file-name>`	Has the Zyxel Device use a specific configuration file. The file name uses up to 76 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-) and must end with .conf.
`cmd config-apply <file-name> option {dry-run| ignore-error}`	Has the Zyxel Device check or apply a specific configuration file to the Zyxel Device. The file name uses up to 76 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-) and must end with .conf. • `dry-run`: Check a specific configuration file without applying any changes to the Zyxel Device. • `ignore-error`: Apply a specific configuration file to the Zyxel Device even if errors occur. This allows the Zyxel Device to apply the correct parts of the configuration. This is not recommended.

33.4 File Manager Backup Commands Summary

The following table lists the commands that you can use to back up configuration files.

Table 130 File Manager Backup Commands Summary

COMMAND	DESCRIPTION
`configuration auto-backup enabled {true| false}`	Backs up the configuration file at a user defined schedule. Note: After the first backup, the back up only occurs if the configuration file is different from the previous backed up configuration file.
`configuration auto-backup schedule daily time <hh:mm>`	Has the Zyxel Device back up its configuration file once a day at the specified hour and minute.

Table 130 File Manager Backup Commands Summary (continued)

COMMAND	DESCRIPTION
`configuration auto-backup schedule weekly week-day <week-day> time <hh:mm>`	Has the Zyxel Device back up its configuration file once a week on the specified day, at the specified hour and minute.
`configuration auto-backup schedule monthly month-day <month-date> time <hh:mm>`	Has the Zyxel Device back up its configuration file once a month on the specified day, at the a specified hour and minute. Note: If the date you select is greater than the number of days in a month, the Zyxel Device automatically backs up its configuration file on the last day of the month. For example, if you select 31 and the month is February, the Zyxel Device backs up its configuration file on day 28 or 29.
`configuration auto-backup email subject <subject>`	Enter a email subject text with 1-60 characters. It may consist of letters, numbers, and the following special characters: '()+,./ :=?;!*#@$%-
`configuration auto-backup email recipient <email-address>`	Enter the receiving email address. You can send the configuration file to a maximum of five email addresses.
`configuration auto-backup email content <content>`	Enter the backup email body text using 1 to 251 single-byte characters, including 0-9a-zA-Z!"#$%&'()*+,-./:;<=>@[\]^_'{|} and spaces are allowed. ? is not allowed.
`cmd config-copy from {start| running} to usb`	Has the Zyxel Device save the starting or running configuration file to your USB stick in the modelname_dir/conf folder. The saved configuration file is displayed as startup-yyyy-mm-dd-hh-mm.conf or running yyyy-mm-dd-hh-mm.conf. • `start`: startup-config.conf • `running`: the running configuration file on your Zyxel Device You must choose FAT32 as the USB file system. If no USB stick is connected to your Zyxel Device, this command will fail.

33.5 Cloud Helper Commands

Cloud Helper lets you know if there is a later firmware available on the Cloud Helper server and lets you download it if there is.

Note: Go to myZyxel, create an account and register your Zyxel Device first. Then you will be able to get notifications on new firmware available when you log into the Zyxel Device web configurator.

Table 131 Cloud Helper Commands

COMMAND	DESCRIPTION
`cloud-helper firmware auto-update {true| false}`	Lets the Zyxel Device automatically check for and download new firmware at the time and day specified.
`cloud-helper firmware auto-reboot {true| false}`	Lets the Zyxel Device automatically reboot when new firmware is downloaded to the Zyxel Device.

Table 131 Cloud Helper Commands (continued)

COMMAND	DESCRIPTION
`cloud-helper firmware update-schedule daily <0...23>`	Has the Zyxel Device check for new firmware every day at the specified time. The time format is the 24 hour clock, so '0' means midnight, 01 means 1AM and so on. Set `cloud-helper firmware auto-reboot` to yes to have the Zyxel Device automatically restart when new firmware is downloaded to the Zyxel Device.
`cloud-helper firmware update-schedule weekly <week-day> time <0...23>`	Has the Zyxel Device check for new firmware once a week on the day and at the time specified. The time format is the 24 hour clock, so '0' means midnight, 01 means 1AM and so on. Set `cloud-helper firmware auto-reboot` to yes to have the Zyxel Device automatically restart when new firmware is downloaded to the Zyxel Device. If you configure both weekly and daily commands, then the command that takes effect is the last one configured.
`cmd cloud-helper get firmware <1..2>`	Downloads the latest firmware on the Cloud Helper server to the specified system space on the Zyxel Device.
`cmd cloud-helper pause-download firmware <1..2>`	Temporarily stops a firmware being downloaded to the specified system space on the Zyxel Device.
`cmd cloud-helper clean-download firmware <1..2>`	Stops and removes a firmware being downloaded to the Zyxel Device.
`show cloud-helper firmware download-status`	Displays the download status of the firmware that is downloaded to the Zyxel Device from the Cloud Helper server.

