NETGEAR®

ProSAFE Dual WAN Gigabit Firewall with SSL & IPsec VPN

Model FVS336Gv2

CLI Reference Manual



March 2014
202-11378-01

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

After installing your device, locate the serial number on the label of your product and use it to register your product at *https://my.netgear.com*. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website. For product updates and web support, visit *http://support.netgear.com*.

Phone (US & Canada only): 1-888-NETGEAR.

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/general/contact/default.aspx*.

Compliance

For regulatory compliance information, visit *http://www.netgear.com/about/regulatory*.

See the regulatory compliance document before connecting the power supply.

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice.
© NETGEAR, Inc. All rights reserved.

Revision History

Publication Part Number	Publish Date	Comments
202-11378-01	March 2014	First publication

Contents

Chapter 1 Introduction

Command Syntax and Conventions 7
Command Conventions 7
Description of a Command 8
Common Parameters 9
Four Categories of Commands 9
Configuration Commands: Four Main Modes 10
Configuration Commands: Save Commands 13
Commands That Require Saving 13
Commands That Do Not Require Saving 13
Global Commands 14
Examples of Three Basic Types of Commands 14
Command Autocompletion and Command Abbreviation 15
Access the CLI 16

Chapter 2 Overview of the Configuration Commands

Network Settings Configuration Commands 18
Security Settings Configuration Commands 21
System Administrative and Monitoring Settings Configuration Commands . . 25
VPN Settings Configuration Commands 26

Chapter 3 Net Mode Configuration Commands

General WAN Commands 30
IPv4 WAN Commands 34
IPv6 WAN Commands 50
IPv6 Tunnel Commands 54
Dynamic DNS Command 57
IPv4 LAN Commands 59
IPv6 LAN Commands 70
IPv4 DMZ Setup Command 81
IPv6 DMZ Setup Commands 83
WAN QoS Commands 90
IPv4 Routing Commands 103
IPv6 Routing Commands 107

Chapter 4 Security Mode Configuration Commands

Security Services Commands 111
Security Schedules Command 120

IPv4 Add Firewall Rule and Edit Firewall Rule Commands 122
IPv4 General Firewall Commands 164
IPv6 Firewall Commands 165
Attack Check and IGMP Passthrough Commands 172
Session Limit, Time-Out, and Advanced Commands 177
Address Filter and IP/MAC Binding Commands 181
Port Triggering Commands 185
UPnP Command 188
Bandwidth Profile Commands 189
Content Filtering Commands 192

Chapter 5 System Mode Configuration Commands

Remote Management Commands 199
SNMP Commands 203
Time Zone Command 208
WAN Traffic Meter Command 213
Firewall Logs and Email Alerts Commands 216
System Reboot Command 223

Chapter 6 VPN Mode Configuration Commands

IPSec VPN Wizard Command 225
IPSec IKE Policy Commands 228
IPSec VPN Policy Commands 234
IPSec VPN Mode Config Commands 246
SSL VPN Wizard Command 249
SSL VPN Portal Layout Commands 254
SSL VPN Authentication Domain Commands 257
SSL VPN Authentication Group Commands 261
SSL VPN User Commands 262
SSL VPN Port Forwarding Commands 268
SSL VPN Client and Client Route Commands 271
SSL VPN Resource Commands 275
SSL VPN Policy Commands 278
RADIUS Server Command 285
PPTP Server Command 287
L2TP Server Command 288

Chapter 7 Overview of the Show Commands

Network Settings Show Commands 291
Security Settings Show Commands 293
Administrative and Monitoring Settings Show Commands 294
VPN Settings Show Commands 295

Chapter 8 Show Commands

Network Settings Show Commands 298
WAN IPv4 and WAN IPv6 Show Commands 298

IPv6 Mode, IPv6 Tunnel, and SIIT Show Commands 302
LAN DHCP Show Commands. 303
Dynamic DNS Show Command 304
IPv4 LAN Show Commands. 305
IPv6 LAN Show Commands. 308
DMZ Show Commands. 310
Routing Show Commands 312
Network Statistics Show Command. 313
Security Settings Show Commands 313
Services Show Commands. 314
Schedules Show Command 315
Firewall Rules Show Commands 315
Attack Checks and IGMP Show Commands 317
Session Limits Show Commands. 319
Advanced Firewall Show Command 319
Address Filter Show Commands 320
Port Triggering Show Commands. 321
UPnP Show Commands 322
Bandwidth Profiles Show Command 322
Content Filtering Show Commands 323
Administrative and Monitoring Settings Show Commands. 324
Remote Management Show Command 325
SNMP Show Commands. 325
Time Show Command. 327
Firmware Version Show Command. 327
Status Show Command 327
WAN Traffic Meter Show Command 330
Logging Configuration Show Commands 331
Logs Show Commands 333
Reboot Show Command. 334
VPN Settings Show Commands. 334
IPSec VPN Show Commands 334
SSL VPN Show Commands. 336
SSL VPN User Show Commands 339
RADIUS Server Show Command. 342
PPTP Server Show Commands 342
L2TP Server Show Commands 343

Chapter 9 Utility Commands

Overview Util Commands. 345
Firmware Backup, Restore, and Upgrade Commands 345
Diagnostic Commands 347

Command List

1 Introduction

This document describes the command-line interface (CLI) for the NETGEAR® ProSAFE® Dual WAN Gigabit Firewall with SSL & IPsec VPN, model FVS336Gv2.

This chapter introduces the CLI interface. It includes the following sections:

- *Command Syntax and Conventions*
- *Four Categories of Commands*
- *Configuration Commands: Four Main Modes*
- *Configuration Commands: Save Commands*
- *Global Commands*
- *Examples of Three Basic Types of Commands*
- *Command Autocompletion and Command Abbreviation*
- *Access the CLI*

Note: For more information about the topics covered in this manual, visit the support website at *support.netgear.com*.

Note: For more information about the features that you can configure using the CLI, see the *ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN FVS336Gv2 Reference Manual*, which you can download from *downloadcenter.netgear.com*.

Note: You cannot generate and upload a certificate through the CLI. You must access the web management interface to manage these tasks.

Command Syntax and Conventions

A command is one or more words that can be followed by one or more keywords and parameters. Keywords and parameters can be required or optional:

- A keyword is a predefined string (word) that narrows the scope of a command. A keyword can be followed by an associated parameter or by associated keywords. In many cases, these associated keywords are mutually exclusive, so you must select one of them. In some cases, this manual refers to a group of words as a keyword.
- A parameter is a variable for which you must type a value. You must replace the parameter name with the appropriate value, which might be a name or number. A parameter can be associated with a command or with a keyword.

This manual lists each command by its full command name and provides a brief description of the command. In addition, for each command, the manual provides the following information:

- **Format**. Shows the command keywords and the required and optional parameters.
- **Mode**. Identifies the command mode that you must be in to access the command. (With some minor exceptions, the mode is always described using lowercase letters.)
- **Related show command or commands**. Identifies and links to the show command or commands that can display the configured information.

For more complicated commands, in addition to the format, mode, and related show command or commands, the following information is provided:

- **Table**. Explains the keywords and parameters that you can use for the command.
- **Example**. Shows a CLI example for the command.

Command Conventions

In this manual, the following type conventions are used:

- A command name is stated in **`bold`** type.
- A keyword name is stated in **`bold`** type.
- A parameter name is stated in *`italic`* type.

The keywords and parameters for a command might include mandatory values, optional values, or choices. The following table describes the conventions that this manual uses to distinguish between value types:

Table 1. Command conventions

Symbol	Example	Description
< > angle brackets	<*value*>	Indicate that you must enter a value in place of the brackets and text inside them. (*value* is the parameter.)
[ ] square brackets	[*value*]	Indicate an optional parameter that you can enter in place of the brackets and text inside them. (*value* is the parameter.)

Table 1. Command conventions (continued)

Symbol	Example	Description
{ } curly braces	{**choice1** | **choice2**}	Indicate that you must select a keyword from the list of choices. (**choice1** and **choice1** are keywords.)
| vertical bars	**choice1** | **choice2**	Separate the mutually exclusive choices. (**choice1** and **choice1** are keywords.)
[{ }] braces within square brackets	[{**choice1** | **choice2**}]	Indicate a choice within an optional element. (**choice1** and **choice1** are keywords.)

Description of a Command

The following example describes the **net radvd pool lan edit** *<row id>* command:

net radvd pool lan edit is the command name.

<row id> is the required parameter for which you must enter a value after you type the command words.

The command lets you enter the net-config [radvd-pool-lan] mode, from which you can issue the following keywords and parameters:

prefix_type {**6To4** {**6to4_interface** {**WAN1** | **WAN2**} {**sla_id** *<ID number>*} | **Global-Local-ISATAP** {**prefix_address** *<ipv6-address>*} {**prefix_length** *<prefix length>*}}

prefix_life_time *<seconds>*

Explanation of the keywords and parameters:

- **prefix_type** is a keyword. The required associated keyword that you must select is either **6to4_interface** or **Global-Local-ISATAP**.
  - If you select **6to4_interface**, you must specify the WAN interface by typing **WAN1** or **WAN2**, and you must issue the **sla_id keyword** and enter a value for the *<ID number>* parameter.
  - If you select **Global-Local-ISATAP**, you must issue the **prefix_address** keyword and enter a value for the *<ipv6-address>* parameter, and you must issue the **prefix_length** keyword and enter a value for the *<prefix length>* parameter.
- **prefix_life_time** is a keyword and *<seconds>* is the required parameter for which you must enter a value.

Command example:

```
FVS336Gv2> net radvd pool lan edit 12
net-config[radvd-pool-lan]> prefix_type Global-Local-ISATAP
net-config[radvd-pool-lan]> prefix_address 10FA:2203:6145:4201::
net-config[radvd-pool-lan]> prefix_length 10
net-config[radvd-pool-lan]> prefix_life_time 3600
net-config[radvd-pool-lan]> save
```

Common Parameters

Parameter values might be names (strings) or numbers. To use spaces as part of a name parameter, enclose the name value in double quotes. For example, the expression “System Name with Spaces” forces the system to accept the spaces. Empty strings (“”) are not valid user-defined strings. The following table describes common parameter values and value formatting:

Table 2. Common parameters

Parameter	Description
ipaddr	This parameter is a valid IPv4 address. You must enter the IP address in the a.b.c.d format, in which each octet is a number in the range from 0 to 255 (both inclusive), for example, 10.12.140.218. The CLI accepts decimal, hexadecimal, and octal formats through the following input formats (where *n* is any valid decimal, hexadecimal, or octal number): • 0x*n* (CLI assumes hexadecimal format) • 0*n* (CLI assumes octal format with leading zeros) • *n* (CLI assumes decimal format)
ipv6-address	This parameter is a valid IPv6 address. You can enter the IPv6 address in one of the following formats: • FE80:0000:0000:0000:020F:24FF:FEBF:DBCB • FE80:0:0:0:20F:24FF:FEBF:DBCB • FE80::20F:24FF:FEBF:DBCB • FE80:0:0:0:20F:24FF:128:141:49:32 For additional information, see *RFC 3513*.
Character strings	Use double quotation marks to identify character strings, for example, “System Name with Spaces”. An empty string (“”) is not valid.

Four Categories of Commands

CLI commands are grouped into four categories:

- **Configuration**. Configuration commands with four main configuration modes. For more information, see *Configuration Commands: Four Main Modes* on page 10.

  Save commands also fall into this category. For more information, see *Configuration Commands: Save Commands* on page 13.

- **Show**. Show commands that are available for the four main configuration modes. For more information, see *Chapter 7, Overview of the Show Commands* and *Chapter 8, Show Commands*.
- **Utility**. See *Chapter 9, Utility Commands*.
- **Global**. See *Global Commands* on page 14.

Configuration Commands: Four Main Modes

For the configuration commands, the CLI provides four main modes: net, security, system, and vpn. *Chapter 2, Overview of the Configuration Commands* lists all commands in these modes, and each of these modes is described in detail in a separate chapter (see *Chapter 3* through *Chapter 6*).

The following table lists the *main* configuration modes, the configuration modes, the features that you can configure in each configuration mode, and, for orientation, the basic web management interface (GUI) path to the feature.

Table 3. Main configuration modes

CLI			Web Management Interface (GUI)
Main Mode	**Submode**	**Feature That You Can Configure**	**Basic Path**
Network configuration commands			
net	ddns	Dynamic DNS	Network Configuration > Dynamic DNS
	dmz	DMZ for IPv4 DMZ for IPv6	Network Configuration > DMZ Setup
	ethernet	VLAN assignment to LAN interface	Network Configuration > LAN Setup
	ipv6	IPv4 or IPv4/IPv6 mode	Network Configuration > WAN Settings
	ipv6_tunnel	IPv6 tunnels	Network Configuration > WAN Settings
	lan	IPv4 LAN settings and VLANs LAN groups for IPv4 Secondary IPv4 LAN addresses Advanced IPv4 LAN settings Fixed and reserved DHCP IPv4 addresses LAN IPv4 traffic meter profiles IPv6 LAN settings Secondary IPv6 LAN addresses IPv6 LAN DHCP address pools IPv6 prefix delegation for the LAN	Network Configuration > LAN Setup
	radvd	IPv6 RADVD and pools for the LAN IPv6 RADVD and pools for the DMZ	Network Configuration > LAN Setup Network Configuration > DMZ Setup
	routing	Dynamic IPv4 routes Static IPv4 routes Static IPv6 routes	Network Configuration > Routing

Table 3. Main configuration modes (continued)

CLI			Web Management Interface (GUI)
Main Mode	**Submode**	**Feature That You Can Configure**	**Basic Path**
net (continued)	siit	Stateless IP/ICMP Translation	Network Configuration > SIIT
	wan	IPv4 WAN (Internet) settings Secondary IPv4 WAN addresses IPv6 WAN (Internet) settings MTU, port speed, and MAC address, failure detection method, and upload/download settings	Network Configuration > WAN Settings
	wan_settings	NAT or Classical Routing Load balancing settings for IPv4	Network Configuration > WAN Settings
Security configuration commands			
security	address_filter	Source MAC filters IP/MAC bindings for IPv4 IP MAC bindings for IPv6	Security > Address Filter
	bandwidth	Bandwidth profiles	Security > Bandwidth Profile
	content_filter	Group filtering Blocked keywords Web components Trusted domains	Security > Content Filtering
	firewall	All IPv4 firewall rules All IPv6 firewall rules Attack checks Session limits and time-outs SIP ALG	Security > Firewall
	porttriggering_rules		Security > Port Triggering
	schedules		Security > Schedule
	services	Custom services Service groups LAN and WAN IP groups LAN QoS profiles	Security > Services
	upnp		Security > UPnP

Table 3. Main configuration modes (continued)

CLI			Web Management Interface (GUI)
Main Mode	**Submode**	**Feature That You Can Configure**	**Basic Path**
Administration and monitoring configuration commands			
system	logging		Monitoring > Firewall Logs & E-mail
	remote_management		Administration > Remote Management
	snmp		Administration > SNMP
	schedule_reboot		Monitoring > Diagnostics
	time		Administration > Time Zone
	traffic_meter	WAN traffic meters	Monitoring > Traffic Meter
VPN configuration commands			
vpn	ipsec	IPSec Wizard IKE policies VPN policies Mode Config records RADIUS servers	VPN > IPSec VPN
	l2tp	L2TP server	VPN > L2TP Server
	pptp	PPTP server	VPN > PPTP Server
	sslvpn	SSL Wizard SSL policies Resources and resource objects Portal layouts SSL VPN clients Client routes Port forwarding	VPN > SSL VPN
		Domains Groups User accounts User login and IP policies	Users

Configuration Commands: Save Commands

The following table describes the configuration commands that let you save or cancel configuration changes in the CLI. You can use these commands in *any* of the four main configuration modes. These commands are *not* preceded by a period.

Table 4. Save commands

Command	Description
save	Save the configuration changes.
exit	Save the configuration changes and exit the current configuration mode.
cancel	Roll back the configuration changes.

Commands That Require Saving

After you issue a command that includes the word **configure**, **add**, or **edit**, you enter a configuration mode from which you can issue keywords and associated parameters.

These are examples of commands for which you must save your changes:

- **net lan ipv4 configure** <*vlan id*> lets you enter the net-config [lan-ipv4] configuration mode. After you make your changes, issue **save** or **exit** to save your changes.
- **security content_filter trusted_domain add** lets you enter the security-config [approved-urls] configuration mode. After you make your changes, issue **save** or **exit** to save your changes.
- **vpn sslvpn users groups add** lets you enter the vpn-config [user-groups] configuration mode. After you make your changes, issue **save** or **exit** to save your changes.

Commands That Do Not Require Saving

You do *not* need to save your changes after you issue a command that deletes, disables, or enables a row ID, name, IP address, or MAC address, or that lets you make a configuration change without entering another configuration mode.

These are examples of commands that you do not need to save:

- **net lan dhcp reserved_ip delete** <*mac address*>
- **vpn ipsec vpnpolicy disable** <*vpn policy name*>
- **security firewall ipv4 enable** <*row id*>
- **security firewall ipv4 default_outbound_policy** {**Allow** | **Block**}

Global Commands

The following table describes the global commands that you can use *anywhere* in the CLI. These commands must be preceded by a period.

Table 5. Global CLI commands

Command	Description
.exit	Exit the current session.
.help	Display an overview of the CLI syntax.
.top	Return to the default command mode or root.
.reboot	Reboot the system.
.history	Display the command-line history of the current session.

Examples of Three Basic Types of Commands

You can encounter the following three basic types of commands in the CLI:

- **Entry commands to enter a configuration mode**. Commands that let you enter a configuration mode from which you can configure various keywords and associated parameters and keywords. For example, the **net wan wan1 ipv4 configure** command lets you enter the net-config [wan1-ipv4] mode, from which you can configure the IPv4 WAN settings.

  This type of command is the most common in the CLI and is always indicated by two steps in this manual, each one showing the format and mode:

Step 1	**Format**	**net wan wan ipv4 configure** <*wan interface*>
	Mode	net
Step 2	**Format**	This section shows the keywords and associated parameters, for example: **isp_connection_type** {**STATIC** | **DHCPC** | **PPPoE** | **PPTP**}
	Mode	net-config [wan1-ipv4]

  Sometimes, you must enter a parameter to enter a configuration mode. For example, **security schedules edit** <*row id*> requires you to enter the row ID (that is, the row number in the table that contains all the schedules) for the schedule that you want to modify. Then, you enter the security-config [schedules] mode, from which you can modify various keywords and associated parameters and keywords.

- **Commands with a single parameter**. Commands that require you to supply one or more parameters and that do not let you enter another configuration mode. The parameter is usually a row number or a name. For example, **security firewall ipv4 delete** <*row id*> requires you to enter the row ID (that is, the row number in the table that contains all the firewall rules) for the firewall rule that you want to delete.

For this type of command, the manual shows the format and mode:

Format `security firewall ipv4 delete <row id>`

Mode security

- **Commands without parameters**. Commands that do *not* require you to supply a parameter after the command and that do not let you enter another configuration mode. For example, **`util restore_factory_defaults`** does not require parameters.

  For this type of command, the manual shows the format and mode:

  Format `util restore_factory_defaults`

  Mode util

Command Autocompletion and Command Abbreviation

Command autocompletion finishes spelling a command when you type enough letters of the command to uniquely identify the command keyword. You must type all of the required keywords and parameters before you can use autocompletion.

Press either of the following keys to let the current command autocomplete. If the command prefix is not unique, press the key again to display possible completions.

- **Enter or Return key**. Autocompletes, syntax-checks, and then executes the command. If a syntax error occurs, the offending part of the command is highlighted and explained.
- **Spacebar**. Autocompletes, or if the command is already resolved, inserts a space.

The following table describes the key combinations that you can use to edit commands or increase the speed of command entry. Access this list from the CLI by issuing **`.help`**.

Table 6. CLI editing conventions

Key or Key Sequence	Description
Invoking context-sensitive help	
?	Displays context-sensitive help. The information that displays consists either of a list of possible command completions with summaries or of the full syntax of the current command. When a command is resolved, a subsequent repeat of the help key displays a detailed reference.
Autocompleting **Note:** Command autocompletion finishes spelling the command when you type enough letters of a command to uniquely identify the command keyword. However, you must type all of the required keywords and parameters before you use autocompletion.	
Enter (or Return)	Autocompletes, syntax-checks, and then executes a command. If a syntax error occurs, the offending part of the command line is highlighted and explained. If the command prefix is not unique, press the key again to display possible completions.

Table 6. CLI editing conventions (continued)

Key or Key Sequence	Description
Spacebar	Autocompletes, or if the command is already resolved, inserts a space. If the command prefix is not unique, press the key again to display possible completions.
Moving around	
Ctrl-A	Go to the beginning of the line.
Ctrl-E	Go to the end of the line.
Up arrow	Go to the previous line in the history buffer.
Down arrow	Go to the next line in the history buffer.
Left arrow	Go backward one character.
Right arrow	Go forward one character.
Deleting	
Ctrl-C	Delete the entire line.
Ctrl-D	Delete the next character.
Ctrl-K	Delete all characters to the end of the line from where the cursor is located.
Backspace	Delete the previous character.
Invoking escape sequences	
!!	Substitute the previous line.
!N	Substitute the Nth line, in which N is the absolute line number as displayed in the output of the **`history`** command.
!-N	Substitute the line that is located N lines before the current line, in which N is a relative number in relation to the current lint.

Access the CLI

You can access the CLI by logging in with the same user credentials (user name and password) that you use to access the web management interface. FVS336Gv2> is the CLI prompt.

```
FVS336Gv2 login: admin
Password:
**********************************************
    Welcome to FVS336Gv2 Command Line Interface
**********************************************
FVS336Gv2>
```

Overview of the Configuration Commands

2

This chapter provides an overview of all configuration commands in the four configuration command modes. The keywords and associated parameters that are available for these commands are explained in *Chapter 3* through *Chapter 6*. The chapter includes the following sections:

- *Network Settings Configuration Commands*
- *Security Settings Configuration Commands*
- *System Administrative and Monitoring Settings Configuration Commands*
- *VPN Settings Configuration Commands*

Network Settings Configuration Commands

Enter the **net ?** command at the CLI prompt to display the submodes in the net mode. The following table lists the submodes and their commands in alphabetical order:

Table 7. Net mode configuration commands

Submode	Command Name	Purpose
ddns	*net ddns configure*	Enable, configure, or disable DDNS service.
dmz	*net dmz ipv4 configure*	Enable, configure, or disable the IPv4 DMZ.
	net dmz ipv6 configure	Enable, configure, or disable the IPv6 DMZ.
	net dmz ipv6 pool configure <ipv6 address>	Configure a new or existing IPv6 DMZ DHCP address pool.
	net dmz ipv6 pool delete < ipv6 address>	Delete an IPv6 DMZ DHCP address pool.
ethernet	*net ethernet configure <interface name or number>*	Configure a VLAN for a LAN interface.
ipv6	*net ipv6 ipmode configure*	Configure the IP mode (IPv4 only or IPv4/IPv6).
ipv6_tunnel	*net ipv6_tunnel isatap add*	Configure a new IPv6 ISATAP tunnel.
	net ipv6_tunnel isatap delete <row id>	Delete an IPv6 ISATAP tunnel.
	net ipv6_tunnel isatap edit <row id>	Configure an existing IPv6 ISATAP tunnel.
	net ipv6_tunnel six_to_four configure	Enable or disable automatic (6to4) tunneling.
lan	*net lan dhcp reserved_ip configure <mac address>*	Bind a MAC address to an IP address for DHCP reservation or change an existing binding, and assign a LAN group.
	net lan dhcp reserved_ip delete <mac address>	Delete the binding of a MAC address to an IP address.
	net lan ipv4 advanced configure	Configure advanced LAN settings such as the MAC address for VLANs and ARP broadcast.
	net lan ipv4 configure <vlan id>	Configure a new or existing VLAN.
	net lan ipv4 default_vlan	Configure the default VLAN for each port.
	net lan ipv4 delete <vlan id>	Delete a VLAN.
	net lan ipv4 disable <vlan id>	Disable a VLAN.
	net lan ipv4 enable <vlan id>	Enable a VLAN.
	net lan ipv4 multi_homing add	Configure a new secondary IPv4 address.
	net lan ipv4 multi_homing delete <row id>	Delete a secondary IPv4 address.

Table 7. Net mode configuration commands (continued)

Submode	Command Name	Purpose
lan (continued)	*net lan ipv4 multi_homing edit <row id>*	Configure an existing secondary IPv4 address.
	net lan ipv4 traffic_meter configure <ip address>	Configure a traffic meter profile for an IPv4 address.
	net lan ipv4 traffic_meter delete <row id>	Delete a traffic meter profile.
	net lan ipv6 configure	Configure the IPv6 LAN address settings and DHCPv6.
	net lan ipv6 multi_homing add	Configure a new secondary IPv6 address.
	net lan ipv6 multi_homing delete <row id>	Delete a secondary IPv6 address.
	net lan ipv6 multi_homing edit <row id>	Configure an existing secondary IPv6 address.
	net lan ipv6 pool add	Configure a new IPv6 LAN DHCP address pool.
	net lan ipv6 pool delete <row id>	Delete an IPv6 LAN DHCP address pool.
	net lan ipv6 pool edit <row id>	Configure an existing IPv6 LAN DHCP address pool.
	net lan ipv6 prefix_delegation add	Configure a new prefix for IPv6 LAN prefix delegation.
	net lan ipv6 prefix_delegation delete <row id>	Delete a prefix for IPv6 LAN prefix delegation.
	net lan ipv6 prefix_delegation edit <row id>	Configure an existing prefix for IPv6 LAN prefix delegation.
	net lan lan_groups edit <row id> <new group name>	Change an existing LAN default group name.
protocol binding	*net protocol_binding add*	Configure a new protocol binding.
	net protocol_binding delete	Delete a protocol binding.
	net protocol_binding disable	Disable a protocol binding.
	net protocol_binding edit <row id>	Configure an existing protocol binding.
	net protocol_binding enable	Enable a protocol binding.

Table 7. Net mode configuration commands (continued)

Submode	Command Name	Purpose
qos	*net qos configure*	Configure the QoS mode for the WAN interfaces.
	net qos profile add	Configure a new WAN QoS profile.
	net qos profile delete <row id>	Delete a WAN QoS profile.
	net qos profile disable <row id>	Disable a WAN QoS profile.
	net qos profile edit <row id>	Configure an existing WAN QoS profile.
	net qos profile enable <row id>	Enable a WAN QoS profile.
radvd	*net radvd configure dmz*	Configure the IPv6 RADVD for the DMZ.
	net radvd configure lan	Configure the IPv6 RADVD for the LAN.
	net radvd pool dmz add	Configure a new IPv6 RADVD pool for the DMZ.
	net radvd pool dmz delete <row id>	Delete an IPv6 RADVD pool from the DMZ.
	net radvd pool dmz edit <row id>	Configure an existing IPv6 RADVD pool for the DMZ.
	net radvd pool lan add	Configure a new IPv6 RADVD pool for the LAN.
	net radvd pool lan delete <row id>	Delete an IPv6 RADVD pool from the LAN.
	net radvd pool lan edit <row id>	Configure an existing IPv6 RADVD pool for the LAN.
routing	*net routing dynamic configure*	Configure RIP and the associated MD5 key information.
	net routing static ipv4 configure <route name>	Configure a new or existing IPv4 static route.
	net routing static ipv4 delete <route name>	Delete an IPv4 static route.
	net routing static ipv4 delete_all	Delete all IPv4 routes.
	net routing static ipv6 configure <route name>	Configure a new or existing IPv6 static route.
	net routing static ipv6 delete <route name>	Delete an IPv6 static route.
	net routing static ipv6 delete_all	Delete all IPv6 routes.
siit	*net siit configure*	Configure Stateless IP/ICMP Translation.
wan	*net wan port_setup ipv4 configure <wan interface>*	Configure the failover method, MTU, port speed, and MAC address of an IPv4 WAN interface.
	net wan port_setup ipv6 configure <wan interface>	Configure the failure detection ping settings of an IPv6 WAN interface.

Table 7. Net mode configuration commands (continued)

Submode	Command Name	Purpose
wan (continued)	*net wan wan ipv4 configure <wan interface>*	Configure the ISP settings of an IPv4 WAN interface.
	net wan wan ipv4 secondary_address add <wan interface>	Configure a secondary IPv4 WAN address.
	net wan wan ipv4 secondary_address delete <row id>	Delete a secondary IPv4 WAN address.
	net wan wan ipv6 configure <wan interface>	Configure the ISP settings of an IPv6 WAN interface.
wan_settings	*net wan_settings load_balancing configure*	Configure the load balancing settings for two WAN interfaces that are configured for IPv4.
	net wan_settings wanmode configure	Configure the mode of IPv4 routing (NAT or classical routing) between the WAN interface and LAN interfaces.

Security Settings Configuration Commands

Enter the **`security ?`** command at the CLI prompt to display the submodes in the security mode. The following table lists the submodes and their commands in alphabetical order:

Table 8. Security mode configuration commands

Submode	Command Name	Purpose
address_filter	*security address_filter ip_or_mac_binding add*	Configure a new IP/MAC binding rule.
	security address_filter ip_or_mac_binding delete <row id>	Delete an IP/MAC binding rule.
	security address_filter ip_or_mac_binding edit <row id>	Configure an existing IP/MAC binding rule.
	security address_filter ip_or_mac_binding enable_email_log <ip version>	Configure the email log for IP/MAC Binding violations.
	security address_filter mac_filter configure	Configure the source MAC address filter.
	security address_filter mac_filter source add	Configure a new MAC source address.
	security address_filter mac_filter source delete <row id>	Delete a MAC source address.

Table 8. Security mode configuration commands (continued)

Submode	Command Name	Purpose
bandwidth	*security bandwidth enable_bandwidth_profiles {Y | N}*	Enable or disable bandwidth profile globally.
	security bandwidth profile add	Configure a new bandwidth profile.
	security bandwidth profile delete <row id>	Delete a bandwidth profile.
	security bandwidth profile edit <row id>	Configure an existing bandwidth profile.
content_filter	*security content_filter block_group disable*	Remove content filtering from groups.
	security content_filter block_group enable	Apply content filtering to groups.
	security content_filter blocked_keywords add	Configure a new blocked keyword.
	security content_filter blocked_keywords delete <row id>	Delete a blocked keyword.
	security content_filter blocked_keywords edit <row id>	Configure an existing blocked keyword.
	security content_filter content_filtering configure	Configure web content filtering.
	security content_filter trusted_domain add	Configure a new trusted domain.
	security content_filter trusted_domain delete <row id>	Delete a trusted domain.
	security content_filter trusted_domain edit <row id>	Configure an existing trusted domain.
firewall	*security firewall advanced algs*	Configure SIP support for the ALG.
	security firewall attack_checks configure ipv4	Configure WAN and LAN security attack checks for IPv4 traffic.
	security firewall attack_checks configure ipv6	Configure WAN security attack checks for IPv6 traffic.
	security firewall attack_checks vpn_passthrough configure	Configure VPN pass-through for IPv4 traffic.
	security firewall igmp alternate_networks add	Configure a new alternate network.
	security firewall igmp alternate_networks delete	Delete an alternate network.
	security firewall igmp configure	Enable or disable multicast pass-through for IPv4 traffic.
	security firewall ipv4 add_rule dmz_wan inbound	Configure a new IPv4 DMZ WAN inbound firewall rule.
	security firewall ipv4 add_rule dmz_wan outbound	Configure a new IPv4 DMZ WAN outbound firewall rule.

Table 8. Security mode configuration commands (continued)

Submode	Command Name	Purpose
firewall (continued)	*security firewall ipv4 add_rule lan_dmz inbound*	Configure a new IPv4 LAN DMZ inbound firewall rule.
	security firewall ipv4 add_rule lan_dmz outbound	Configure a new IPv4 LAN DMZ outbound firewall rule.
	security firewall ipv4 add_rule lan_wan inbound	Configure a new IPv4 LAN WAN inbound firewall rule.
	security firewall ipv4 add_rule lan_wan outbound	Configure a new IPv4 LAN WAN outbound firewall rule.
	security firewall ipv4 default_outbound_policy {Allow | Block}	Configure the default outbound policy for IPv4 traffic.
	security firewall ipv4 delete <row id>	Delete an IPv4 firewall rule.
	security firewall ipv4 disable <row id>	Disable an IPv4 firewall rule.
	security firewall ipv4 edit_rule dmz_wan inbound <row id>	Configure an existing IPv4 DMZ WAN inbound firewall rule.
	security firewall ipv4 edit_rule dmz_wan outbound <row id>	Configure an existing IPv4 DMZ WAN outbound firewall rule.
	security firewall ipv4 edit_rule lan_dmz inbound <row id>	Configure an existing IPv4 LAN DMZ inbound firewall rule.
	security firewall ipv4 edit_rule lan_dmz outbound <row id>	Configure an existing IPv4 LAN DMZ outbound firewall rule.
	security firewall ipv4 edit_rule lan_wan inbound <row id>	Configure an existing IPv4 LAN WAN inbound firewall rule.
	security firewall ipv4 edit_rule lan_wan outbound <row id>	Configure an existing IPv4 LAN WAN outbound firewall rule.
	security firewall ipv4 enable <row id>	Enable an IPv4 firewall rule.
	security firewall ipv6 configure	Configure a new IPv6 firewall rule.
	security firewall ipv6 default_outbound_policy {Allow | Block}	Configure the default outbound policy for IPv6 traffic.
	security firewall ipv6 delete <row id>	Delete an IPv6 firewall rule.
	security firewall ipv6 disable <row id>	Disable an IPv6 firewall rule.
	security firewall ipv6 edit <row id>	Configure an existing IPv6 firewall rule.
	security firewall ipv6 enable <row id>	Enable an IPv6 firewall rule.
	security firewall session_limit configure	Configure global session limits.
	security firewall session_settings configure	Configure global session time-outs.

Table 8. Security mode configuration commands (continued)

Submode	Command Name	Purpose
porttriggering_rules	*security porttriggering_rules add*	Configure a new port triggering rule.
	security porttriggering_rules delete <row id>	Delete a port triggering rule.
	security porttriggering_rules edit <row id>	Configure an existing port triggering rule.
schedules	*security schedules edit {1 | 2 | 3}*	Configure one of the three security schedules.
services	*security services add*	Configure a new custom service.
	security services delete <row id>	Delete a custom service.
	security services edit <row id>	Configure an existing custom service.
	security services ip_group add	Configure a new LAN or WAN IP group.
	security services ip_group add_ip_to <group name>	Add an IP address to a LAN or WAN IP group.
	security services ip_group delete <row id>	Delete a LAN or WAN IP group.
	security services ip_group delete_ip <row id>	Remove an IP address from a LAN or WAN IP group.
	security services ip_group edit <row id>	Configure an existing LAN or WAN IP group.
	security services qos_profile add	Add a QoS profile.
	security services qos_profile delete <row id>	Delete a QoS profile.
	security services qos_profile edit <row id>	Configure an existing QoS profile.
	security services service_group add	Add a service group.
	security services service_group edit <row id>	Delete a service group.
	security services service_group delete <row id>	Configure an existing service group.
upnp	*security upnp configure*	Configure UPnP.

System Administrative and Monitoring Settings Configuration Commands

Enter the **system ?** command at the CLI prompt to display the submodes in the system mode. The following table lists the submodes and their commands in alphabetical order:

Table 9. System mode configuration commands

Submode	Command Name	Purpose
logging	*system logging configure*	Configure routing logs for accepted and dropped IPv4 and IPv6 packets.
	system logging remote configure	Configure email logs and alerts, schedule email logs and alerts, and configure a syslog server.
remote_management	*system remote_management https configure*	Configure remote management over HTTPS.
	system remote_management telnet configure	Configure remote management over Telnet.
schedule_reboot	*system schedule_reboot configure*	Schedule the VPN firewall to be rebooted.
snmp	*system snmp remote_snmp enable*	Enable or disable SNMP access from the WAN.
	system snmp sys configure	Configure the SNMP system information.
	system snmp trap configure <ip address>	Configure an SNMP agent and community.
	system snmp trap delete <ipaddress>	Delete an SNMP agent.
	system snmp trapevent edit	Change the default SNMP trap events.
	system snmp v3_users edit	Change the default SNMPv3 users.
time	*system time configure*	Configure the system time, date, and NTP servers.
traffic_meter	*system traffic_meter configure <wan interface>*	Configure the WAN traffic meter.

VPN Settings Configuration Commands

Enter the **vpn ?** command at the CLI prompt to display the submodes in the vpn mode. The following table lists the submodes and their commands in alphabetical order:

Table 10. Configuration commands: vpn mode

Submode	Command Name	Purpose
ipsec	*vpn ipsec ikepolicy configure <ike policy name>*	Configure a new or existing manual IPSec IKE policy.
	vpn ipsec ikepolicy delete <ike policy name>	Delete an IPSec policy.
	vpn ipsec mode_config configure <record name>	Configure a new or existing Mode Config record.
	vpn ipsec mode_config delete <record name>	Delete a Mode Config record.
	vpn ipsec radius configure	Configure the RADIUS servers.
	vpn ipsec vpnpolicy configure <vpn policy name>	Configure a new or existing auto IPSec VPN policy or manual IPSec VPN policy.
	vpn ipsec vpnpolicy connect <vpn policy name>	Establish a VPN connection.
	vpn ipsec vpnpolicy delete <vpn policy name>	Delete an IPSec VPN policy.
	vpn ipsec vpnpolicy disable <vpn policy name>	Disable an IPSec VPN policy.
	vpn ipsec vpnpolicy drop <vpn policy name>	Terminate an IPSec VPN connection.
	vpn ipsec vpnpolicy enable <vpn policy name>	Enable an IPSec VPN policy.
	vpn ipsec wizard configure <Gateway | VPN_Client>	Configure the IPSec VPN wizard for a gateway-to-gateway or gateway-to-VPN client connection.
l2tp	*vpn l2tp server configure*	Configure the L2TP server.
pptp	*vpn pptp server configure*	Configure the PPTP server.
sslvpn	*vpn sslvpn client ipv4*	Configure the SSL client IPv4 address range.
	vpn sslvpn client ipv6	Configure the SSL client IPv6 address range.
	vpn sslvpn policy add	Configure a new SSL VPN policy.
	vpn sslvpn policy delete <row id>	Delete an SSL VPN policy.
	vpn sslvpn policy edit <row id>	Configure an existing SSL VPN policy.
	vpn sslvpn portal_layouts add	Configure a new SSL VPN portal layout.
	vpn sslvpn portal_layouts delete <row id>	Delete an SSL VPN portal layout.