CHAPTER 34
Logs

34.1 Logs Overview

This chapter provides information about the Zyxel Device's logs. When the system log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

See the User's Guide for the maximum number of system log messages in the Zyxel Device.

34.2 Log Command Input Values

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

Table 132 Log Command Input Values

LABEL	DESCRIPTION
interface	The name of the interface. Ethernet interface: For some Zyxel Device models, use ge*x*, *x* = 1 - N, where N equals the highest numbered Ethernet interface for your Zyxel Device model. For othere Zyxel Device models, use a name such as wan1, wan2, opt, lan1, or dmz. Virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: ge*x*:*y*, *x* = 1 - N, *y* = 1 - 4 VLAN interface: vlan*x*, *x* = 0 - 4094 Bridge interface: br*x*, *x* = 0 - N, where N depends on the number of bridge interfaces your Zyxel Device model supports. Virtual interface on top of bridge interface: br*x*:*y*, *x* = the number of the bridge interface, *y* = 1 - 4 PPPoE interface: ppp*x*, *x* = 0 - N, where N depends on the number of PPPoE interfaces your Zyxel Device model supports.
source	The name of the category. The `all` category includes all messages in all categories.
protocol	The name of a protocol such as TCP, UDP, ICMP.

34.2.1 Log General Commands

This table lists the log general commands.

Table 133 Log General Commands

COMMAND	DESCRIPTION
`logging log-statistic enabled {true| false}`	Has the Zyxel Device count how many logs there are in different categories.
`show logging last-boot entries`	Displays the log entries saved before the Zyxel Device reboots.
`show logging status`	Displays the Zyxel Device log settings status.
`show logging _source mapping`	Displays the mapping between the log categories and the associated IDs.
`show logging log-statistics`	Displays the number of logs in different categories.

34.2.2 Log Entries Commands

This table lists the commands to look at log entries.

Table 134 Log Entries Commands

COMMAND	DESCRIPTION
`show logging entries {details idkey` *`id`*`| priority` *`priority`*`| source` *`source`*`| srcip` *`ipv4`*`| src-geoip` *`country`*`| sport` *`source-port`*`| dstip` *`ipv4`*`| dst-geoip` *`country`*`| dport` *`destination-port`*`| srciface` *`interface`*`| dstiface` *`interface`*`| protocol` *`protocol`*`| keyword` *`keyword`*`| line-range begin` *`number`* `end` *`number`*`}`	Displays the specified entries in the system log. 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.

34.2.3 System Log Commands

This table lists the commands for the system log settings.

Table 135 System Log Commands

COMMAND	DESCRIPTION
`logging system-log source {all| source-list` *`source`*`}`	Specifies what kind of information, if any, is logged in the system log for the specified category. Uses `all` to select all categories.
`logging system-log suppression enabled {true| false}`	Enable log consolidation in the system log.
`logging system-log suppression interval <`*`10...600`*`>`	Sets the log consolidation interval for the system log. The default value is 10.

34.2.3.1 System Log Command Examples

The following command displays the current status of the system log.

```
usgflex200hp> edit running
usgflex200hp running config# show logging status system-log
show-zylog-status-system-log
    ok
        events-logged 13
        suppression-active false
        suppression-interval 10
        source-list default
            level all
            ..
        source-list content-filter
            level normal
            ..
        source-list forward-web-sites
            level normal
            ..
        source-list blocked-web-sites
            level normal
            ..
        source-list warning-web-sites
            level normal
            ..
        source-list user
            level normal
            ..
        source-list pki
            level normal
```

34.2.4 Debug Log Commands

This table lists the commands for the debug log settings.