Table 10. Configuration commands: vpn mode (continued)

Submode	Command Name	Purpose
sslvpn (continued)	*vpn sslvpn portal_layouts edit <row id>*	Configure an existing SSL VPN portal layout.
	vpn sslvpn portal_layouts set_default <row id>	Configure the default SSL VPN portal layout.
	vpn sslvpn portforwarding appconfig add	Configure a new SSL port forwarding application.
	vpn sslvpn portforwarding appconfig delete <row id>	Delete an SSL VPN port forwarding application.
	vpn sslvpn portforwarding hostconfig add	Configure a new host name for an SSL port forwarding application.
	vpn sslvpn portforwarding hostconfig delete <row id>	Delete a host name for an SSL port forwarding application.
	vpn sslvpn resource add	Add a new SSL VPN resource.
	vpn sslvpn resource configure add <resource name>	Configure an SSL VPN resource object.
	vpn sslvpn resource configure delete <row id>	Delete an SSL VPN resource object.
	vpn sslvpn resource delete <row id>	Delete an SSL VPN resource.
	vpn sslvpn route add	Add an SSL VPN client route.
	vpn sslvpn route delete <row id>	Delete an SSL VPN client route.
	vpn sslvpn users domains add	Configure a new authentication domain.
	vpn sslvpn users domains delete <row id>	Delete an authentication domain.
	vpn sslvpn users domains disable_Local_Authentication {Y | N}	Enable or disable local authentication for users.
	vpn sslvpn users domains edit <row id>	Configure an existing authentication domain.
	vpn sslvpn users groups add	Configure a new authentication group.
	vpn sslvpn users groups delete <row id>	Delete an authentication group.
	vpn sslvpn users groups edit <row id>	Configure an existing authentication group.
	vpn sslvpn users users add	Add a new user account.
	vpn sslvpn users users browser_policies <row id>	Configure the client browsers from which a user is either allowed or denied access.
	vpn sslvpn users users delete <row id>	Delete a user account.
	vpn sslvpn users users edit <row id>	Configure an existing user account.

Table 10. Configuration commands: vpn mode (continued)

Submode	Command Name	Purpose
sslvpn (continued)	*vpn sslvpn users users ip_policies configure <row id>*	Configure source IP addresses from which a user is either allowed or denied access.
	vpn sslvpn users users ip_policies delete <row id>	Delete a source IP address for a user.
	vpn sslvpn users users login_policies <row id>	Configure the login policy for a user.
	vpn sslvpn wizard configure	Configure the SSL VPN wizard for an SSL portal.

Net Mode Configuration Commands

3

This chapter explains the configuration commands, keywords, and associated parameters in the net mode. The chapter includes the following sections:

- *General WAN Commands*
- *IPv4 WAN Commands*
- *IPv6 WAN Commands*
- *IPv6 Tunnel Commands*
- *Dynamic DNS Command*
- *IPv4 LAN Commands*
- *IPv6 LAN Commands*
- *IPv4 DMZ Setup Command*
- *IPv6 DMZ Setup Commands*
- *WAN QoS Commands*
- *IPv4 Routing Commands*
- *IPv6 Routing Commands*

IMPORTANT:

After you issue a command that includes the word `configure`, `add`, or `edit`, you must save (or cancel) your changes. For more information, see *Configuration Commands: Save Commands* on page 13.

General WAN Commands

This section describes the following commands:

- *net wan port_setup ipv4 configure <wan interface>*
- *net wan port_setup ipv6 configure <wan interface>*

net wan port_setup ipv4 configure <wan interface>

This command configures the advanced WAN settings for an IPv4 WAN interface, that is, the MTU, port speed, MAC address, failure detection method, and upload and download settings of the VPN firewall. After you issue the **net wan port_setup ipv4 configure** command to specify one of the two WAN interfaces (that is, WAN1 or WAN2), you enter the net-config [port_setup_ipv4] mode and then you can configure the advanced settings for the specified interface in the order that you prefer.

Step 1 **Format** **net wan port_setup ipv4 configure** <*wan interface*>

Mode net

Step 2 **Format** **def_mtu** {**Default** | **Custom** {**mtu_size** <*number*>}}

port_speed {**Auto_Sense** | **10_BaseT_Half_Duplex** |
10_BaseT_Full_Duplex | **100_BaseT_Half_Duplex** |
100_BaseT_Full_Duplex | **1000_BaseT_Full_Duplex**}

mac_type {**Use-Default-Mac** | **Use-This-Computers-Mac** |
Use-This-Mac {**mac_address** <*mac address*>}}

failover_method type {**None** | **WAN-DNS** {**failover_method**
retry_interval <*seconds*>} {**failover_method retry_attempts**
<*number*>}| **CUSTOM-DNS** {**failover_method dns_ipaddress_wan**
<*ipaddress*>} {**failover_method retry_interval** <*seconds*>}
{**failover_method retry_attempts** <*number*>}|
Ping {**failover_method ping_ipaddress_wan** <*ipaddress*>}
{**failover_method retry_interval** <*seconds*>} {**failover_method**
retry_attempts <*number*>}}

upload_download wan_conn_type {**DSL** | **ADSL** | **T1** | **T3** | **Other**}
upload_download upload_speed_type {**56-Kbps** | **128-Kbps** |
256-Kbps | **384-Kbps** | **512-Kbps** | **768-Kbps** | **1500-Kbps** |
1544-Kbps | **10-Mbps** | **44.736-Mbps** | **100-Mbps** | **1-Gbps** |
Custom {**upload_download upload_speed** <*speed*>}}
upload_download download_speed_type {**56-Kbps** | **128-Kbps** |
256-Kbps | **384-Kbps** | **512-Kbps** | **768-Kbps** | **1500-Kbps** |
1544-Kbps | **10-Mbps** | **44.736-Mbps** | **100-Mbps** | **1-Gbps** |
Custom {**upload_download download_speed** <*speed*>}}

Mode net-config [port_setup_ipv4]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
MTU		
def_mtu	**Default** or **Custom**	Specifies whether the default MTU or a custom MTU is used. If you select **Custom**, you must issue the **mtu_size** keyword and specify the size of the MTU.
mtu_size	*number*	The size of the default MTU in bytes for the WAN port: • If you configured IPv4 mode, type a number between 68 and 1500 bytes. • If you configured IPv4/IPv6 mode, type a number between 1280 and 1500 bytes.
Port speed		
port_speed	**Auto_Sense**, **10_BaseT_Half_Duplex**, **10_BaseT_Full_Duplex**, **100_BaseT_Half_Duplex**, **100_BaseT_Full_Duplex**, or **1000_BaseT_Full_Duplex**	Specifies the port speed and duplex mode of the WAN port. The keywords are self-explanatory.
MAC address		
mac_type	**Use-Default-Mac**, **Use-This-Computers-Mac**, or **Use-This-Mac**	Specifies the source for the MAC address. The default setting is **Use-Default-Mac**. If your ISP requires MAC authentication and another MAC address was previously registered with your ISP, select either **Use-This-Computers-Mac** or **Use-This-Mac**. If you select the latter keyword, you must issue the **mac_address** keyword and specify the MAC address that is expected by your ISP.
mac_address	*mac address*	The MAC address that the ISP requires for MAC authentication when the **mac_type** keyword is set to **Use-This-Mac**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Failure detection method		
failover_method type	**None**, **WAN-DNS**, **CUSTOM-DNS**, or **Ping**	Specifies the type of failover method for IPv4 connections. You can specify only one type of method: • **None**. No failover method is configured. • **WAN-DNS**. DNS queries are sent to the DNS server that you configure through the *net wan wan ipv4 configure <wan interface>* command. • **CUSTOM-DNS**. DNS queries are sent to the DNS server that you must specify with the **failover_method dns_ipaddress_wan** keyword. • **Ping**. Pings are sent to a server with a public IP address that you must specify with the **failover_method ping_ipaddress_wan** keyword. For all three failover methods, you also must issue the **failover_method retry_interval** keyword to specify and interval and the and **failover_method retry_attempts** keywords to specify the number of attempts.
failover_method retry_interval	*seconds*	The retry interval in seconds, from 5 to 999 seconds. The DNS query or ping is sent periodically after every test period.
failover_method retry_attempts	*number*	The number of failover attempts, from 2 to 999. The primary WAN interface is considered down after the specified number of queries fails to elicit a reply. The backup interface is brought up after this situation has occurred.
failover_method dns_ipaddress_wan	*ipaddress*	The address of the DNS server to which the DNS queries are sent if the failover method is set to **CUSTOM-DNS**.
failover_method ping_ipaddress_wan	*ipaddress*	The ping address to which the pings are sent if the failover method is set to **Ping**.
Upload and download settings		
upload_download wan_conn_type	**DSL**, **ADSL**, **T1**, **T3**, or **Other**	Specifies the type of WAN connection that the VPN firewall uses to connect to the Internet.
upload_download upload_speed_type	**56-Kbps**, **128-Kbps**, **256-Kbps**, **384-Kbps**, **512-Kbps**, **768-Kbps**, **1500-Kbps**, **1544-Kbps**, **10-Mbps**, **44.736-Mbps**, **100-Mbps**, **1-Gbps**, or **Custom**	Specifies the maximum upload speed that is provided by your ISP. If you select **Custom**, you must specify the speed in Kbps with the **upload_download upload_speed** keyword.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
upload_download upload_speed	*speed*	The upload speed in Kbps if the type of WAN connection is **Custom**.
upload_download download_speed_type	**56-Kbps**, **128-Kbps**, **256-Kbps**, **384-Kbps**, **512-Kbps**, **768-Kbps**, **1500-Kbps**, **1544-Kbps**, **10-Mbps**, **44.736-Mbps**, **100-Mbps**, **1-Gbps**, or **Custom**	Specifies the maximum download speed that is provided by your ISP. If you select **Custom**, you must specify the speed in Kbps with the **upload_download download_speed** keyword.
upload_download download_speed	*speed*	The download speed in Kbps if the type of WAN connection is **Custom**.

Command example:

```
FVS336Gv2> net wan port_setup ipv4 configure WAN1
net-config[port_setup_ipv4]> def_mtu Custom
net-config[port_setup_ipv4]> mtu_size 1498
net-config[port_setup_ipv4]> port_speed 1000_BaseT_Full_Duplex
net-config[port_setup_ipv4]> mac_type Use-This-Computers-Mac
net-config[port_setup_ipv4]> failover_method type Ping
net-config[port_setup_ipv4]> failover_method ping_ipaddress_wan 10.147.38.217
net-config[port_setup_ipv4]> failover_method retry_interval 30
net-config[port_setup_ipv4]> failover_method retry_attempts 4
net-config[port_setup_ipv4]> upload_download wan_conn_type DSL
net-config[port_setup_ipv4]> upload_download upload_speed_type 1-Gbps
net-config[port_setup_ipv4]> upload_download download_speed_type 1-Gbps
net-config[port_setup_ipv4]> save
```

Related show command: *show net wan port_setup ipv4 <wan interface>*

net wan port_setup ipv6 configure <wan interface>

This command configures the advanced WAN settings for an IPv6 WAN interface, that is, the failure detection ping settings. After you issue the **net wan port_setup ipv6 configure** command to specify one of the two WAN interfaces (that is, WAN1 or WAN2), you enter the net-config [port_setup_ipv6] mode and then you can configure the failure detection ping settings.

Step 1	**Format**	**net wan port_setup ipv6 configure** <*wan interface*>
	Mode	net
Step 2	**Format**	**ping_ipaddress_wan** <*ipv6-address*>} {**retry_interval** <*seconds*>} {**retry_attempts** <*number*>}
	Mode	net-config [port_setup_ipv6]

Keyword	Associated Keyword to Select or Parameter to Type	Description
ping_ipaddress_wan	*ipv6-address*	The IPv6 ping address to which the pings are sent.
retry_interval	*seconds*	The retry interval in seconds, from 5 to 999 seconds. The ping is sent periodically after every test period.
retry_attempts	*number*	The number of failover attempts, from 2 to 999. The primary WAN interface is considered down after the specified number of queries fails to elicit a reply. The backup interface is brought up after this situation occurs.

Command example:

```
FVS336Gv2> net wan port_setup ipv6 configure WAN1
net-config[port_setup_ipv6]> ping_ipaddress_wan fec1::1
net-config[port_setup_ipv6]> retry_interval 30
net-config[port_setup_ipv6]> retry_attempts 4
net-config[port_setup_ipv6]> save
```

Related show command: *show net wan port_setup ipv6 <wan interface>*

IPv4 WAN Commands

This section describes the following commands:

- *net wan_settings wanmode configure*
- *net wan wan ipv4 configure <wan interface>*
- *net wan wan ipv4 secondary_address add <wan interface>*
- *net wan wan ipv4 secondary_address delete <row id>*
- *net wan_settings load_balancing configure*
- *net protocol_binding add*
- *net protocol_binding edit <row id>*
- *net protocol_binding delete*
- *net protocol_binding disable*
- *net protocol_binding enable*

net wan_settings wanmode configure

This command configures the mode of IPv4 routing between the WAN interface and LAN interfaces. After you issue the **net wan_settings wanmode configure** command, you enter the net-config [routing-mode] mode and then you can configure NAT or classical routing.



WARNING:

Changing the mode of IPv4 routing causes all LAN–WAN and DMZ–WAN inbound firewall settings to revert to default settings.

Step 1	**Format**	**net wan_settings wanmode configure**
	Mode	net
Step 2	**Format**	**type** {**NAT** | **Classical_Routing**}
	Mode	net-config [routing-mode]

Keyword	Associated Keyword to Select	Description
type	**NAT** or **Classical_Routing**	Specifies the IPv4 routing mode.

Command example:

```
FVS336Gv2> net wan_settings wanmode configure
net-config[routing-mode]> NAT
net-config[routing-mode]> save
```

Related show command: *show net wan_settings wanmode*

net wan wan ipv4 configure <wan interface>

This command configures the IPv4 settings for a WAN interface. After you issue the **net wan wan ipv4 configure** command to specify one of the two WAN interfaces (that is, WAN1 or WAN2), you enter the net-config [wan-ipv4] mode. First, specify the ISP connection type (you can select only a single type). Then, for the selected ISP connection type, configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. If you select a static ISP connection type, no further configuration is required.

Step 1	**Format**	**net wan wan ipv4 configure** *<wan interface>*
	Mode	net
Step 2	**Format**	**isp_connection_type** {**static** | **dhcp** | **pppoe** | **pptp**} **Yes** **isp_login_required** {**Y** | **N**} **static ip_address** *<ipaddress>* **static subnet_mask** *<subnet mask>* **static gateway_address** *<ipaddress>* **static primary_dns** *<ipaddress>* **static secondary_dns** *<ipaddress>*

```
dhcpc account_name <account name>
dhcpc domain_name <domain name>
dhcpc client_identifier {Y | N}
dhcpc vendor_identifier {Y | N}
dhcpc get_dns_from_isp {Y | N {dhcpc primary_dns <ipaddress>}
   [dhcpc secondary_dns <ipaddress>]}

pppoe username <user name>
pppoe password <password>
pppoe AccountName <account name>
pppoe DomainName <domain name>
pppoe connectivity_type {keepalive | idletimeout {pppoe idletime
   <minutes>}}
pppoe get_ip_dynamically {Y | N {pppoe static_ip <ipaddress>}
   {pppoe subnet_mask <subnet mask>}}
pppoe get_dns_from_isp {Y | N {pppoe primary_dns <ipaddress>}
   [pppoe secondary_dns <ipaddress>]}

pptp username <user name>
pptp password <password>
pptp AccountName <account name>
pptp DomainName <domain name>
pptp connectivity_type {keepalive | idletimeout
   {pptp idle_time <seconds>}}
pptp my_address <ipaddress>
pptp server_address <ipaddress>
pptp get_ip_dynamically {Y | N {pptp static_ip <ipaddress>}
   {pptp subnet_mask <subnet mask>}}
pppoe get_dns_from_isp {Y | N {pptp primary_dns <ipaddress>}
   [pptp secondary_dns <ipaddress>]}

connection_reset {N | Y {reset_hour <hour>} {reset_min <minutes>}
   {delay_in_reset <seconds>}}
```

Mode net-config [wan-ipv4]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
isp_connection_type	**static, dhcp, pppoe**, or **pptp**	Specifies the type of ISP connection. You can specify only one type of connection, and you must confirm your selection by typing **Yes** (that is, **Yes**, and not just **Y**): • **static**. Configure the keywords and parameters that are shown in the Static section of this table. • **dhcp**. Configure the keywords and parameters that are shown in the DHCPC section of this table. • **pppoe**. Configure the keywords and parameters that are shown in the PPPoE section of this table. • **pptp**. Configure the keywords and parameters that are shown in the PPTP section of this table.
	Yes	
isp_login_required	**Y** or **N**	If the type of ISP connection is PPPoE or PPTP, enforces the ISP login requirement or allows ISP access without login.
Static		
static ip_address	*ipaddress*	The static IP address.
static subnet_mask	*subnet mask*	The subnet mask that is associated with the static IP address.
static gateway_address	*ipaddress*	The IP address of the ISP gateway.
static primary_dns	*ipaddress*	The IP address of the primary DNS server.
static secondary_dns	*ipaddress*	The IP address of the optional secondary DNS server.
DHCPC		
dhcpc account_name	*account name*	The ISP account name (alphanumeric string).
dhcpc domain_name	*domain name*	The ISP domain name (alphanumeric string).
dhcpc client_identifier	**Y** or **N**	Enables or disables the DHCP client-identifier option. If enabled, the DHCP client-identifier is sent to the ISP server. By default, the option is not sent.
dhcpc vendor_identifier	**Y** or **N**	Enables or disables the DHCP vendor-class-identifier option. If enabled, the DHCP vendor-class-identifier is sent to the ISP server. By default, the option is not sent.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
dhcpc get_dns_from_isp	**Y** or **N**	Specifies whether or not the IP address of the DNS server is dynamically received from the ISP. If you select **N**, you must issue the **dhcpc primary_dns** keyword and enter the IP address of the primary DNS server. For a secondary DNS server, issue the **dhcpc secondary_dns** keyword, and enter the IP address.
dhcpc primary_dns	*ipaddress*	The IP address of the primary DNS server if your IP address is not dynamically received from the ISP.
dhcpc secondary_dns	*ipaddress*	The IP address of the optional secondary DNS server if your IP address is not dynamically received from the ISP.
PPPoE		
pppoe username	*user name*	The user name (alphanumeric string) to log in to the PPPoE service, if required.
pppoe password	*password*	The password (alphanumeric string) to log in to the PPPoE service, if required.
pppoe AccountName	*account name*	The PPPoE account name (alphanumeric string).
pppoe DomainName	*domain name*	The PPPoE domain name (alphanumeric string).
pppoe connectivity_type	**keepalive** or **idletimeout**	Specifies the type of PPPoE connection. If you select **idletimeout**, you must issue the **idle_time** keyword and enter the idle time-out in minutes.
pppoe idle_time	*minutes*	The idle time-out period in minutes, from 5 to 999 minutes.
pppoe get_ip_dynamically	**Y** or **N**	Specifies whether or not the IP address is dynamically received from the ISP. If you select **N**, you must issue the **pppoe static_ip** keyword and enter the static IP address, and issue the **pppoe subnet_mask** keyword and enter the subnet mask.
pppoe static_ip	*ipaddress*	The static IP address if your IP address is not dynamically received from the ISP.
pppoe subnet_mask	*subnet mask*	The subnet mask if your IP address is not dynamically received from the ISP.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
pppoe get_dns_from_isp	**Y** or **N**	Specifies whether or not the IP address of the DNS server is dynamically received from the ISP. If you select **N**, you must issue the pppoe **primary_dns** keyword and enter the IP address of the primary DNS server. For a secondary DNS server, issue the **pppoe secondary_dns** keyword, and enter the IP address.
pppoe primary_dns	*ipaddress*	The IP address of the primary DNS server if your IP address is not dynamically received from the ISP.
pppoe secondary_dns	*ipaddress*	The IP address of the optional secondary DNS server if your IP address is not dynamically received from the ISP.
PPTP		
pptp username	*user name*	The user name (alphanumeric string) to log in to the PPTP service, if required.
pptp password	*password*	The password (alphanumeric string) to log in to the PPTP service, if required.
pptp AccountName	*account name*	The PPPoE account name (alphanumeric string).
pptp DomainName	*domain name*	The PPPoE domain name (alphanumeric string).
pptp connectivity_type	**keepalive** or **idletimeout**	Specifies the type of PPTP connection. If you select **idletimeout**, you must issue the **pptp idle_time** keyword and enter the idle time-out period.
pptp idle_time	*minutes*	The idle time-out period in minutes (5 to 999), if the PPTP connection is configured for idle time-out.
pptp my_address	*ipaddress*	The IP address that was assigned by the ISP to make a connection with the ISP's PPTP server.
pptp server_address	*ipaddress*	The IP address of the PPTP server.
pptp get_ip_dynamically	**Y** or **N**	Specifies whether or not the IP address is dynamically received from the ISP. If you select **N**, you must issue the **pptp static_ip** keyword and enter the static IP address, and issue the **pptp subnet_mask** keyword and enter the subnet mask.
pptp static_ip	*ipaddress*	The static IP address if your IP address is not dynamically received from the ISP.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
pptp subnet_mask	*subnet mask*	The subnet mask if your IP address is not dynamically received from the ISP.
pptp get_dns_from_isp	**Y** or **N**	Specifies whether or not the IP address of the DNS server is dynamically received from the ISP. If you select **N**, you must issue the **pptp primary_dns** keyword and enter the IP address of the primary DNS server. For a secondary DNS server, issue the **pptp secondary_dns** keyword, and enter the IP address.
pptp primary_dns	*ipaddress*	The IP address of the primary DNS server if your IP address is not dynamically received from the ISP.
pptp secondary_dns	*ipaddress*	The IP address of the optional secondary DNS server if your IP address is not dynamically received from the ISP.
Connection Reset		
connection_reset	**Y** or **N**	Specifies whether or not the connection is automatically reset. If it is reset, you must issue the **reset_hour** and **reset_min** keywords and enter the hour and minutes after which the connection is reset. You also must issue the **delay_in_reset** keyword and enter the number of seconds of delay.
reset_hour	*hour*	The hour at which the connection is reset.
reset_min	*minutes*	The minutes at which the connection is reset.
delay_in_reset	*seconds*	After the connection resets, the number of seconds of delay before a connection attempt is made.

Command example:

```
FVS336Gv2> net wan wan ipv4 configure WAN2
net-config[wan-ipv4]> isp_connection_type dhcp
net-config[wan-ipv4]> dhcpc client_identifier Y
net-config[wan-ipv4]> dhcpc get_dns_from_isp N
net-config[wan-ipv4]> dhcpc primary_dns 10.124.56.118
net-config[wan-ipv4]> dhcpc secondary_dns 10.124.56.132
net-config[wan-ipv4]> save
```

Related show commands: *show net wan wan ipv4 setup <wan interface>* and *show net wan wan ipv4 status <wan interface>*

net wan wan ipv4 secondary_address add <wan interface>

This command configures a secondary IPv4 WAN address. After you issue the **net wan wan ipv4 secondary_address add** command to specify one of the two WAN interfaces (that is, WAN1 or WAN2), you enter the net-config [wan-secondary-address] mode and then you can configure the secondary WAN address and subnet mask in the order that you prefer.

Step 1	**Format**	**net lan ipv4 multi_homing add** {**WAN1** | **WAN2**}
	Mode	net
Step 2	**Format**	**ip_address** *<ipaddress>* **subnet_mask** *<subnet mask>*
	Mode	net-config [wan-secondary-address]

Keyword	Associated Parameter to Type	Description
ip_address	*ipaddress*	The secondary IPv4 address for the selected WAN interface.
subnet_mask	*subnet mask*	The subnet mask for the secondary IP address.

Command example:

```
FVS336Gv2> net wan wan ipv4 secondary_address add WAN2
net-config[wan-secondary-address]> ip_address 10.168.50.1
net-config[wan-secondary-address]> subnet_mask 255.255.255.0
net-config[wan-secondary-address]> save
```

Related show command: *show net wan wan ipv4 secondary_addresses <wan interface>*

---

net wan wan ipv4 secondary_address delete <row id>

This command deletes a secondary IPv4 WAN address by deleting its row ID.

Format	**net wan wan ipv4 secondary_address delete** *<row id>*
Mode	net

Related show command: *show net wan wan ipv4 secondary_addresses <wan interface>*

---

net wan_settings load_balancing configure

This command configures the load balancing settings for two WAN interfaces that are configured for IPv4. After you issue the **net wan_settings load_balancing configure** command, you enter the net-config [load-balancing] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the **wan_mode_type** keyword determines which other keywords and parameters you can apply.

Note: You can configure the load balancing settings only if the *net ipv6 ipmode configure* command is set to IPv4_Only.

Step 1 **Format** `net wan_settings load-balancing configure`

Mode net

Step 2 **Format**
```
wan_mode_type {Primary-WAN {primary_wan_interface {WAN1 | WAN2}}
{auto_rollover {N | Y {secondary_wan_interface
   {WAN1 | WAN2}}}} | Load-Balancing {loadbal_algo
   {Round-Robin | Weighted-LB}}}
```

Mode net-config [load-balancing]

Keyword	Associated Keyword to Select or Parameter to Type	Description
Common settings		
`wan_mode_type`	`Primary-WAN` or `Load-Balancing`	Specifies the load balancing settings: • **`Primary-WAN`**. One WAN interface is made the primary interface. The other three interfaces are disabled. As an option, another WAN interface can be made the rollover link. The remaining two interfaces are disabled. Configure the keywords and parameters that are shown in the Primary WAN mode and auto-rollover mode settings section of this table. • **`Load-Balancing`**. The VPN firewall distributes the outbound traffic equally among the WAN interfaces that are functional. Configure the keywords and parameters that are shown in the Load balancing settings section of this table, that is, issue the **`loadbal_algo`** keyword and specify the load balancing method.
Primary WAN mode and auto-rollover mode settings		
`primary_wan_interface`	`WAN1` or `WAN2`	Specifies the interface that functions as the primary WAN interface.
`auto_rollover`	`Y` or `N`	Enables or disables auto-rollover mode. Issue the **`secondary_wan_interface`** keyword to specify the secondary WAN interface.
`secondary_wan_interface`	`WAN1` or `WAN2`	The interface that functions as the secondary WAN interface if auto-rollover mode is enabled.

Keyword	Associated Keyword to Select or Parameter to Type	Description
Load balancing settings		
loadbal_algo	**Round-Robin** or **Weighted-LB**	Specifies the load balancing method: • **Round-robin**. With round-robin load balancing, new traffic connections are sent over a WAN link in a serial method irrespective of bandwidth or link speed. This load-balancing method ensures that a single WAN interface does not carry a disproportionate distribution of sessions. • **Weighted LB**. With weighted load balancing, balance weights are calculated based on WAN link speed and available WAN bandwidth. This is the most efficient load-balancing algorithm.

Command example:

```
FVS336Gv2> net wan_settings load_balancing configure WAN1
net-config[load-balancing]> wan_mode_type Primary-WAN
net-config[load-balancing]> primary_wan_interface WAN1
net-config[load-balancing]> auto_rollover Y
net-config[load-balancing]> secondary_wan_interface WAN2
net-config[load-balancing]> save
```

Related show command: *show net wan port_setup ipv4 <wan interface>*

net protocol_binding add

This command configures a new protocol binding, that is, it binds a service to a WAN interface. After you issue the **net protocol_binding add** command, you enter the net-config [protocol-binding] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**net protocol_binding add**
	Mode	net

Step 2 **Format**

```
service_name {default_services <default service name> |
   {custom_services <custom service name>}
local gateway {WAN1 | WAN2}
source_network_type {address_wise {ANY | SINGLE_ADDRESS
   {source_network_start_ip <ipaddress>} | ADDRESS_RANGE
   {source_network_start_ip <ipaddress>}
   {source_network_end_ip <ipaddress>}} | group_wise
   <group name>}
destination_network_type {address_wise {ANY | SINGLE_ADDRESS
   {destination_network_start_ip <ipaddress>} | ADDRESS_RANGE
   {destination_network_start_ip <ipaddress>}
   {destination_network_end_ip <ipaddress>}} | group_wise
   <group name>}
```

Mode net-config [protocol-binding]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the protocol binding applies.
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the protocol binding applies.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
local_gateway	**WAN1** or **WAN2**	Specifies the interface to which the service is bound.
source_network_type address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of LAN source address. The **address_wise** and **group_wise** keywords are mutually exclusive.
source_network_start_ip	*ipaddress*	The following two options are available: • The IP address if the **source_network_type address_wise** keywords are set to **SINGLE_ADDRESS**. • The start IP address if the **source_network_type address_wise** keywords are set to **ADDRESS_RANGE**.
source_network_end_ip	*ipaddress*	The end IP address if the **source_network_type address_wise** keywords are set to **ADDRESS_RANGE**.
source_network_type group_wise	*group name*	The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specify with the *net lan lan_groups edit <row id> <new group name>* command. The LAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.
destination_network_type address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN destination address. The **address_wise** and **group_wise** keywords are mutually exclusive.
destination_network_start_ip	*ipaddress*	The following two options are available: • The IP address if the **source_network_type address_wise** keywords are set to **SINGLE_ADDRESS**. • The start IP address if the **source_network_type address_wise** keywords are set to **ADDRESS_RANGE**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
destination_network_end_ip	*ipaddress*	The end IP address if the **source_network_type address_wise** keywords are set to **ADDRESS_RANGE**.
destination_network_type group_wise	*group name*	The name of the WAN IP group. The WAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.

Command example:

```
FVS336Gv2> net protocol_binding add
net-config[protocol-binding]> service_name default_services FTP
net-config[protocol-binding]> local_gateway WAN1
net-config[protocol-binding]> source_network_type address_wise ANY
net-config[protocol-binding]> destination_network_type address_wise SINGLE_ADDRESS
net-config[protocol-binding]> destination_network_start_ip 10.122.178.214
net-config[protocol-binding]> save
```

Related show command: *show net protocol_binding setup*

net protocol_binding edit <row id>

This command configures an existing protocol binding, that is, it binds a service to a WAN interface. After you issue the **net protocol_binding edit** command to specify the row to be edited, you enter the net-config [protocol-binding] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**net protocol_binding edit** *<row id>*
	Mode	net

Step 2 **Format**

```
service_name {default_services <default service name> |
   {custom_services <custom service name>}
local gateway {WAN1 | WAN2}
source_network_type {address_wise {ANY | SINGLE_ADDRESS
   {source_network_start_ip <ipaddress>} | ADDRESS_RANGE
   {source_network_start_ip <ipaddress>}
   {source_network_end_ip <ipaddress>}} | group_wise
   <group name>}
destination_network_type {address_wise {ANY | SINGLE_ADDRESS
   {destination_network_start_ip <ipaddress>} | ADDRESS_RANGE
   {destination_network_start_ip <ipaddress>}
   {destination_network_end_ip <ipaddress>}} | group_wise
   <group name>}
```

Mode net-config [protocol-binding]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the protocol binding applies.
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the protocol binding applies.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
local_gateway	**WAN1** or **WAN2**	Specifies the interface to which the service is bound.
source_network_type address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of LAN source address. The **address_wise** and **group_wise** keywords are mutually exclusive.
source_network_start_ip	*ipaddress*	The following two options are available: • The IP address if the **source_network_type address_wise** keywords are set to **SINGLE_ADDRESS**. • The start IP address if the **source_network_type address_wise** keywords are set to **ADDRESS_RANGE**.
source_network_end_ip	*ipaddress*	The end IP address if the **source_network_type address_wise** keywords are set to **ADDRESS_RANGE**.
source_network_type group_wise	*group name*	The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specify with the *net lan lan_groups edit <row id> <new group name>* command. The LAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.
destination_network_type address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN destination address. The **address_wise** and **group_wise** keywords are mutually exclusive.
destination_network_start_ip	*ipaddress*	The following two options are available: • The IP address if the **source_network_type address_wise** keywords are set to **SINGLE_ADDRESS**. • The start IP address if the **source_network_type address_wise** keywords are set to **ADDRESS_RANGE**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
destination_network_end_ip	*ipaddress*	The end IP address if the **source_network_type address_wise** keywords are set to **ADDRESS_RANGE**.
destination_network_type group_wise	*group name*	The name of the WAN IP group. The WAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.

Related show command: *show net protocol_binding setup*

net protocol_binding delete

This command deletes a protocol binding by deleting its row ID.

Format **net protocol_binding delete** *<row id>*

Mode net

Related show command: *show net protocol_binding setup*

net protocol_binding disable

This command disables a protocol binding by specifying its row ID.

Format **net protocol binding disable** *<row id>*

Mode security

Related show command: *show net protocol_binding setup*

net protocol_binding enable

This command enables a protocol binding by specifying its row ID.

Format **net protocol binding enable** *<row id>*

Mode security

Related show command: *show net protocol_binding setup*

IPv6 WAN Commands

This section describes the following commands:

- *net ipv6 ipmode configure*
- *net wan wan ipv6 configure <wan interface>*
- *net siit configure*

net ipv6 ipmode configure

This command configures the IPv6 mode. After you issue the **net ipv6 ipmode configure** command, you enter the net-config [mode] mode and then you can configure the IP mode. You can select support for IPv4 only or for both IPv4 and IPv6.



WARNING:

Changing the IP mode causes the VPN firewall to reboot.

Step 1	**Format**	**net ipv6 ipmode configure**
	Mode	net
Step 2	**Format**	**ip_type** {**IPv4_Only** | **IPv4/IPv6**}
	Mode	net-config [mode]

Keyword	Associated Keyword to Select	Description
ip_type	**IPv4_Only** or **IPv4/IPv6**	Specifies the IPv6 routing mode.

Command example:

```
FVS336Gv2> net ipv6 ipmode configure
net-config[mode]> ip_type IPv4/IPv6
net-config[mode]> save
```

Related show command: *show net ipv6 ipmode setup*

net wan wan ipv6 configure <wan interface>

This command configures the IPv6 settings for a WAN interface. After you issue the **net wan wan ipv6 configure** command to specify one of the two WAN interfaces (that is, WAN1 or WAN2), you enter the net-config [wan-ipv6] mode. First, specify the ISP connection type (you can select only a single type). Then, for the selected ISP connection type, configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1 **Format** `net wan wan ipv6 configure`

Mode net

Step 2 **Format** `isp type {STATIC | DHCPC | PPPoE}`

```
static ip_address <ipv6-address>
static prefix <prefix-length>
static gateway_address <ipv6-address>
static primary_dns <ipv6-address>
static secondary_dns <ipv6-address>

dhcpc stateless_mode_enable {StatelessAddrAutoConfig
[prefix_delegation_enable {Y | N}] | StatefulAddrAutoConfig}

pppoe user_name <user name>
pppoe password <password>
pppoe dhcpv6_option {Disable-DHCPv6 {pppoe primary_dns
   <ipv6-address>} {pppoe secondary_dns <ipv6-address>} |
   DHCPv6-StatelessMode | DHCPv6-StatefulMode |
   DHCPv6-Prefix-Delegation}
```

Mode net-config [wan-ipv6]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
`isp type`	**STATIC**, **DHCPC**, or **PPPoE**	Specifies the type of ISP connection: • **STATIC**. Configure the keywords and parameters that are shown in the Static section of this table. • **DHCPC**. Configure the keywords and parameters that are shown in the DHCPC section of this table. • **PPPoE**. Configure the keywords and parameters that are shown in the PPPoE section of this table.
Static		
`static ip_address`	*ipv6-address*	The IPv6 address of the WAN interface.
`static prefix`	*prefix-length*	The prefix length (integer) for the static address.
`static gateway_address`	*ipv6-address*	The IPv6 address of the gateway.
`static primary_dns`	*ipv6-address*	The IPv6 address of the primary DNS server.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
static secondary_dns	*ipv6-address*	The IPv6 address of the secondary DNS server.
DHCPC		
dhcpc stateless_mode_enable	**StatelessAddrAutoConfig** or **StatefulAddrAutoConfig**	Specifies the type of DHCPv6 mode (stateless or stateful). If you set the **dhcpc stateless_mode_enable** keywords to **StatelessAddrAutoConfig**, you have the option to set the **dhcpc prefix_delegation_enable** keywords and associated parameter.
prefix_delegation_enable	**Y** or **N**	Enables or disables prefix delegation if the **dhcpc stateless_mode_enable** keywords are set to **StatelessAddrAutoConfig**. Prefix delegation allows the ISP's stateful DHCPv6 server to assign a prefix.
PPPoE		
pppoe user_name	*user name*	The PPPoE user name that is provided by the ISP.
pppoe password	*password*	The PPPoE password that is provided by the ISP.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
pppoe dhcpv6_option	**Disable-DHCPv6**, **DHCPv6-StatelessMode**, **DHCPv6-StatefulMode**, or **DHCPv6-Prefix-Delegation**	Specifies the DHCPv6 server options for the PPPoE configuration: • **Disable-DHCPv6**. DHCPv6 is disabled. You must issue the **pppoe primary_dns** and **pppoe secondary_dns** keywords and specify DNS servers to receive an IP address from the ISP. • **DHCPv6-StatelessMode**. The VPN firewall generates its own IP address by using a combination of locally available information and router advertisements, but receives DNS server information from the ISP's DHCPv6 server. Router advertisements include a prefix that identifies the subnet that is associated with the WAN port. The IP address is formed by combining this prefix and the MAC address of the WAN port. The IP address is a dynamic address. • **DHCPv6-StatefulMode**. The VPN firewall obtains an interface address, configuration information such as DNS server information, and other parameters from the ISP's DHCPv6 server. The IP address is a dynamic address. • **DHCPv6-Prefix-Delegation**. The VPN firewall obtains a prefix from the ISP's DHCPv6 server through prefix delegation. The VPN firewall's own stateless DHCPv6 server can assign this prefix to its IPv6 LAN clients.
pppoe primary_dns	*ipv6-address*	The IPv6 address of the primary DNS server if the DHCPv6 server option is **Disable-DHCPv6**.
pppoe secondary_dns	*ipv6-address*	The IPv6 address of the secondary DNS server if the DHCPv6 server option is **Disable-DHCPv6**.