Table 136 Debug Log Commands

COMMAND	DESCRIPTION
show logging debug entries {details idkey *id*| priority *priority*| source *source*| srcip *ipv4*| dstip *ipv4*| srciface *interface*| dstiface *interface*| protocol *protocol*| keyword *keyword*| line-range begin *number* end *number*}	Displays the specified entries in the debug log.

34.2.5 Remote Syslog Server Commands

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

Table 137 Remote Syslog Server Commands

COMMAND	DESCRIPTION
`logging syslog remote-server <1...4> source {all| source-list source}`	Specifies what kind of information, if any, is logged in the specified syslog remote server for the specified category. Uses `all` to select all categories.
`logging syslog remote-server <1...4> enabled {true| false}`	Enable the specified remote server.
`logging syslog remote-server <1...4> server-address <ipv4-address>`	Sets the IPv4 address of the specified remote server.
`logging syslog remote-server <1...4> server-port <port-number>`	Sets the port of the specified remote server.
`logging syslog remote-server <1...4> log-format {cef| syslog}`	Sets the format of the log information. `cef`: Common Event Format, syslog-compatible format. `syslog`: syslog format.
`logging syslog remote-server <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.

34.3 USB Storage Commands

The Zyxel Device can use a connected USB device to store system logs, diagnostic information and firmware.

Note: The USB device must allow writing (it cannot be read-only) and use the FAT16, FAT32, EXT2, or EXT3 file system.

For Zyxel Devices that have more than one USB port, these commands only apply to the first USB storage device that is attached to the Zyxel Device.

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

You must use `edit running` to be in configuration mode to use the indented commands shown below.

Table 138 USB Storage Commands

COMMAND	DESCRIPTION
`logging usb-storage enabled {true| false}`	Enable or disable the connected USB storage service.
`logging usb-storage keep-duration enabled {true| false} duration <1...365>`	Sets a number of days that the Zyxel Device keeps the log.

Table 138 USB Storage Commands (continued)

COMMAND	DESCRIPTION
`logging usb-storage source {all| source-list source}`	Sets the logging settings for the specified category for the connected USB storage device. Uses `all` to select all categories.
`logging usb-storage flush-threshold <1...100>`	Sets the maximum number of logs the Zyxel Device can store. When the number of logs exceeds the threshold you set, new logs will be stored in the connected USB storage device.

34.4 Email Daily Report Commands

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

Table 139 Input Values for Email Daily Report Commands

LABEL	DESCRIPTION
email-address	An e-mail address. You can use up to 80 alphanumeric characters, underscores (_), periods (.), or dashes (-), and you must use the @ character.

Use these commands to have the Zyxel Device send various statistics reports every day. You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 140 Email Daily Report Commands

COMMAND	DESCRIPTION
`system daily-report enabled {true| false}`	Enable to send reports by email every day.
`system daily-report report-items {cpu-usage| mem-usage| port-usage| session-usage| interface-usage| app-patrol| content-filter| anti-malware| ip-reputation| ips| dhcp} {true| false}`	Specifies the information to include in the report.
`system daily-report mail to <email-address>`	Sets the email address (or addresses) to which the outgoing email is delivered.
`system daily-report mail from <email-address>`	Sets the email address from which the outgoing email is sent.
`system daily-report mail subject append-system-name {true| false}`	Determines whether the system name will be appended to the subject of the report e-mails.
`system daily-report mail subject append-date-time {true| false}`	Determines whether the sending date and time will be appended at subject of the report e-mails.
`system daily-report mail subject set <mail-subject>`	Sets the subject line for outgoing email from the Zyxel Device. You can use up to 60 single-byte characters, including 0-9a-zA-Z'()+,./:=?;!#@$_%-
`system daily-report schedule <hh:mm>`	Sets the time of the day the report is emailed.
`system daily-report reset-counter {true| false}`	Determines whether or not to start all of the report statistics data counters over at zero every 24 hours.
`cmd system daily-report send now`	Sends the daily e-mail report immediately.

34.4.1 Email Daily Report Example

This example sets the following about sending a daily report e-mail:

- Enables reporting.
- Sets the subject of the report e-mails to test.
- Stops the system name from being appended to the mail subject.
- Appends the date and time to the mail subject.
- Sets the sender as my-email@example.com.
- Sets the sender as receiver@example.com.
- Sets the Zyxel Device to send the report at 1:57 PM.
- Has the Zyxel Device not reset the counters after sending the report.
- Has the report include CPU, memory, and session usage.

```
usgflex200hp> edit running
usgflex200hp running config# system daily-report enabled true
usgflex200hp running config# system daily-report mail subject set test
usgflex200hp running config# system daily-report mail subject append-system-name
false
usgflex200hp running config# system daily-report mail subject append-date-time true
usgflex200hp running config# system daily-report mail from my-email@example.com
usgflex200hp running config# system daily-report mail to receiver@example.com
usgflex200hp running config# system daily-report schedule 13:57
usgflex200hp running config# system daily-report reset-counter false
usgflex200hp running config# system daily-report report-items cpu-usage true
usgflex200hp running config# system daily-report report-items mem-usage true
usgflex200hp running config# system daily-report report-items session-usage true
usgflex200hp running config# commit
Configuration committed.
```

CHAPTER 35
SecuReporter

35.1 SecuReporter Overview

SecuReporter is a security analytics portal accessible, that collects and analyzes logs from SecuReporter-licensed Zyxel Devices in order to identify anomalies, alert on potential internal / external threats, and report on network usage.

You need to buy a SecuReporter license for your Zyxel Device and register it at myZyxel using your myZyxel account. The SecuReporter license must be activated on each Zyxel Device. The Zyxel Device must be able to communicate with the myZyxel server.

35.1.1 SecuReporter Commands

SecuReporter stores logs in a temporary file for uploading to the SecuReporter portal for security analysis. How often to upload is determined by the upload interval (default every 600 seconds) or upload file size (default is when the temporary log file reaches 10 MB). More frequent uploads provides better real-time log analysis, but uses more network bandwidth and Zyxel Device CPU processing power.

You must use the `edit running` command to enter the configuration mode before you can use these commands.

Table 141 SecuReporter Commands

COMMAND	DESCRIPTION
`vrf main secureporter enabled {true| false}`	Sends security-related logs to the SecuReporter portal. Uses `false` to disable SecuReporter logging. SecuReporter must be enabled to collect and analyze logs from this Zyxel Device. • You must read and accept the General Data Protection Regulation (GDPR) privacy policy by enabling SecuReporter in the Web Configurator before you can enable it by using the CLI. • SecuReporter is enabled by default if you have activated a SecuReporter Standard license, • SecuReporter is disabled by default if you have a SecuReporter Trial license. • You cannot enable SecuReporter if you do not have a SecuReporter license.
`vrf main secureporter upload-filesize <1...10>`	A temporary log file is uploaded to the SecuReporter security analytics portal when it meets the size set here (in megabytes) or the interval defined in the following field. 10 MB is the default. Set it to a smaller number for more frequent uploads.
`vrf main secureporter upload-interval <60...600>`	A temporary log file is uploaded to the SecuReporter security analytics portal at the interval defined here or when it meets the size set in the previous field. 600 seconds is the default. Set it to a smaller number for more frequent uploads.

Table 141 SecuReporter Commands (continued)

COMMAND	DESCRIPTION
vrf main secureporter app-patrol enabled {true| false}	The true command will have the Zyxel Device send application patrol logs to SecuReporter for analysis and trend spotting.
vrf main secureporter anti-malware enabled {true| false}	The true command will have the Zyxel Device send anti-malware logs to SecuReporter for analysis and trend spotting.
vrf main secureporter threat-protection enabled {true| false}	The true command will have the Zyxel Device send IPS and DoS prevention logs to SecuReporter for analysis and trend spotting.
vrf main secureporter content-filter enabled {true| false}	The true command will have the Zyxel Device send content filtering logs to SecuReporter for analysis and trend spotting.
vrf main secureporter reputation-filter enabled {true| false}	The true command will have the Zyxel Device send IP reputation and URL Threat filter logs to SecuReporter for analysis and trend spotting.
vrf main secureporter traffic-log enabled {true| false}	The true command will have the Zyxel Device send traffic logs to SecuReporter for analysis and trend spotting.
vrf main secureporter interface-statistics enabled {true| false}	The true command will have the Zyxel Device send logs of interface statistics to SecuReporter for analysis and trend spotting.
vrf main secureporter app-statistics enabled {true| false}	The true command will have the Zyxel Device send app traffic logs to SecuReporter for analysis and trend spotting.
vrf main secureporter sandboxing enabled {true| false}	The true command will have the Zyxel Device send sandbox traffic logs to SecuReporter for analysis and trend spotting.
vrf main secureporter ike enabled {true| false}	The true command will have the Zyxel Device send VPN logs to SecuReporter for analysis and trend spotting.
cmd securpt-claim-device device-name <*name*> organization <*organization-name*> organization_id <*organization-id*> gdpr {none| partial| fully}	Enter the name of the Zyxel Device. Add it to an existing organization by entering the organization name and ID. Enter the name of the Zyxel Device. Add it to a new organization by entering a name for the organization you want to create. none: Has your personal data, such as user names, MAC addresses, email addresses and host names to be identifiable in downloaded logs. partial: Has your personal data, such as user names, MAC addresses, email addresses and host names to be replaced with artificial identifiers in downloaded logs. fully: Has your personal data, such as user names, MAC addresses, email addresses and host names to be replaced with anonymized information in downloaded logs.
show securpt-claim-status	Displays: • If the Zyxel Device is claimed by an organization. • The names and IDs of all organizations.