Command example:

```
FVS336Gv2> net wan wan ipv6 configure WAN2
net-config[wan-ipv6]> isp type DHCPC
net-config[wan-ipv6]> dhcpc stateless_mode_enable StatelessAddrAutoConfig
net-config[wan-ipv6]> prefix_delegation_enable Y
net-config[wan-ipv6]> save
```

Related show commands: *show net wan wan ipv6 setup <wan interface>* and *show net wan wan ipv6 status <wan interface>*

---

net siit configure

This command enables and configures Stateless IP/ICMP Translation (SIIT). After you issue the **`net siit configure`** command, you enter the net-config [siit] mode and then you can enable SIIT and configure the IPv4 address.

Step 1	**Format**	**`net siit configure`**
	Mode	net
Step 2	**Format**	**`enable`** {**`Y`** | **`N`**} **`ipv4_address`** *<ipaddress>*
	Mode	net-config [siit]

Keyword	Associated Keyword to Select or Parameter to Type	Description
`enable`	**`Y`** or **`N`**	Enables or disables SIIT.
`ipv4_address`	*`subnet mask`*	The IPv4 address for the SIIT configuration.

Command example:

```
FVS336Gv2> net siit configure
net-config[siit]> enable Y
net-config[siit]> ipv4_address 192.168.5.117
net-config[siit]> save
```

Related show command: *show net siit setup*

IPv6 Tunnel Commands

This section describes the following commands:

- *net ipv6_tunnel isatap add*
- *net ipv6_tunnel isatap edit <row id>*
- *net ipv6_tunnel isatap delete <row id>*
- *net ipv6_tunnel six_to_four configure*

net ipv6_tunnel isatap add

This command configures a new ISATAP tunnel. After you issue the **net ipv6_tunnel isatap add** command, you enter the net-config [isatap-tunnel] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Note: To be able to configure an ISATAP tunnel, you first must set the IP mode to **IPv4/IPv6** (see the *net ipv6 ipmode configure* command).

Step 1	**Format**	**net ipv6_tunnel isatap add**
	Mode	net
Step 2	**Format**	**subnet_prefix** <*subnet prefix*> **end_point_type** {**LAN** | **Other_IP** {**ipv4_address** <*address*>}}
	Mode	net-config [isatap-tunnel]

Keyword	Associated Keyword to Select or Parameter to Type	Description
subnet_prefix	*subnet prefix*	The IPv6 64-bit subnet prefix (string) that is assigned to the logical ISATAP subnet for this intranet.
end_point_type	**LAN** or **Other_IP**	Specifies the local endpoint IP address for the tunnel that is initiated on the VPN firewall. The endpoint can be the LAN interface or a specific LAN IPv4 address. If you select **Other_IP**, you also must issue the **ipv4_address** keyword to specify an IPv4 address.
ipv4_address	*ipaddress*	The IPv4 address of a local endpoint that is not a LAN IPv4 address.

Command example:

```
FVS336Gv2> net ipv6_tunnel isatap add
net-config[isatap-tunnel]> subnet_prefix 2004::
net-config[isatap-tunnel]> end_point_type Other_IP
net-config[isatap-tunnel]> ipv4_address 10.29.33.4
net-config[isatap-tunnel]> save
```

Related show commands: *show net ipv6_tunnel setup* and *show net ipv6_tunnel status*

net ipv6_tunnel isatap edit <row id>

This command configures an existing ISATAP tunnel. After you issue the **net ipv6_tunnel isatap edit** command to specify the row to be edited, you enter the net-config [isatap-tunnel] mode and then you can change one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**net ipv6_tunnel isatap edit** *<row id>*
	Mode	net
Step 2	**Format**	**subnet_prefix** *<subnet prefix>* **end_point_type** {**LAN** | **Other_IP** {**ipv4_address** *<address>*}}
	Mode	net-config [isatap-tunnel]

Keyword	Associated Keyword to Select or Parameter to Type	Description
subnet_prefix	*subnet prefix*	The IPv6 64-bit subnet prefix (string) that is assigned to the logical ISATAP subnet for this intranet.
end_point_type	**LAN** or **Other_IP**	Specifies the local endpoint IP address for the tunnel that is initiated on the VPN firewall. The endpoint can be the LAN interface or a specific LAN IPv4 address. If you select **Other_IP**, you also must issue the **ipv4_address** keyword to specify an IPv4 address.
ipv4_address	*ipaddress*	The IPv4 address of a local endpoint that is not a LAN IPv4 address.

Related show commands: *show net ipv6_tunnel setup* and *show net ipv6_tunnel status*

net ipv6_tunnel isatap delete <row id>

This command deletes an ISATAP tunnel by deleting its row ID.

Note: Before you can delete an ISATAP tunnel, you first must set the IP mode to **IPv4/IPv6** (see the *net ipv6 ipmode configure* command).

Format	**net ipv6_tunnel isatap delete** *<row id>*
Mode	net

Related show commands: *show net ipv6_tunnel setup* and *show net ipv6_tunnel status*

net ipv6_tunnel six_to_four configure

This command enables or disables automatic tunneling, which allows traffic from an IPv6 LAN to be tunneled through an IPv4 WAN to reach an IPv6 network. After you issue the **net ipv6_tunnel six_to_four configure** command, you enter the net-config [six-to-four-tunnel] mode and then you can configure automatic tunneling.

Step 1	**Format**	**net ipv6_tunnel six_to_four configure**
	Mode	net
Step 2	**Format**	**automatic_tunneling_enable** {**Y** | **N**}
	Mode	net-config [six-to-four-tunnel]

Keyword	Associated Keyword to Select	Description
automatic_tunneling_enable	**Y** or **N**	Enables or disables automatic tunneling.

Command example:

```
FVS336Gv2> net ipv6_tunnel six_to_four configure
net-config[six-to-four-tunnel]> automatic_tunneling_enable Y
net-config[six-to-four-tunnel]> save
```

Related show commands: *show net ipv6_tunnel setup* and *show net ipv6_tunnel status*

Dynamic DNS Command

This section describes the **net ddns configure** command.

net ddns configure

This command enables, configures, or disables Dynamic DNS (DDNS) service. After you issue the **net ddns configure** command, you enter the net-config [ddns] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. Before you specify a keyword, you must specify the WAN interface to which the configuration applies.

Step 1	**Format**	**net ddns configure**
	Mode	net

Step 2 **Format** {wan1 | wan2} enable {Disable | DynDNS | TZO | DNS_Oray | 3322_DDNS}
{wan1 | wan2} hostname <*host name*>
{wan1 | wan2} username <*user name*>
{wan1 | wan2} password <*password*>
{wan1 | wan2} wild_flag_enable {Y | N}
{wan1 | wan2} time_update_enable {Y | N}

Mode net-config [ddns]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
{wan1 | wan2} enable	**Disable**, **DynDNS**, **TZO**, **DNS_Oray**, or **3322_DDNS**	Specifies whether DDNS is disabled or enabled with a particular service. Use the **Disable** keyword to disable DDNS after you have first enabled the service. The other keywords represent DDNS service providers and are self-explanatory.
{wan1 | wan2} hostname	*host name*	Configures a host name (string) for a DDNS server.
{wan1 | wan2} username	*user name*	Configures a user name (string) for a DDNS server.
{wan1 | wan2} password	*password*	Configures a password (string) for a DDNS server.
{wan1 | wan2} wild_flag_enable	**Y** or **N**	Enables or disables the use of wildcards for DDNS.
{wan1 | wan2} time_update_enable	**Y** or **N**	Enables or disables the automatic update of the DDNS service after 30 days.

Command example:

```
FVS336Gv2> net ddns configure
net-config[ddns]> wan2 enable DynDNS
net-config[ddns]> wan2 hostname adminnetgear.dyndns.org
net-config[ddns]> wan2 username jaybrown
net-config[ddns]> wan2 password 4hg!RA278s
net-config[ddns]> wan2 wild_flag_enable N
net-config[ddns]> wan2 time_update_enable Y
net-config[ddns]> save
```

Related show command: *show net ddns setup*

IPv4 LAN Commands

This section describes the following commands:

- *net lan ipv4 configure <vlan id>*
- *net lan ipv4 delete <vlan id>*
- *net lan ipv4 disable <vlan id>*
- *net lan ipv4 enable <vlan id>*
- *net ethernet configure <interface name or number>*
- *net lan ipv4 default_vlan*
- *net lan ipv4 advanced configure*
- *net lan dhcp reserved_ip configure <mac address>*
- *net lan dhcp reserved_ip delete <mac address>*
- *net lan lan_groups edit <row id> <new group name>*
- *net lan ipv4 multi_homing add*
- *net lan ipv4 multi_homing edit <row id>*
- *net lan ipv4 multi_homing delete <row id>*
- *net lan ipv4 traffic_meter configure <ip address>*
- *net lan ipv4 traffic_meter delete <row id>*

net lan ipv4 configure <vlan id>

This command configures a new or existing VLAN, that is, a VLAN ID and a VLAN profile. After you issue the **`net lan ipv4 configure`** command to specify a new or existing VLAN ID, you enter the net-config [lan-ipv4] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**`net lan ipv4 configure`** *<vlan id>*
	Mode	net
Step 2	**Format**	**`profile_name`** *<name>* **`port_membership`** {[**`port 1`** {**`Y`** | **`N`**}] | [**`port 2`** {**`Y`** | **`N`**}] | [**`port 3`** {**`Y`** | **`N`**}] | [**`port 4`** {**`Y`** | **`N`**}]} **`static address`** *<ipaddress>* **`static subnet_mask`** *<subnet mask>* **`dhcp dhcp_mode`** {**`None`** | **`DHCP-Server`** | **`DHCP-Relay`**} **`proxy dns_enable`** {**`Y`** | **`N`**} **`inter_vlan_routing`** {**`Y`** | **`N`**}

```
dhcp domain_name <domain name>
dhcp start_address <ipaddress>
dhcp end_address <ipaddress>
dhcp primary_dns <ipaddress>
dhcp secondary_dns <ipaddress>
dhcp wins_server <ipaddress>
dhcp lease_time <hours>
enable_ldap {Y | N}
ldap_serverip <ipaddress>
ldap_search_base <search base>
ldap_port <number>

dhcp relay_gateway <ipaddress>
```

Mode net-config [lan-ipv4]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
profile_name	*name*	The name of the VLAN profile.
port_membership port1	**Y** or **N**	Specifies whether or not the port is a member of the VLAN. You must specify each port individually.
port_membership port2		
port_membership port3		
port_membership port4		
static address	*ipaddress*	The static IPv4 address for the VLAN.
static subnet_mask	*subnet mask*	The IPv4 subnet mask for the VLAN profile.
dhcp dhcp_mode	**None**, **DHCP-Server**, or **DHCP-Relay**	Specifies the DHCP mode for the devices that are connected to the VLAN: • **None**. The DHCP server is disabled. No further DHCP configuration is required. • **DHCP-Server**. Configure the keywords and parameters that are shown in the DHCP server section of this table. • **DHCP-Relay**. Configure the keywords and parameters that are shown in the DHCP relay section of this table.
proxy dns_enable	**Y** or **N**	Enables or disables the LAN DNS proxy.
inter_vlan_routing	**Y** or **N**	Enables or disables inter-VLAN routing.
DHCP server		
dhcp domain_name	*domain name*	The FQDN or domain name of the DHCP server.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
dhcp start_address	*ipaddress*	The start IP address for the DHCP address range.
dhcp end_address	*ipaddress*	The end IP address for the DHCP address range.
dhcp primary_dns	*ipaddress*	The IP address of the primary DNS server for the DHCP server.
dhcp secondary_dns	*ipaddress*	The IP address of the secondary DNS server for the DHCP server.
dhcp wins_server	*ipaddress*	The IP address of the WINS server for the DHCP server.
dhcp lease_time	*hours*	The DHCP lease time in hours.
enable_ldap	**Y** or **N**	Enables or disables LDAP.
ldap_serverip	*ipaddress*	The IP address of the LDAP server.
ldap_search_base	*search base*	The search base (string) for LDAP
ldap_port	*number*	The port number for the LDAP server.
DHCP relay		
dhcp relay_gateway	*ipaddress*	The IP address of the DHCP relay gateway.

Command example:

```
FVS336Gv2> net lan ipv4 configure 4
net-config[lan-ipv4]> profile_name Marketing
net-config[lan-ipv4]> port_membership port 1 Y
net-config[lan-ipv4]> port_membership port 3 Y
net-config[lan-ipv4]> port_membership port 4 Y
net-config[lan-ipv4]> static address 192.168.1.1
net-config[lan-ipv4]> static subnet_mask 255.255.255.0
net-config[lan-ipv4]> dhcp dhcp_mode DHCP-Relay
net-config[lan-ipv4]> dhcp relay_gateway 10.172.214.198
net-config[lan-ipv4]> proxy dns_enable N
net-config[lan-ipv4]> inter_vlan_routing Y
net-config[lan-ipv4]> save
```

Related show command: *show net lan ipv4 setup*

net lan ipv4 delete <vlan id>

This command deletes a VLAN by deleting its ID. You cannot delete VLAN 1, the default VLAN.

Format	**net lan ipv4 delete** *<vlan id>*
Mode	net

Related show command: *show net lan ipv4 setup*

---

net lan ipv4 disable <vlan id>

This command disables a VLAN by specifying its ID. You cannot disable VLAN 1, the default VLAN.

Format	**net lan ipv4 disable** *<vlan id>*
Mode	net

Related show command: *show net lan ipv4 setup*

---

net lan ipv4 enable <vlan id>

This command enables a VLAN by specifying its ID. VLAN 1, the default VLAN, is always enabled.

Format	**net lan ipv4 enable** *<vlan id>*
Mode	net

Related show command: *show net lan ipv4 setup*

---

net ethernet configure <interface name or number>

This command configures a VLAN for a LAN interface. After you issue the **net ethernet configure** command to specify a LAN interface, you enter net-config [ethernet] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**net ethernet configure** *<interface name* or number>
	Mode	net

Step 2	**Format**	**vlanid** *<number>* **vlan-enable** {**Y** | **N**} **native-vlan** {**Y** | **N**}
	Mode	net-config [ethernet]

Keyword	Associated Keyword to Select or Parameter to Type	Description
vlanid	*number*	The VLAN ID.
vlan-enable	**Y** or **N**	Enables or disables the VLAN for this interface.
native-vlan	**Y** or **N**	Enables or disables the default (native) VLAN for this interface.

Command example:

```
FVS336Gv2> net ethernet configure eth0
net-config[ethernet]> vlanid 12
net-config[ethernet]> vlan-enable Y
net-config[ethernet]> native-vlan N
net-config[ethernet]> save
```

Note: To enter the net-config [ethernet] mode, you can issue the **net ethernet configure** command with either an interface name such as **eth0** or an interface number such as **0**.

Related show command: *show net ethernet*

net lan ipv4 default_vlan

This command configures the default VLAN for each port. After you issue the **net lan ipv4 default_vlan** command, you enter the net-config [lan-ipv4-defvlan] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**net lan ipv4 default_vlan**
	Mode	net
Step 2	**Format**	**port1** *<vlan name>* **port2** *<vlan name>* **port3** *<vlan name>* **port4** *<vlan name>*
	Mode	net-config [lan-ipv4-defvlan]

Keyword	Associated Parameter to Type	Description
port1	*vlan name*	Specifies the default VLAN name. You must specify the name for each port individually.
port2		
port3		
port4		

Command example:

```
FVS336Gv2> net lan ipv4 default_vlan
net-config[lan-ipv4-defvlan]> port1 Default
net-config[lan-ipv4-defvlan]> port2 Default
net-config[lan-ipv4-defvlan]> port3 Management
net-config[lan-ipv4-defvlan]> port4 Sales
net-config[lan-ipv4-defvlan]> save
```

Related show command: *show net lan ipv4 setup*

net lan ipv4 advanced configure

This command configures advanced LAN settings such as the MAC address for VLANs and ARP broadcast. After you issue the **net lan ipv4 advanced configure** command, you enter the net-config [lan-ipv4-adv] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**net lan ipv4 advanced configure**
	Mode	net
Step 2	**Format**	**vlan_mac_offset_type** {**Same** | **Unique**} **enable_arp_broadcast** {**Y** | **N**}
	Mode	net-config [lan-ipv4-adv]

Keyword	Associated Keyword to Select	Description
vlan_mac_offset_type	**Same** or **Unique**	Specifies the MAC address for VLANs: • **Same**. All VLAN profiles use the same MAC address as the LAN ports. (All LAN ports share the same MAC address.) • **Unique**. Each VLAN (up to 16 VLANs) is assigned a unique MAC address.
enable_arp_broadcast	**Y** or **N**	Enables or disables the broadcast of ARP packets.

Command example:

```
FVS336Gv2> net lan ipv4 advanced configure
net-config[lan-ipv4-adv]> vlan_mac_offset_type Same
```

```
net-config[lan-ipv4-adv]> enable_arp_broadcast Y
net-config[lan-ipv4-adv]> save
```

Related show command: *show net lan ipv4 advanced setup*

net lan dhcp reserved_ip configure <mac address>

This command binds a MAC address to an IP address for DHCP reservation or lets you edit an existing binding. The command also assigns the device or computer to which the MAC address belongs to one of eight LAN groups. After you issue the **net lan dhcp reserved_ip configure** command to configure the MAC address, you enter the net-config [dhcp-reserved-ip] mode and then you can configure the IP address for the binding configuration.

Step 1	**Format**	**net lan dhcp reserved_ip configure** *<mac address>*
	Mode	net
Step 2	**Format**	**ip_mac_name** *<device name>* **ip_addr_type** {**Fixed_set_on_PC** | **Dhcp_Reserved_IP**} **ip_address** *<ipaddress>* **group_name** {**Group1** | **Group2** | **Group3** | **Group4** | **Group5** | **Group6** | **Group7** | **Group8** | *<custom group name>*} **vlan_profile** *<vlan name>*
	Mode	net-config [dhcp-reserved-ip]

Keyword	Associated Keyword to Select or Parameter to Type	Description
ip_mac_name	*device name*	The name of the computer or device.
ip_addr_type	**Fixed_set_on_PC** or **Dhcp_Reserved_IP**	Specifies the IP address type: • **Fixed_set_on_PC**. The IP address is statically assigned on the computer or device. • **Dhcp_Reserved_IP**. The DHCP server of the wireless VPN firewall always assigns the specified IP address to this client during the DHCP negotiation.
ip_address	*ipaddress*	The IP address to be bound to the specified MAC address. The IP address must be in the IP subnet of the VLAN to which the computer or device is assigned.
group_name	**Group1**, **Group2**, **Group3**, **Group4**, **Group5**, **Group6**, **Group7**, or **Group8**, or *custom group name*	Specifies the group to which the computer or device must be assigned. You can also enter a custom group name that you specify with the *net lan lan_groups edit <row id> <new group name>* command.
vlan_profile	*vlan name*	The name of the VLAN to which the computer or device must be assigned.

Command example:

```
FVS336Gv2> net lan dhcp reserved_ip configure AA:BB:CC:1A:2B:3C
net-config[dhcp-reserved-ip]> ip_addr_type Dhcp_Reserved_IP
net-config[dhcp-reserved-ip]> ip_address 192.168.27.219
net-config[dhcp-reserved-ip]> group_name Group3
net-config[dhcp-reserved-ip]> vlan_profile Default
net-config[dhcp-reserved-ip]> save
```

Related show commands: *show net lan dhcp reserved_ip setup* and *show net lan dhcp leased_clients list*

---

net lan dhcp reserved_ip delete <mac address>

This command deletes the binding of a MAC address to an IP address.

Format	**net lan dhcp reserved_ip delete** *<mac address>*
Mode	net

Related show commands: *show net lan dhcp reserved_ip setup* and *show net lan dhcp leased_clients list*

---

net lan lan_groups edit <row id> <new group name>

This command specifies an IPv4 LAN group name, that is, it changes a default group name such as Group1, Group2, or Group3. You must specify both the row id that represents the group (for example, 2 for Group2, or 5 for Group5) and the new name for the group.

Format	**net lan lan_group edit <**row id**>** <new *group name*>
Mode	net

Related show command: *show net lan lan_groups*

---

net lan ipv4 multi_homing add

This command configures a new IPv4 alias, that is, a secondary IPv4 address. After you issue the **net lan ipv4 multi_homing add** command, you enter the net-config [lan-ipv4-multihoming] mode and then you can configure the secondary address and subnet mask in the order that you prefer.

Step 1	**Format**	**net lan ipv4 multi_homing add**
	Mode	net

Step 2	**Format**	**ip_address** *<ipaddress>* **subnet_mask** *<subnet mask>*
	Mode	net-config [lan-ipv4-multihoming]

Keyword	Associated Parameter to Type	Description
ip_address	*ipaddress*	The secondary IPv4 address for the LAN.
subnet_mask	*subnet mask*	The subnet mask for the secondary IPv4 address.

Command example:

```
FVS336Gv2> net lan ipv4 multi_homing add
net-config[lan-ipv4-multihoming]> ip_address 192.168.16.110
net-config[lan-ipv4-multihoming]> subnet_mask 255.255.255.248
net-config[lan-ipv4-multihoming]> save
```

Related show command: *show net lan ipv4 multiHoming*

net lan ipv4 multi_homing edit <row id>

This command configures an existing IPv4 alias, that is, a secondary IPv4 address. After you issue the **net lan ipv4 multi_homing edit** command to specify the row to be edited, you enter the net-config [lan-ipv4-multihoming] mode and then you can configure the secondary address and subnet mask in the order that you prefer.

Step 1	**Format**	**net lan ipv4 multi_homing edit**
	Mode	net
Step 2	**Format**	**ip_address** *<ipaddress>* **subnet_mask** *<subnet mask>*
	Mode	net-config [lan-ipv4-multihoming]

Keyword	Associated Parameter to Type	Description
ip_address	*ipaddress*	The secondary IPv4 address for the LAN.
subnet_mask	*subnet mask*	The subnet mask for the secondary IPv4 address.

Related show command: *show net lan ipv4 multiHoming*

net lan ipv4 multi_homing delete <row id>

This command deletes a secondary IPv4 address by specifying its row ID.

Format	**net lan ipv4 multi_homing delete** *<row id>*
Mode	net

Related show command: *show net lan ipv4 multiHoming*

---

net lan ipv4 traffic_meter configure <ip address>

This command configures a LAN traffic meter profile for an IP address. When the traffic limit is reached, further traffic for that IP address is blocked. After you issue the **net lan ipv4 traffic_meter configure** command to specify the IP address, you enter the net-config [lan-ipv4-traffic-meter] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**net lan ipv4 traffic_meter configure** *<ip address>*
	Mode	net
Step 2	**Format**	**direction** {**Downloadonly** | **BothDirections**} **limit** *<number>* **counter** {**RestartCounter** | **SpecificTime** {**day_of_month** *<day>*} {**time_hour** *<hour>*} {**time_meridiem** {**AM** | **PM**}} {**time_minute** *<minute>*}} **send_email_report** {**Y** | **N**} **send_email_alert** {**Y** | **N**}
	Mode	net-config [lan-ipv4-traffic-meter]

Keyword	Associated Keyword to Select or Parameter to Type	Description
Traffic meter configuration		
direction	**Downloadonly** or **BothDirections**	Specifies the type of traffic limit: • **Downloadonly**. The traffic limit applies to downloaded traffic only. • **BothDirections**. The traffic limit applies to both downloaded and uploaded traffic.
limit	*number*	The limit for the traffic meter in MB. The maximum limit that you can enter is 256,000 MB (about 250 GB).

Keyword	Associated Keyword to Select or Parameter to Type	Description
Traffic counter configuration		
counter	**SpecificTime** or **RestartCounter**	Specifies how the traffic counter is restarted: • **SpecificTime**. Restarts the traffic counter on a specific day and time. You must set the **day_of_month**, **time_hour**, **time_meridiem**, and **time_minute** keywords and associated parameters. • **RestartCounter**. Restarts the traffic counter after you save the command.
day_of_month	*day*	The day in the format DD (01 to 31) that the traffic counter restarts. This keyword applies only if you set the **counter** keyword to **SpecificTime**.
time_hour	*hour*	The hour in the format HH (00 to 12) that the traffic counter restarts. This keyword applies only if you set the **counter** keyword to **SpecificTime**.
time_meridiem	**AM** or **PM**	Specifies the meridiem for the hour that the traffic counter restarts. This keyword applies only if you set the **counter** keyword to **SpecificTime**.
time_minute	*minutes*	The minutes in the format MM (00 to 59) that the traffic counter restarts. This keyword applies only if you set the **counter** keyword to **SpecificTime**.
send_email_report	**Y** or **N**	Specifies whether or not an email report is sent when the traffic counter restarts.
Action when limit is reached		
send_email_alert	**Y** or **N**	Specifies whether or not an email alert is sent when the traffic limit is reached and further traffic is blocked.

Command example:

```
FVS336Gv2> net lan ipv4 traffic_meter configure 192.168.11.204
net-config[lan-ipv4-traffic-meter]> direction BothDirections
net-config[lan-ipv4-traffic-meter]> limit 45000
net-config[lan-ipv4-traffic-meter]> counter RestartCounter
```

```
net-config[lan-ipv4-traffic-meter]> send_email_report N
net-config[lan-ipv4-traffic-meter]> send_email_alert N
net-config[lan-ipv4-traffic-meter]> save
```

Related show commands: *show net lan ipv4 traffic_meter setup* and *show net lan ipv4 traffic_meter detailed_setup <row id>*

---

net lan ipv4 traffic_meter delete <row id>

This command deletes a LAN traffic meter profile by specifying its row ID.

Format	**net lan ipv4 traffic_meter delete** *<row id>*
Mode	net

Related show command: *show net lan ipv4 traffic_meter setup*

IPv6 LAN Commands

This section describes the following commands:

- *net lan ipv6 configure*
- *net lan ipv6 pool add*
- *net lan ipv6 pool edit <row id>*
- *net lan ipv6 pool delete <row id>*
- *net lan ipv6 multi_homing add*
- *net lan ipv6 multi_homing edit <row id>*
- *net lan ipv6 multi_homing delete <row id>*
- *net radvd configure lan*
- *net radvd pool lan add*
- *net radvd pool lan edit <row id>*
- *net radvd pool lan delete <row id>*
- *net lan ipv6 prefix_delegation add*
- *net lan ipv6 prefix_delegation edit <row id>*
- *net lan ipv6 prefix_delegation delete <row id>*

net lan ipv6 configure

This command configures the IPv6 LAN address settings and DHCPv6. After you issue the **net lan ipv6 configure** command, you enter the net-config [lan-ipv6] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1

Format **net lan ipv6 configure**

Mode net

Step 2

Format

```
static address <ipv6-address>
static prefix_length <prefix length>
dhcp server_enable {N | Y {dhcp mode {Stateless | Stateful}}}
dhcp prefix_delegation_enable {Y | N}
dhcp domain name <domain name>
dhcp server_preference <number>
dhcp dns_type {useDnsProxy | useDnsFromISP | useEnteredDns
   {dhcp primary_dns <ipv6-address>} [dhcp secondary_dns
   <ipv6-address>]}
dhcp rebind_time <seconds>
```

Mode net-config [lan-ipv6]

Keyword (consists of two separate words)	Associated Keyword to Select or Parameter to Type	Description
static address	*ipv6-address*	The link-local IPv6 address.
static prefix_length	*prefix length*	The IPv6 prefix length (integer) of the link-local IPv6 address.
dhcp server_enable	**Y** or **N**	Enables or disables DHCPv6. If you enable DHCPv6, you also must issue the **dhcp mode** keywords to specify a stateless or stateful DCHPv6 server and configure the server.
dhcp mode	**Stateless** or **Stateful**	Specifies the DHCPv6 mode (stateless or stateful).
dhcp prefix_delegation_enable	**Y** or **N**	Enables or disables prefix delegation. This option is available only if the **dhcp mode** keywords are set to **Stateless**. For information about how to configure prefixes, see the *net lan ipv6 prefix_delegation add* command.
dhcp domain_name	*domain name*	The server domain name (string) or FQDN for the DHCP server.
dhcp server_preference	*number*	The preference number (integer) of the DHCP server.

Keyword (consists of two separate words)	Associated Keyword to Select or Parameter to Type	Description
dhcp dns_type	**useDnsProxy**, **useDnsFromISP**, or **useEnteredDns**	Specifies the DNS server type. If you select **useEnteredDns**, you also must issue the **dhcp primary_dns** keyword and associated parameter. The **dhcp secondary_dns** keyword and associated parameter are optional.
dhcp primary_dns	*ipv6-address*	The IPv6 address for the primary DNS server in the DHCP configuration if the **dhcp dns_type** keywords are set to **useEnteredDns**.
dhcp secondary_dns	*ipv6-address*	The IPv6 address for the secondary DNS server in the DHCP configuration if the **dhcp dns_type** keywords are set to **useEnteredDns**.
dhcp rebind_time	*seconds*	The lease time in seconds (integer), from 0 to 604800 seconds.

Command example:

```
FVS336Gv2> net lan ipv6 configure
net-config[lan-ipv6]> static address fec0::3
net-config[lan-ipv6]> static prefix_length 64
net-config[lan-ipv6]> dhcp server_enable Y
net-config[lan-ipv6]> dhcp mode Stateless
net-config[lan-ipv6]> dhcp prefix_delegation_enable Y
net-config[lan-ipv6]> dhcp domain name netgear.com
net-config[lan-ipv6]> dhcp server_preference 236
net-config[lan-ipv6]> dhcp dns_type useDnsProxy
net-config[lan-ipv6]> dhcp rebind_time 43200
net-config[lan-ipv6]> save
```

Related show command: *show net lan ipv6 setup*

net lan ipv6 pool add

This command configures a new IPv6 DHCP address pool for the LAN. After you issue the **net lan ipv6 pool add** command, you enter the net-config [lan-ipv6-pool] mode and then you can configure the IPv6 start and end addresses and the IPv6 prefix length for the IPv6 pool in the order that you prefer.

Step 1	**Format**	**net lan ipv6 pool add**
	Mode	net
Step 2	**Format**	**start_address** *<ipv6-address>* **end_address** *<ipv6-address>* **prefix_length** *<prefix length>*
	Mode	net-config [lan-ipv6-pool]

Keyword	Associated Parameter to Type	Description
start_address	*ipv6-address*	The start address of the IPv6 address pool.
end_address	*ipv6-address*	The end address of the IPv6 address pool.
prefix_length	*prefix length*	The prefix length for the IPv6 address pool.

Command example:

```
FVS336Gv2> net lan ipv6 pool add
net-config[lan-ipv6-pool]> start_address 2001::1025
net-config[lan-ipv6-pool]> end_address 2001::1030
net-config[lan-ipv6-pool]> prefix_length 56
net-config[lan-ipv6-pool]> save
```

Related show command: *show net lan ipv6 setup*

net lan ipv6 pool edit <row id>

This command configures an existing IPv6 DHCP address pool for the LAN. After you issue the **net lan ipv6 pool edit** command to specify the row to be edited, you enter the net-config [lan-ipv6-pool] mode and then you can configure the IPv6 start and end addresses and the IPv6 prefix length for the IPv6 pool in the order that you prefer.

Step 1	**Format**	**net lan ipv6 pool edit** *<row id>*
	Mode	net
Step 2	**Format**	**start_address** *<ipv6-address>* **end_address** *<ipv6-address>* **prefix_length** *<prefix length>*
	Mode	net-config [lan-ipv6-pool]

Keyword	Associated Parameter to Type	Description
start_address	*ipv6-address*	The start address of the IPv6 address pool.
end_address	*ipv6-address*	The end address of the IPv6 address pool.
prefix_length	*prefix length*	The prefix length for the IPv6 address pool.

Related show command: *show net lan ipv6 setup*

net lan ipv6 pool delete <row id>

This command deletes an IPv6 DHCP address pool by specifying its row ID.

Format	**net lan ipv6 pool delete** *<row id>*
Mode	net

Related show command: *show net lan ipv6 setup*

---

net lan ipv6 multi_homing add

This command configures a new IPv6 alias, that is, a secondary IPv6 address. After you issue the **net lan ipv6 multi_homing add** command, you enter the net-config [lan-ipv6-multihoming] mode and then you can configure the secondary address and IPv6 prefix length in the order that you prefer.

Step 1	**Format**	**net lan ipv6 multi_homing add**
	Mode	net
Step 2	**Format**	**ip_address** *<ipv6-address>* **prefix_length** *<prefix length>*
	Mode	net-config [lan-ipv6-multihoming]

Keyword	Associated Parameter to Type	Description
ip_address	*ipv6-address*	The secondary IPv6 address for the LAN.
prefix_length	*prefix length*	The prefix length for the secondary IPv6 address.

Command example:

```
FVS336Gv2> net lan ipv6 multi_homing add
net-config[lan-ipv6-multihoming]> ip_address 2002::1006
net-config[lan-ipv6-multihoming]> prefix_length 10
net-config[lan-ipv6-multihoming]> save
```

Related show command: *show net lan ipv6 multiHoming*

---

net lan ipv6 multi_homing edit <row id>

This command configures an existing IPv6 alias, that is, a secondary IPv6 address. After you issue the **net lan ipv6 multi_homing edit** command to specify the row to be edited, you enter the net-config [lan-ipv6-multihoming] mode and then you can configure the secondary address and IPv6 prefix length in the order that you prefer.

Step 1	**Format**	**net lan ipv6 multi_homing edit** *<row id>*
	Mode	net
Step 2	**Format**	**ip_address** *<ipv6-address>* **prefix_length** *<prefix length>*
	Mode	net-config [lan-ipv6-multihoming]

Keyword	Associated Parameter to Type	Description
ip_address	*ipv6-address*	The secondary IPv6 address for the LAN.
prefix_length	*prefix length*	The prefix length for the secondary IPv6 address.

Related show command: *show net lan ipv6 multiHoming*

net lan ipv6 multi_homing delete <row id>

This command deletes a secondary IPv6 address by specifying its row ID.

Format	**net lan ipv6 multi_homing delete** *<row id>*
Mode	net

Related show command: *show net lan ipv6 multiHoming*

net radvd configure lan

This command configures the Router Advertisement Daemon (RADVD) for the link-local advertisements of IPv6 router addresses and prefixes in the LAN. After you issue the **net radvd configure lan** command, you enter the net-config [radvd-lan] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**net radvd configure lan**
	Mode	net

Step 2 **Format** **enable** {**Y** | **N**}
mode {**Unsolicited-Multicast** | **Unicast-Only**}
interval <*seconds*>
flags {**Managed** | **Other**}
preference {**Low** | **Medium** | **High**}
mtu <*number*>
life_time <*seconds*>

Mode net-config [radvd-lan]

Keyword	Associated Keyword to Select or Parameter to Type	Description
enable	**Y** or **N**	Enables the RADVD process to allow stateless autoconfiguration of the IPv6 LAN or disables the RADVD process.
mode	**Unsolicited-Multicast** or **Unicast-Only**	Specifies the advertisement mode: • **Unsolicited-Multicast**. Allows unsolicited multicast and unicast communication with the hosts. Router advertisements (RAs) are sent to all interfaces at the rate that is defined by the **interval** keyword and parameter. • **Unicast-Only**. Responds to unicast packet requests only. No unsolicited packets are advertised.
interval	*seconds*	The interval in seconds (integer) between unsolicited multicast RAs. Enter a period from 10 to 1800 seconds. The default is 30 seconds.
flags	**Managed** or **Other**	Specifies the flag: • **Managed**. The DHCPv6 stateful protocol is used for autoconfiguration of the address. • **Other**. The DHCPv6 stateful protocol is used for autoconfiguration of other (that is, nonaddress) information.
preference	**Low**, **Medium**, or **High**	Specifies the VPN firewall's preference in relation to other hosts and routers in the LAN.
mtu	*number*	The MTU size (integer) that is used in the RAs to ensure that all nodes in the network use the same MTU size. The default is 1500 seconds.
life_time	*seconds*	The advertisement lifetime in seconds (integer) of the route. The default is 3600 seconds.

Command example:

```
FVS336Gv2> net radvd configure lan
net-config[radvd-lan]> enable Y
net-config[radvd-lan]> mode Unsolicited-Multicast
net-config[radvd-lan]> interval 60
net-config[radvd-lan]> flags Managed
```

```
net-config[radvd-lan]> preference Medium
net-config[radvd-lan]> mtu 1496
net-config[radvd-lan]> life_time 7200
net-config[radvd-lan]> save
```

Related show command: *show net radvd lan setup*

net radvd pool lan add

This command configures the IPv6 RADVD pool of advertisement prefixes for the LAN. After you issue the **net radvd pool lan add** command, you enter the net-config [radvd-pool-lan] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**net radvd pool lan add**
	Mode	net
Step 2	**Format**	**prefix_type** {**6To4** {**6to4_interface** {**WAN1** | **WAN2**} {**sla_id** <*ID number*>} | **Global-Local-ISATAP** {**prefix_address** <*ipv6-address*>} {**prefix_length** <*prefix length*>}} **prefix_life_time** <*seconds*>
	Mode	net-config [radvd-pool-lan]

Keyword	Associated Keyword to Select or Parameter to Type	Description
prefix_type	**6To4** or **Global-Local-ISATAP**	Specifies the prefix type for communication between the interfaces: • **6To4**. The prefix is for a 6to4 address. You must issue the **6to4_interface** keyword and specify the WAN interface and the **sla_id** keyword and specify the interface ID. • **Global-Local-ISATAP**. The prefix is for a global, local, or ISATAP address. This must be a global prefix, not the site-local or link-local prefix. You must issue the **prefix_address** and **prefix_length** keywords and associated parameters.
6to4_interface	**WAN1** or **WAN2**	Specifies the WAN interface on which the 6to4 prefix is added.
sla_id	*ID number*	The site-level aggregation identifier (SLA ID) (integer) in the 6to4 address prefix is the ID of the interface from which the advertisements are sent.
prefix_address	*ipv6-address*	The IPv6 address for a global, local, or ISATAP prefix.
prefix_length	*prefix length*	The IPv6 prefix length (integer) for a global, local, or ISATAP prefix. This is a decimal value that indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address.

Keyword	Associated Keyword to Select or Parameter to Type	Description
prefix_life_time	*seconds*	The period in seconds (integer) during which the requesting router is allowed to use the prefix.