35.1.2 SecuReporter Commands Example

The following example shows SecuReporter configurations. Set the upload file size to 5 MB. Set the upload interval to 100 seconds.

```
usgflex200hp> edit running
usgflex200hp running config# vrf main secureporter enabled true
usgflex200hp running config# vrf main secureporter upload-filesize 5
usgflex200hp running config# vrf main secureporter upload-interval 100
usgflex200hp running config# vrf main secureporter anti-malware enabled true
usgflex200hp running config# vrf main secureporter threat-protection enabled true
usgflex200hp running config# commit
Configuration committed.
```

CHAPTER 36
Diagnostics and Maintenance Tools

36.1 Diagnostics Overview

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

36.1.1 Diagnostic Commands

The following table lists the commands that you can use to have the Zyxel Device collect diagnostics information. Use the `edit running` command to enter the configuration mode to be able to use these commands.

Table 142 Diagnostic Commands

COMMAND	DESCRIPTION
`diagnostics diaginfo ac categories` *<1...2047>*	Collects information on the AP controller (the Zyxel Device) according to the category you set. For example, set the category number to 2 to collect AAA related information. Set the category number to 128 to collect VPN related information. Uses this command with the assistantance of the customer support.
`diagnostics diaginfo copy-to-usb {true| false}`	Has the Zyxel Device create a copy of the diagnostic file to a connected USB storage device.
`cmd diagnostics diaginfo collect ac {start| stop}`	Starts collecting or stops collecting information on the AP controller (the Zyxel Device).
`show diagnostics mem status all`	Displays the current DRAM memory utilization percentage for each application used on the Zyxel Device and each application's running time in hours - minutes - seconds.
`show diagnostics cpu average`	Displays the current percentage usage of each CPU in the Zyxel Device as a percentage of total processing power and the current CPU utilization percentage for each application used on the Zyxel Device.
`show diagnostics cpu status average`	Displays the Zyxel Device average CPU utilization.
`show diagnostics cpu all`	Displays all the Zyxel Device CPU utilization.
`show diagnostics diaginfo collect status`	Displays whether the Zyxel Device is collecting diagnostics information (Standby) or the Zyxel Device has finished collecting diagnostics information (Busy on device).

36.1.2 Diagnosis Commands Example

The following example shows you how to check all the Zyxel Device CPU utilization.

```
usgflex200hp running config# show diagnostics cpu all
cpu-all-diagnostics
    ok
        cpu_core_list 0
            cpu-utilization "11.9 %"
            cpu-utilization-for-1-min "12.3 %"
            cpu-utilization-for-5-min "12.8 %"
            ..
        cpu_core_list 1
            cpu-utilization "5.9 %"
            cpu-utilization-for-1-min "8.7 %"
            cpu-utilization-for-5-min "7.5 %"
            ..
        cpu_core_list 2
            cpu-utilization "100.0 %"
            cpu-utilization-for-1-min "100.0 %"
            cpu-utilization-for-5-min "100.0 %"
            ..
        cpu_core_list 3
            cpu-utilization "100.0 %"
            cpu-utilization-for-1-min "100.0 %"
            cpu-utilization-for-5-min "100.0 %"
            ..
```

36.2 Maintenance Tools Overview

Use the maintenance tool commands to check traffic going through the Zyxel Device and troubleshoot network problems.