Command example:

```
FVS336Gv2> net radvd pool lan add
net-config[radvd-pool-lan]> prefix_type 6To4
net-config[radvd-pool-lan]> 6to4_interface WAN1
net-config[radvd-pool-lan]> sla_id 67
net-config[radvd-pool-lan]> prefix_life_time 3600
net-config[radvd-pool-lan]> save
```

Related show command: *show net radvd lan setup*

net radvd pool lan edit <row id>

This command configures an existing IPv6 RADVD address pool for the LAN. After you issue the **net radvd pool lan edit** command to specify the row to be edited, you enter the net-config [radvd-pool-lan] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**net radvd pool lan edit** *<row id>*
	Mode	net
Step 2	**Format**	**prefix_type** {**6To4** {**6to4_interface** {**WAN1** | **WAN2**} {**sla_id** *<ID number>*} | **Global-Local-ISATAP** {**prefix_address** *<ipv6-address>*} {**prefix_length** *<prefix length>*}} **prefix_life_time** *<seconds>*
	Mode	net-config [radvd-pool-lan]

Keyword	Associated Keyword to Select or Parameter to Type	Description
prefix_type	**6To4** or **Global-Local-ISATAP**	Specifies the prefix type for communication between the interfaces: • **6To4**. The prefix is for a 6to4 address. You must issue the **6to4_interface** keyword and specify the WAN interface and the **sla_id** keyword and specify the interface ID. • **Global-Local-ISATAP**. The prefix is for a global, local, or ISATAP address. This must be a global prefix, not the site-local or link-local prefix. You must issue the **prefix_address** and **prefix_length** keywords and associated parameters.
6to4_interface	**WAN1** or **WAN2**	Specifies the WAN interface on which the 6to4 prefix is added.

Keyword	Associated Keyword to Select or Parameter to Type	Description
sla_id	*ID number*	The site-level aggregation identifier (SLA ID) (integer) in the 6to4 address prefix is the ID of the interface from which the advertisements are sent.
prefix_address	*ipv6-address*	The IPv6 address for a global, local, or ISATAP prefix.
prefix_length	*prefix length*	The IPv6 prefix length (integer) for a global, local, or ISATAP prefix. This is a decimal value that indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address.
prefix_life_time	*seconds*	The period in seconds (integer) during which the requesting router is allowed to use the prefix.

Related show command: *show net radvd lan setup*

net radvd pool lan delete <row id>

This command deletes an RADVD address pool for the LAN by deleting its row ID.

Format	**net radvd pool lan delete** *<row id>*
Mode	net

Related show command: *show net radvd lan setup*

net lan ipv6 prefix_delegation add

This command configures a new IPv6 prefix for LAN prefix delegation. For information about how to enable prefix delegation for the IPv6 LAN, see the *net lan ipv6 configure* command. After you issue the **net lan ipv6 prefix_delegation add** command, you enter the net-config [lan-prefix-delegation] mode and then you can configure the IPv6 prefix and IPv6 prefix length in the order that you prefer.

Step 1	**Format**	**net lan ipv6 prefix_delegation add**
	Mode	net
Step 2	**Format**	**prefix** *<prefix>* **prefix_length** *<prefix length>*
	Mode	net-config [lan-prefix-delegation]

Keyword	Associated Parameter to Type	Description
prefix	*prefix*	The IPv6 prefix.
prefix_length	*prefix length*	The prefix length for the IPv6 prefix.

Command example:

```
FVS336Gv2> net lan ipv6 prefix_delegation add
net-config[lan-prefix-delegation]> prefix 2001:db8::
net-config[lan-prefix-delegation]> prefix_length 64
net-config[lan-prefix-delegation]> save
```

Related show command: *show net lan ipv6 setup*

net lan ipv6 prefix_delegation edit <row id>

This command configures an existing IPv6 prefix for LAN prefix delegation. After you issue the **net lan ipv6 prefix_delegation edit** command to specify the row to be edited, you enter the net-config [lan-prefix-delegation] mode and then you can configure the IPv6 prefix and IPv6 prefix length in the order that you prefer.

Step 1	**Format**	**net lan ipv6 prefix_delegation edit** <*row id*>
	Mode	net
Step 2	**Format**	**prefix** <*prefix*> **prefix_length** <*prefix length*>
	Mode	net-config [lan-prefix-delegation]

Keyword	Associated Parameter to Type	Description
prefix	*prefix*	The IPv6 prefix.
prefix_length	*prefix length*	The prefix length for the IPv6 prefix.

Related show command: *show net lan ipv6 setup*

net lan ipv6 prefix_delegation delete <row id>

This command deletes an IPv6 prefix for LAN prefix delegation by deleting its row ID.

Format	**net lan ipv6 prefix_delegation delete** <*row id*>
Mode	net

Related show command: *show net lan ipv6 setup*

IPv4 DMZ Setup Command

This section describes the **net dmz ipv4 configure** command.

net dmz ipv4 configure

This command enables, configures, or disables the IPv4 DMZ. After you issue the **net dmz ipv4 configure** command, you enter the net-config [dmz-ipv4] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1

Format **net dmz ipv4 configure**

Mode net

Step 2

Format

```
enable_dmz {Y | N}
ip_address <ipaddress>
subnet_mask <subnet mask>
dhcp_mode {None | DHCP-Server | DHCP-Relay}
dns_proxy_enable {Y | N}

domain_name <domain name>
starting_ip_address <ipaddress>
ending_ip_address <ipaddress>
primary_dns_server <ipaddress>
secondary_dns_server <ipaddress>
wins_server <ipaddress>
lease_time <hours>
enable_ldap {Y | N}
ldap_serverip <ipaddress>
ldap_search_base <search base>
ldap_port <number>

relay_gateway <ipaddress>
```

Mode net-config [dmz-ipv4]

Keyword	Associated Keyword to Select or Parameter to Type	Description
enable_dmz	**Y** or **N**	Enables or disables the DMZ.
ip_address	*ipaddress*	The IP address of the DMZ port.
subnet_mask	*subnet mask*	The subnet mask of the DMZ port.

Keyword	Associated Keyword to Select or Parameter to Type	Description
dhcp_mode	**None**, **DHCP-Serves** or **DHCP-Relay**	Specifies the DHCP mode: • **None**. DHCP is disabled for the DMZ. • **DHCP-Server**. DHCP is enabled for the DMZ. You can configure all keywords and parameters except the **relay_gateway** keyword and associated parameter. • **DHCP-Relay**. Addresses are assigned in the DMZ by a DHCP relay. Configure the **relay_gateway** keyword and associated parameter.
dns_proxy_enable	**Y** or **N**	Enables or disables the DNS proxy.
DHCP server		
domain_name	*domain name*	The server domain name (string) or FQDN for the DHCP server.
starting_ip_address	*ipaddress*	The start IP address for the DHCP address pool.
ending_ip_address	*ipaddress*	The end IP address for the DHCP address pool.
primary_dns_server	*ipaddress*	The IP address of the primary DNS server in the DMZ DHCP configuration.
secondary_dns_server	*ipaddress*	The IP address of the secondary DNS server in the DMZ DHCP configuration.
wins_server	*ipaddress*	The IP address of the WINS server in the DMZ DHCP configuration.
lease_time	*hours*	The duration in hours for which an IP address is leased.
enable_ldap	**Y** or **N**	Enables or disables LDAP.
ldap_serverip	*ipaddress*	The IP address of the LDAP server.
ldap_search_base	*search base*	The search base (string) for LDAP.
ldap_port	*number*	The port number for the LDAP server.
DHCP relay		
relay_gateway	*ipaddress*	Set the DHCP relay gateway server.

Command example:

```
FVS336Gv2> net dmz ipv4 configure
net-config[dmz-ipv4]> enable_dmz
net-config[dmz-ipv4]> ip_address 10.126.32.59
net-config[dmz-ipv4]> subnet_mask 2525.255.255.0
net-config[dmz-ipv4]> dhcp_mode None
net-config[dmz-ipv4]> dns_proxy_enable Y
net-config[dmz-ipv4]> save
```

Related show command: *show net dmz ipv4 setup*

IPv6 DMZ Setup Commands

This section describes the following commands:

- *net dmz ipv6 configure*
- *net dmz ipv6 pool configure <ipv6 address>*
- *net dmz ipv6 pool delete < ipv6 address>*
- *net radvd configure dmz*
- *net radvd pool dmz add*
- *net radvd pool dmz edit <row id>*
- *net radvd pool dmz delete <row id>*

net dmz ipv6 configure

This command enables, configures, or disables the IPv6 DMZ. After you issue the **`net dmz ipv6 configure`** command, you enter the net-config [dmz-ipv6] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**`net dmz ipv6 configure`**
	Mode	net
Step 2	**Format**	**`enable_dmz`** {**`Y`** | **`N`**} **`static ip_address`** *<ipv6-address>* **`static prefix_length`** *<prefix length>* **`dhcp server_enable`** {**`N`** | **`Y`** {**`dhcp dhcp_mode`** {**`Stateless`** | **`Stateful`**}}} **`dhcp domain name`** *<domain-name>* **`dhcp server_preference`** *<number>* **`dhcp dns_type`** {**`useDnsProxy`** | **`useDnsFromISP`** | **`useEnteredDns`** {**`dhcp primary_dns`** *<ipv6-address>*} [**`dhcp secondary_dns`** *<ipv6-address>*]} **`dhcp lease_time`** *<seconds>*
	Mode	net-config [dmz-ipv6]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
enable_dmz	**Y** or **N**	Enables or disables the DMZ.
static ip_address	*ipv6-address*	The IPv6 address of the DMZ port.
static prefix_length	*prefix length*	The prefix length (integer) for the DMZ port.
DHCPv6 server		
dhcp server_enable	**Y** or **N**	Enables or disables the DHCP server for the DMZ.
dhcp dhcp_mode	**Stateless** or **Stateful**	Specifies the DHCPv6 mode.
dhcp domain_name	*domain name*	The server domain name (string) for the DHCP server.
dhcp server_preference	*number*	The preference number (integer) of the DHCP server.
dhcp dns_type	**useDnsProxy, useDnsFromISP**, or **useEnteredDns**	Specifies the DNS server type. If you select **useEnteredDns**, you also must issue the **dhcp primary_dns** keywords and associated parameter. The **dhcp secondary_dns** keywords and associated parameter are optional.
dhcp primary_dns	*ipv6-address*	The IPv6 address for the primary DNS server in the DMZ configuration.
dhcp secondary_dns	*ipv6-address*	The IPv6 address of the secondary DNS server in the DMZ configuration.
dhcp lease_time	*seconds*	The duration in seconds for which an IP address is leased.

Command example:

```
FVS336Gv2> net dmz ipv6 configure
net-config[dmz-ipv6]> enable_dmz Y
net-config[dmz-ipv6]> static ip_address 2001:176::1
net-config[dmz-ipv6]> static prefix_length 64
net-config[dmz-ipv6]> dhcp server_enable Y
net-config[dmz-ipv6]> dhcp dhcp_mode Stateful
net-config[dmz-ipv6]> dhcp domain_name netgear.com
net-config[dmz-ipv6]> dhcp server_preference 210
net-config[dmz-ipv6]> dhcp dns_type useDnsProxy
net-config[dmz-ipv6]> dhcp lease_time 43200
net-config[dmz-ipv6]> save
```

Related show command: *show net dmz ipv6 setup*

net dmz ipv6 pool configure <ipv6 address>

This command configures a new or existing IPv6 DHCP address pool for the DMZ. After you issue the **net dmz ipv6 pool configure** command to specify the IPv6 start address of the IPv6 pool, you enter the net-config [dmz-ipv6-pool] mode and then you can configure the IPv6 end address and the IPv6 prefix length for the IPv6 pool in the order that you prefer.

Step 1	**Format**	**net dmz ipv6 pool configure** *<ipv6-address>*
	Mode	net
Step 2	**Format**	**ending_ip_address** *<ipv6-address>* **prefix_length** *<prefix length>*
	Mode	net-config [dmz-ipv6-pool]

Keyword	Associated Parameter to Type	Description
ending_ip_address	*ipv6-address*	The end address of the IPv6 address pool.
prefix_length	*prefix length*	The prefix length for the IPv6 address pool.

Command example:

```
FVS336Gv2> net dmz ipv6 pool configure 2001::1100
net-config[dmz-ipv6-pool]> ending_ip_address 2001::1120
net-config[dmz-ipv6-pool]> prefix_length 56
net-config[dmz-ipv6-pool]> save
```

Related show command: *show net dmz ipv6 setup*

---

net dmz ipv6 pool delete < ipv6 address>

This command deletes an IPv6 DHCP address pool for the DMZ by deleting the start address of the pool.

Format	**net dmz ipv6 pool delete** *<ipv6-address>*
Mode	net

Related show command: *show net dmz ipv6 setup*

---

net radvd configure dmz

This command configures the router advertisement daemon (RADVD) process for the link-local advertisements of IPv6 router addresses and prefixes in the DMZ. After you issue the **net radvd configure dmz** command, you enter the net-config [radvd-dmz] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1 **Format** `net radvd configure dmz`

Mode net

Step 2 **Format** `enable {Y | N}`
`mode {Unsolicited-Multicast | Unicast-Only}`
`interval <seconds>`
`flags {Managed | Other}`
`preference {Low | Medium | High}`
`mtu <number>`
`life_time <seconds>`

Mode net-config [radvd-dmz]

Keyword	Associated Keyword to Select or Parameter to Type	Description
enable	**Y** or **N**	Enables the RADVD process to allow stateless autoconfiguration of the IPv6 DMZ or disables the RADVD process.
mode	**Unsolicited-Multicast** or **Unicast-Only**	Specifies the advertisement mode: • **Unsolicited-Multicast**. Allows unsolicited multicast and unicast communication with the hosts. Router advertisements (RAs) are sent to all interfaces at the rate that is defined by the **interval** keyword and associated parameter. • **Unicast-Only**. Responds to unicast packet requests only. No unsolicited packets are advertised.
interval	*seconds*	The interval in seconds (integer) between unsolicited multicast RAs. Enter a period from 10 to 1800 seconds. The default is 30 seconds.
flags	**Managed** or **Other**	Specifies the flag: • **Managed**. Specifies that the DHCPv6 stateful protocol is used for autoconfiguration of the address. • **Other**. Specifies that the DHCPv6 stateful protocol is used for autoconfiguration of other (that is, nonaddress) information.
preference	**Low**, **Medium**, or **High**	Specifies the VPN firewall's preference in relation to other hosts and routers in the DMZ.
mtu	*number*	The MTU size (integer) that is used in the RAs to ensure that all nodes in the network use the same MTU size. The default is 1500 seconds.
life_time	*seconds*	The advertisement lifetime in seconds (integer) of the route. The default is 3600 seconds.

Command example:

```
FVS336Gv2> net radvd configure dmz
net-config[radvd-dmz]> enable Y
net-config[radvd-dmz]> mode Unicast-Only
net-config[radvd-dmz]> flags Managed
net-config[radvd-dmz]> preference High
net-config[radvd-dmz]> mtu 1500
net-config[radvd-dmz]> life_time 7200
net-config[radvd-dmz]> save
```

Related show command: *show net radvd dmz setup*

net radvd pool dmz add

This command configures the IPv6 RADVD pool of advertisement prefixes for the DMZ. After you issue the **net radvd pool dmz add** command, you enter the net-config [radvd-pool-dmz] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**net radvd pool dmz add**
	Mode	net
Step 2	**Format**	**prefix_type** {**6To4** {**6to4_interface** {**WAN1** | **WAN2**} {**sla_id** <*ID number*>} | **Global-Local-ISATAP** {**prefix_address** <*ipv6-address*>} {**prefix_length** <*prefix length*>}} **prefix_life_time** <*seconds*>
	Mode	net-config [radvd-pool-dmz]

Keyword	Associated Keyword to Select or Parameter to Type	Description
prefix_type	**6To4** or **Global-Local-ISATAP**	Specifies the prefix type for communication between the interfaces: • **6To4**. The prefix is for a 6to4 address. You must issue the **6to4_interface** keyword and specify the WAN interface and the **sla_id** keyword and specify the interface ID. • **Global-Local-ISATAP**. The prefix is for a global, local, or ISATAP address. This must be a global prefix, not the site-local or link-local prefix. You must issue the **prefix_address** and **prefix_length** keywords and associated parameters.
6to4_interface	**WAN1** or **WAN2**	Specifies the WAN interface on which the 6to4 prefix is added.
sla_id	*ID number*	The site-level aggregation identifier (SLA ID) (integer) in the 6to4 address prefix is the ID of the interface from which the advertisements are sent.
prefix_address	*ipv6-address*	The IPv6 address for a global, local, or ISATAP prefix.

Keyword	Associated Keyword to Select or Parameter to Type	Description
prefix_length	*prefix length*	The IPv6 prefix length (integer) for a global, local, or ISATAP prefix. This is a decimal value that indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address.
prefix_life_time	*seconds*	The period in seconds (integer) during which the requesting router is allowed to use the prefix.

Command example:

```
FVS336Gv2> net radvd pool dmz add
net-config[radvd-pool-dmz]> prefix_type Global-Local-ISATAP
net-config[radvd-pool-dmz]> prefix_address 2002:3a2b
net-config[radvd-pool-dmz]> prefix_length 64
net-config[radvd-pool-dmz]> prefix_life_time 3600
net-config[radvd-pool-dmz]> save
```

Related show command: *show net radvd dmz setup*

net radvd pool dmz edit <row id>

This command configures an existing IPv6 RADVD address pool for the DMZ. After you issue the **net radvd pool dmz edit** command to specify the row to be edited, you enter the net-config [radvd-pool-dmz] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**net radvd pool dmz edit** *<row id>*
	Mode	net
Step 2	**Format**	**prefix_type** {**6To4** {**6to4_interface** {**WAN1** | **WAN2**} {**sla_id** *<ID number>*} | **Global-Local-ISATAP** {**prefix_address** *<ipv6-address>*} {**prefix_length** *<prefix length>*}} **prefix_life_time** *<seconds>*
	Mode	net-config [radvd-pool-dmz]

Keyword	Associated Keyword to Select or Parameter to Type	Description
prefix_type	**6To4** or **Global-Local-ISATAP**	Specifies the prefix type for communication between the interfaces: • **6To4**. The prefix is for a 6to4 address. You must issue the **6to4_interface** keyword and specify the WAN interface and the **sla_id** keyword and specify the interface ID. • **Global-Local-ISATAP**. The prefix is for a global, local, or ISATAP address. This must be a global prefix, not the site-local or link-local prefix. You must issue the **prefix_address** and **prefix_length** keywords and associated parameters.
6to4_interface	**WAN1** or **WAN2**	Specifies the WAN interface on which the 6to4 prefix is added.
sla_id	*ID number*	The site-level aggregation identifier (SLA ID) (integer) in the 6to4 address prefix is the ID of the interface from which the advertisements are sent.
prefix_address	*ipv6-address*	The IPv6 address for a global, local, or ISATAP prefix.
prefix_length	*prefix length*	The IPv6 prefix length (integer) for a global, local, or ISATAP prefix. This is a decimal value that indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address.
prefix_life_time	*seconds*	The period in seconds (integer) during which the requesting router is allowed to use the prefix.

Related show command: *show net radvd dmz setup*

net radvd pool dmz delete <row id>

This command deletes an RADVD address pool for the DMZ by deleting its row ID.

Format **net radvd pool dmz delete** *<row id>*

Mode net

Related show command: *show net radvd dmz setup*

WAN QoS Commands

This section describes the following commands:

- *net qos configure*
- *net qos profile add*
- *net qos profile edit <row id>*
- *net qos profile delete <row id>*
- *net qos profile disable <row id>*
- *net qos profile enable <row id>*

net qos configure

This command configures the QoS mode for the WAN interfaces. After you issue the **net qos configure** command, you enter the net-config [network-qos] mode and then you can enable QoS and set the QoS mode to rate control or priority.