36.2.1 Packet Capture Commands

Use the packet capture commands to capture network traffic going through the Zyxel Device's interfaces. Studying these packet captures may help you identify network problems.

Table 143 Packet Capture Commands

COMMAND	DESCRIPTION
`cmd diagnostics packet-capture enabled {true| false}`	Enable packet capture on the Zyxel Device.
`cmd diagnostics packet-capture config ftp {server` *`ip-address`*`| port` *`port-number`*`| username` *`name`*`| password` *`password`*`}`	Sets the FTP server for which to capture packets.
`cmd diagnostics packet-capture config ip-version {ip| ip6| any}`	Sets whether to capture IPv4 or IPv6 traffic. any means to capture packets for all types of traffic.

Table 143 Packet Capture Commands (continued)

COMMAND	DESCRIPTION
cmd diagnostics packet-capture config proto-type {icmp| icmp6| igmp| igrp| plm| ah| esp| vrrp| udp| tcp| any}	Sets the protocol of traffic for which to capture packets. any means to capture packets for all types of traffic.
cmd diagnostics packet-capture config host-ip {*ip-address*| any}	Sets a host IP address for which to capture packets. any means to capture packets for all hosts.
cmd diagnostics packet-capture config host-object <*profile-name*>	Sets a host IP address object for which to capture packets.
cmd diagnostics packet-capture config host-port <*0...65535*>	If you set the IP type to any, tcp, or udp using the proto-type command, you can specify the port number of traffic to capture.
cmd diagnostics packet-capture config files-size <*1...1000000000*>	Specifies a maximum size limit in megabytes for the total combined size of all the capture files on the ZyWALL, including any existing capture files and any new capture files you generate. The Zyxel Device stops the capture and generates the capture file when either the file reaches this size or the time period specified (using the duration command above) expires.
cmd diagnostics packet-capture config split-size <*1...2048*>	Specifies a maximum size limit in megabytes for individual packet capture files. After a packet capture file reaches this size, the Zyxel Device starts another packet capture file.
cmd diagnostics packet-capture config ring-buffer {true| false}	Enable or disable the ring buffer used as a temporary storage.
cmd diagnostics packet-capture config storage {internal| usbstorage| ftpserver}	Has the Zyxel Device only store packet capture entries on the Zyxel Device (internal) or on a USB storage or on a FTP server connected to the Zyxel Device.
cmd diagnostics packet-capture config duration <*0...300*>	Sets a time limit in seconds for the capture. The Zyxel Device stops the capture and generates the capture file when either this period of time has passed or the file reaches the size specified using the files-size command. 0 means there is no time limit.
cmd diagnostics packet-capture config file-suffix <*profile-name*>	Specifies text to add to the end of the file name (before the dot and filename extension) to help you identify the packet capture files. Modifying the file suffix also avoids making new capture files that overwrite existing files of the same name. The file name format is “interface name-file suffix.cap”, for example “vlan2-packet-capture.cap”.
cmd diagnostics packet-capture config snaplen <*0...1514*>	Specifies the maximum number of bytes to capture per packet. The Zyxel Device automatically truncates packets that exceed this size. As a result, when you view the packet capture files in a packet analyzer, the actual size of the packets may be larger than the size of captured packets.
cmd diagnostics packet-capture config iface {add| del} <*interface-name*>	Adds or deletes an interface or a virtual interface for which to capture packets to the capture interfaces list.
show diagnostics packet-capture config	Displays the packet capture settings.
show diagnostics packet-capture status	Displays whether the packet capture is ongoing.

36.2.2 Trace Route Commands

Use the trace route commands to identify where packets are dropped for troubleshooting.

Table 144 Trace Route Commands

COMMAND	DESCRIPTION
cmd diagnostics traceroute stop {true| false}	Stops tracing the route to the specified host name or IP address.
cmd diagnostics traceroute Extension-Option <*extended-option*>	Enter the extended option if you want to use an extended trace route command. *extended-option*: Use 1-256 single-byte characters, spaces, or '()+,/:=?;!*#@$_%.- characters.
cmd diagnostics traceroute ip ipv4-or-domainname <*ipv4*| *hostname*>	Displays the route taken by packets to the specified destination. Sets the source address or host name to specify interface IPv4 address or host name. Use Ctrl+C to return to the prompt.
cmd diagnostics traceroute ip ipv6-or-domainname <*ipv6*| *hostname*>	Displays the route taken by packets to the specified destination. Sets the source address or host name to specify interface IPv6 address or host name. Use Ctrl+C to return to the prompt.
cmd diagnostics traceroute interface <*interface*>	Displays the route packets take to an IPv4 network host. Specifies a network interface to obtain the source IP address for outgoing probe packets.
show diagnostics traceroute status	Displays whether the trace route is ongoing.

36.2.3 Ping Commands

Use the commands listed below to ping a specified IP address.

Table 145 Ping Commands

COMMAND	DESCRIPTION
cmd diagnostics ping stop {true| false}	Stops pinging the specified host name or IP address.
cmd diagnostics ping Extension-Option <*extended-option*>	Enter the extended option if you want to use an extended ping command. *extended-option*: Use 1-256 single-byte characters, spaces, or '()+,/:=?;!*#@$_%.- characters.
cmd diagnostics ping ip ipv4-or-domainname <*ipv4*| *hostname*>	Sends an ICMP ECHO_REQUEST to test the reachability of a host on an IPv4 network and to measure the round-trip time for a message sent from the originating host to the destination computer. Sets the source address or host name to specified interface IPv4 address.
cmd diagnostics ping ip ipv6-or-domainname <*ipv6*| *hostname*>	Sends an ICMP ECHO_REQUEST to test the reachability of a host on an IPv6 network and to measure the round-trip time for a message sent from the originating host to the destination computer. Sets the source address or host name to specified interface IPv6 address when pinging IPv6 link-local address this option is required.
show diagnostics ping status	Displays whether the testing of the reachability of a host is ongoing.

36.2.4 NSLOOKUP Commands

Use the NSLOOKUP commands to perform name server lookup for querying the Domain Name System (DNS) to get the domain name or IP address mapping.

Table 146 NSLOOKUP Commands

COMMAND	DESCRIPTION
`cmd diagnostics nslookup Query-Server <ip-address>`	Enter the IP address of a server to which the Zyxel Device sends queries for NSLOOKUP.
`cmd diagnostics nslookup Extension-Option <extended-option>`	Enter the extended option if you want to use an extended NSLOOKUP command. *extended-option*: Use 1-256 single-byte characters, spaces, or '()+,/:=?;!*#@$_%.- characters.
`cmd diagnostics nslookup domain-name-or-ip {domain-name domain-name| ipv4 ipv4| ipv6 ipv6}`	Performs name server lookup for querying a DNS server to get the domain name or IPv4/IPv6 address mapping.

CHAPTER 37
Shutdown/Reboot

Use these commands to turn off or restart the Zyxel Device. Use copy running startup to save your current configurations as the startup configurations before you reboot or shutdown the Zyxel Device. The Zyxel Device uses the startup configurations the next time you turn on the Zyxel Device.

Note: You cannot shut down or reboot the Zyxel Device if you did not save your current configurations as the startup configurations. Use the force command to shut down or reboot the Zyxel Device without saving the current configurations as the startup configurations. The configurations you made using the CLI will be lost.

Table 147 Shutdown/Reboot Commands

COMMAND	DESCRIPTION
cmd reboot {force| delay| cancel}	force: Reboots the Zyxel Device immediately without turning the power off. Your current configurations are not saved. Make sure to back up your current configurations before rebooting the Zyxel Device. delay: Sets the number of seconds the Zyxel Device waits before rebooting. The default value is 3. cancel: Stops the Zyxel Device from rebooting.
cmd poweroff {force| delay| cancel}	Wait for the **PWR/SYS** LED to turn off before you remove the Zyxel Device power cable. force: Turns off the Zyxel Device immediately. Your current configurations are not saved. Make sure to back up your current configurations before turning off the Zyxel Device. delay: Sets the number of seconds the Zyxel Device waits before turning off. The default value is 3. cancel: Stops the Zyxel Device from turning off.

List of Commands (Alphabetical)

This section lists the commands and sub-commands in alphabetical order. Commands and subcommands appear at the same level.