The configured QoS mode determines which WAN QoS profiles can be active, that is, you can add both rate control and priority WAN QoS profiles (see the *net qos profile add* command), but only the profiles for the configured QoS mode can be active. For example, if you set the QoS mode to priority, only the profiles with a priority configuration can be active.

Step 1	**Format**	**net qos configure**
	Mode	net
Step 2	**Format**	**enable** {**Y** | **N**} **qos_type** {**Rate-Control** | **Priority**}
	Mode	net-config [network-qos]

Keyword	Associated Keyword to Select	Description
enable	**Y** or **N**	Enables or disables QoS for all WAN interfaces.
qos_type	**Rate-Control** or **Priority**	Specifies whether QoS uses rate control or priority profiles.

Related show command: *show net qos setup*

net qos profile add

This command configures a new WAN QoS profile. After you issue the **net qos profile add** command, you enter the net-config [network-qos-profile] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1 **Format** **net qos profile add**

Mode net

Step 2 **Format** The following settings apply to both rate control profiles and priority profiles:

qos_type {**Rate-Control** | **Priority**}
interface {**WAN1** | **WAN2**}
service_name {**default_services** <*default service name*> |
{**custom_services** <*custom service name*>}
diffserv_qos_match <*number*>
diffserv_qos_remark <*number*>

The following settings apply only to rate control profiles:

direction_for_rate_control {**Inbound** | **Outbound** | **Both**}
congestion_priority {**Default** | **High** | **Medium-high** | **Medium** | **Low**}
hosts {**Single-IP-Address** {**hosts_start_ip** <*ipaddress*>} |
IP-Address-Range {**hosts_start_ip** <*ipaddress*>} {**hosts_end_ip** <*ipaddress*>} | **Group** {**hosts_group** {**Group1** | **Group2** | **Group3** | **Group4** | **Group5** | **Group6** | **Group7** | **Group8**}}}
bandwidth_allocation {**Shared** | **Individual**}
outbound_min_bandwidth <*bandwidth*>
outbound_max_bandwidth <*bandwidth*>
inbound_min_bandwidth <*bandwidth*>
inbound_max_bandwidth <*bandwidth*>

The following settings apply only to priority profiles:

direction_for_priority {**Inbound-Traffic** | **Outbound-Traffic**}
priority {**Low** | **High**}

Mode net-config [network-qos-profile]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Common settings		
qos_type	**Rate-Control** or **Priority**	Specifies the type of profile: • **Rate-Control**. Configure the keywords and parameters that are shown in the Common settings section and Rate control profile settings section of this table. • **Priority**. Configure the keywords and parameters that are shown in the Common settings section and Priority profile settings section of this table.
interface	**WAN1** or **WAN2**	Specifies the interface to which the profile applies.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the profile applies.
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the profile applies.
diffserv_qos_match	*number*	(Optional) The DSCP value, from 0 through 63. Packets are classified against this value.
diffserv_qos_remark	*number*	(Optional) The DSCP value, from 0 through 63. Packets are marked with this value.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Rate control profile settings		
direction_for_rate_control	**Inbound**, **Outbound**, or **Both**	Specifies the direction to which rate control applies: • **Inbound**. Rate control applies to inbound packets only. You must issue the **inbound_min_bandwidth** and **inbound_max_bandwidth** keywords and specify the bandwidth that is allocated. • **Outbound**. Rate control applies to outbound packets only. You must issue the **outbound_min_bandwidth** and **outbound_max_bandwidth** keywords and specify the bandwidth that is allocated. • **Both**. Rate control applies to both inbound and outbound packets. You must issue the **inbound_min_bandwidth**, **inbound_max_bandwidth**, **outbound_min_bandwidth**, and **outbound_max_bandwidth** keywords and specify the bandwidth that is allocated.
congestion_priority	**Default**, **High**, **Medium-high**, **Medium**, or **Low**	Specifies the priority queue that determines the allocation of excess bandwidth and the classification level of the packets among other priority queues on the VPN firewall: • **Default**. Traffic is mapped based on the ToS field in the packet's IP header. • **High**. This queue includes the following DSCP values: AF41, AF42, AF43, AF44, and CS4. • **Medium-high**. This queue includes the following DSCP values: AF31, AF32, AF33, AF34, and CS3. • **Medium**. This queue includes the following DSCP values: AF21, AF22, AF23, AF24, and CS2. • **Low**. This queue includes the following DSCP values: AF11, AF12, AF13, AF14, CS1, 0, and all other values.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
hosts	**Single-IP-Address**, **IP-Address-Range**, or **Group**	Specifies the IP address, range of IP addresses, or group to which the profile applies: • **Single-IP-Address**. The profile applies to a single IP address. Issue the **hosts_start_ip** keyword to specify the IP address. • **IP-Address-Range**. The profile applies to an IP address range. Issue the **hosts_start_ip** and **hosts_end_ip** keywords to specify the start and end IP addresses of the range. In addition, issue the **bandwidth_allocation** keyword to specify if bandwidth is shared between all IP addresses in the range or is allocated to each IP address in the range. • **Group**. The profile applies to a group. Issue the **hosts_group** keyword to specify the group. In addition, issue the **bandwidth_allocation** keyword to specify if bandwidth is shared between all members of the group or is allocated to each member in the group.
hosts_start_ip	*ipaddress*	The following two options are available: • The IP address if the **hosts** keyword is set to **Single-IP-Address**. • The start IP address if the **hosts** keyword is set to **IP-Address-Range**.
hosts_end_ip	*ipaddress*	The end IP address if the **hosts** keyword is set to **IP-Address-Range**.
hosts_group	**Group1**, **Group2**, **Group3**, **Group4**, **Group5**, **Group6**, **Group7**, or **Group8**	Specifies the group if the **hosts** keyword is set to **Group**. **Note:** You cannot enter group names that you specify with the *net lan lan_groups edit <row id> <new group name>* command.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
bandwidth_allocation	**Shared** or **Individual**	Specifies how bandwidth is allocated. These options apply when the **hosts** keyword is set to **IP-Address-Range** or to **group**. • **Shared**. The bandwidth is shared among all IP addresses in a range or all members of a group. • **Individual**. The bandwidth is allocated to each IP address in the range or each member of a group.
outbound_min_bandwidth	*bandwidth*	The outbound minimum bandwidth in Kbps, from 0 to 100,000. This option applies if the **direction_for_rate_control** keyword is set to **outbound** or **both**.
outbound_max_bandwidth	*bandwidth*	The outbound maximum bandwidth in Kbps, from 100 to 100,000. This option applies if the **direction_for_rate_control** keyword is set to **outbound** or **both**.
inbound_min_bandwidth	*bandwidth*	The inbound minimum bandwidth in Kbps, from 0 to 100,000. This option applies if the **direction_for_rate_control** keyword is set to **inbound** or **both**.
inbound_max_bandwidth	*bandwidth*	The inbound maximum bandwidth in Kbps, from 100 to 100,000. This option applies if the **direction_for_rate_control** keyword is set to **inbound** or **both**.
Priority profile settings		
direction_for_priority	**Inbound-Traffic** or **Outbound-Traffic**	Specifies the direction to which the priority queue applies: • **Inbound-Traffic**. The priority queue applies to inbound traffic only. • **Outbound-Traffic**. The priority queue applies to outbound traffic only.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
priority	**Low** or **High**	Specifies the priority queue that determines the allocation of bandwidth: • **Low**. All services that are assigned a low-priority queue share 10 percent of interface bandwidth. • **High**. All services that are assigned a high-priority queue share 60 percent of interface bandwidth. **Note:** By default, all services are assigned the medium-priority queue in which they share 30 percent of the interface bandwidth.

Command example:

```
FVS336Gv2> net qos profile add
net-config[network-qos-profile]> qos_type Rate-Control
net-config[network-qos-profile]> interface WAN2
net-config[network-qos-profile]> service_name default_services http
net-config[network-qos-profile]> direction_for_rate_control Inbound
net-config[network-qos-profile]> congestion_priority High
net-config[network-qos-profile]> hosts IP-Address-Range
net-config[network-qos-profile]> hosts_start_ip 192.168.110.2
net-config[network-qos-profile]> hosts_end_ip 192.168.110.199
net-config[network-qos-profile]> bandwidth_allocation Shared
net-config[network-qos-profile]> inbound_min_bandwidth 7500
net-config[network-qos-profile]> inbound_max_bandwidth 15000
net-config[network-qos-profile]> diffserv_qos_match 5
net-config[network-qos-profile]> diffserv_qos_remark 12
net-config[network-qos-profile]> save
```

Related show command: *show net qos setup*

net qos profile edit <row id>

This command configures an existing WAN QoS profile. After you issue the **net qos profile edit** command to specify the row to be edited, you enter the net-config [network-qos-profile] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**net qos profile edit** *<row id>*
	Mode	net

Step 2 **Format** The following settings apply to both rate control profiles and priority profiles:

```
qos_type {Rate-Control | Priority}
interface {WAN1 | WAN2}
service_name {default_services <default service name> |
   {custom_services <custom service name>}
diffserv_qos_match <number>
diffserv_qos_remark <number>
```

The following settings apply only to rate control profiles:

```
direction_for_rate_control {Inbound | Outbound | Both}
congestion_priority {Default | High | Medium-high | Medium | Low}
hosts {Single-IP-Address {hosts_start_ip <ipaddress>} |
   IP-Address-Range {hosts_start_ip <ipaddress>} {hosts_end_ip
   <ipaddress>} | Group {hosts_group {Group1 |Group2|Group3|
   Group4 |Group5 |Group6 |Group7|Group8}}}
bandwidth_allocation {Shared | Individual}
outbound_min_bandwidth <bandwidth>
outbound_max_bandwidth <bandwidth>
inbound_min_bandwidth <bandwidth>
inbound_max_bandwidth <bandwidth>
```

The following settings apply only to priority profiles:

```
direction_for_priority {Inbound-Traffic | Outbound-Traffic}
priority {Low | High}
```

Mode net-config [network-qos-profile]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Common settings		
qos_type	**Rate-Control** or **Priority**	Specifies the type of profile: • **Rate-Control**. Configure the keywords and parameters that are shown in the Common settings section and Rate control profile settings section of this table. • **Priority**. Configure the keywords and parameters that are shown in the Common settings section and Priority profile settings section of this table.
interface	**WAN1** or **WAN2**	Specifies the interface to which the profile applies.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the profile applies.
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the profile applies.
diffserv_qos_match	*number*	(Optional) The DSCP value, from 0 through 63. Packets are classified against this value.
diffserv_qos_remark	*number*	(Optional) The DSCP value, from 0 through 63. Packets are marked with this value.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Rate control profile settings		
direction_for_rate_control	**Inbound**, **Outbound**, or **Both**	Specifies the direction to which rate control applies: • **Inbound**. Rate control applies to inbound packets only. You must issue the **inbound_min_bandwidth** and **inbound_max_bandwidth** keywords and specify the bandwidth that is allocated. • **Outbound**. Rate control applies to outbound packets only. You must issue the **outbound_min_bandwidth** and **outbound_max_bandwidth** keywords and specify the bandwidth that is allocated. • **Both**. Rate control applies to both inbound and outbound packets. You must issue the **inbound_min_bandwidth**, **inbound_max_bandwidth**, **outbound_min_bandwidth**, and **outbound_max_bandwidth** keywords and specify the bandwidth that is allocated.
congestion_priority	**Default**, **High**, **Medium-high**, **Medium**, or **Low**	Specifies the priority queue that determines the allocation of excess bandwidth and the classification level of the packets among other priority queues on the VPN firewall: • **Default**. Traffic is mapped based on the ToS field in the packet's IP header. • **High**. This queue includes the following DSCP values: AF41, AF42, AF43, AF44, and CS4. • **Medium-high**. This queue includes the following DSCP values: AF31, AF32, AF33, AF34, and CS3. • **Medium**. This queue includes the following DSCP values: AF21, AF22, AF23, AF24, and CS2. • **Low**. This queue includes the following DSCP values: AF11, AF12, AF13, AF14, CS1, 0, and all other values.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
hosts	**Single-IP-Address**, **IP-Address-Range**, or **Group**	Specifies the IP address, range of IP addresses, or group to which the profile applies: • **Single-IP-Address**. The profile applies to a single IP address. Issue the **hosts_start_ip** keyword to specify the IP address. • **IP-Address-Range**. The profile applies to an IP address range. Issue the **hosts_start_ip** and **hosts_end_ip** keywords to specify the start and end IP addresses of the range. In addition, issue the **bandwidth_allocation** keyword to specify if bandwidth is shared between all IP addresses in the range or is allocated to each IP address in the range. • **Group**. The profile applies to a group. Issue the **hosts_group** keyword to specify the group. In addition, issue the **bandwidth_allocation** keyword to specify if bandwidth is shared between all members of the group or is allocated to each member in the group.
hosts_start_ip	*ipaddress*	The following two options are available: • The IP address if the **hosts** keyword is set to **Single-IP-Address**. • The start IP address if the **hosts** keyword is set to **IP-Address-Range**.
hosts_end_ip	*ipaddress*	The end IP address if the **hosts** keyword is set to **IP-Address-Range**.
hosts_group	**Group1**, **Group2**, **Group3**, **Group4**, **Group5**, **Group6**, **Group7**, or **Group8**	Specifies the group if the **hosts** keyword is set to **Group**. **Note:** You cannot enter group names that you specify with the *net lan lan_groups edit <row id> <new group name>* command.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
bandwidth_allocation	**Shared** or **Individual**	Specifies how bandwidth is allocated. These options apply when the **hosts** keyword is set to **IP-Address-Range** or to **group**. • **Shared**. The bandwidth is shared among all IP addresses in a range or all members of a group. • **Individual**. The bandwidth is allocated to each IP address in the range or each member of a group.
outbound_min_bandwidth	*bandwidth*	The outbound minimum bandwidth in Kbps, from 0 to 100,000. This option applies if the **direction_for_rate_control** keyword is set to **outbound** or **both**.
outbound_max_bandwidth	*bandwidth*	The outbound maximum bandwidth in Kbps, from 100 to 100,000. This option applies if the **direction_for_rate_control** keyword is set to **outbound** or **both**.
inbound_min_bandwidth	*bandwidth*	The inbound minimum bandwidth in Kbps, from 0 to 100,000. This option applies if the **direction_for_rate_control** keyword is set to **inbound** or **both**.
inbound_max_bandwidth	*bandwidth*	The inbound maximum bandwidth in Kbps, from 100 to 100,000. This option applies if the **direction_for_rate_control** keyword is set to **inbound** or **both**.
Priority profile settings		
direction_for_priority	**Inbound-Traffic** or **Outbound-Traffic**	Specifies the direction to which the priority queue applies: • **Inbound-Traffic**. The priority queue applies to inbound traffic only. • **Outbound-Traffic**. The priority queue applies to outbound traffic only.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
priority	**Low** or **High**	Specifies the priority queue that determines the allocation of bandwidth: • **Low**. All services that are assigned a low-priority queue share 10 percent of interface bandwidth. • **High**. All services that are assigned a high-priority queue share 60 percent of interface bandwidth. **Note:** By default, all services are assigned the medium-priority queue in which they share 30 percent of the interface bandwidth.

Related show command: *show net qos setup*

net qos profile delete <row id>

This command deletes a WAN QoS profile by deleting its row ID.

Format **net qos profile delete** <*row id*>

Mode net

Related show command: *show net qos setup*

net qos profile disable <row id>

This command disables a WAN QoS profile by specifying its row ID.

Format **net qos profile disable** <*row id*>

Mode net

Related show command: *show net qos setup*

net qos profile enable <row id>

This command enables a WAN QoS profile by specifying its row ID.

Format **net qos profile enable** <*row id*>

Mode net

Related show command: *show net qos setup*

IPv4 Routing Commands

This section describes the following commands:

- *net routing static ipv4 configure <route name>*
- *net routing static ipv4 delete <route name>*
- *net routing static ipv4 delete_all*
- *net routing dynamic configure*

net routing static ipv4 configure <route name>

This command configures an IPv4 static route. After you issue the **net routing static ipv4 configure** command to specify the name of the new route, you enter the net-config [static-routing-ipv4] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1

Format **net routing static ipv4 configure** <*route name*>

Mode net

Step 2

Format
active_flag {**Y** | **N**}
private_flag {**Y** | **N**}
destination_address <*ipaddress*>
subnet_mask <*subnet mask*>
interface {**custom_vlan** <*VLAN name*> | **dmz** | **lan** | **wan** {**WAN1** | **WAN2**}}
gateway_address <*ipaddress*>
metric <*number*>

Mode net-config [static-routing-ipv4]

Keyword	Associated Keyword to Select or Parameter to Type	Description
active_flag	**Y** or **N**	Specifies whether or not the route is an active route.
private_flag	**Y** or **N**	Specifies whether the route is private or can be shared with other gateways when RIP is enabled.
destination_address	*ipaddress*	The destination IP address.
subnet_mask	*subnet mask*	The destination subnet mask.
interface	**custom_vlan** <*VLAN name*>, **dmz**, **lan**, or **wan**	Specifies the interface for which the route applies. The **dmz** and **lan** keywords do not require additional selections. The **custom vlan** and **wan** keywords require additional selections: • If you issue the **custom_vlan** keyword, you also must specify the VLAN name. • If you issue the **wan** keyword, you also must specify the WAN interface (WAN1 or WAN2).

Keyword	Associated Keyword to Select or Parameter to Type	Description
gateway_address	*ipaddress*	The gateway IP address.
metric	*number*	The metric (integer) for this route. The number can be from 2 to 15.

Command example:

```
FVS336Gv2> net routing static ipv4 configure Orly
net-config[static-routing-ipv4]> active_flag Y
net-config[static-routing-ipv4]> private_flag Y
net-config[static-routing-ipv4]> destination_address 10.118.215.178
net-config[static-routing-ipv4]> subnet_mask 255.255.255.0
net-config[static-routing-ipv4]> interface wan WAN1
net-config[static-routing-ipv4]> gateway_address 10.192.44.13
net-config[static-routing-ipv4]> metric 7
net-config[static-routing-ipv4]> save
```

Related show command: *show net routing static ipv4 setup*

net routing static ipv4 delete <route name>

This command deletes a static IPv4 route by deleting its name.

Format	**net routing static ipv4 delete** *<route name>*
Mode	net

Related show command: *show net routing static ipv4 setup*

net routing static ipv4 delete_all

This command deletes all static IPv4 routes.

Format	**net routing static ipv4 delete_all**
Mode	net

Related show command: *show net routing static ipv4 setup*

net routing dynamic configure

This command configures RIP and the associated MD5 key information. After you issue the **net routing dynamic configure** command, you enter the net-config [dynamic-routing] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1 **Format** `net routing dynamic configure`

Mode net

Step 2 **Format**

```
authentication_enable {Y | N}
direction {None | In-only | Out-only | Both}
version {Disabled | Rip1 | Rip2B | Rip2M}

first_key authentication_id <authentication key>
first_key id_number <number>
first_key valid_from {day <day>}
first_key valid_from {month <month>}
first_key valid_from {year <year>}}
first_key valid_from {hour <hour> |
first_key valid_from {minute <minute>}
first_key valid_from {second <second>}
first_key valid_to {day <day>}
first_key valid_to {month <month>}
first_key valid_to {year <year>}}
first_key valid_to {hour <hour> |
first_key valid_to {minute <minute>}
first_key valid_to {second <second>}

second_key authentication_id <authentication key>
second_key id_number <number>
second_key valid_from {day <day>}
second_key valid_from {month <month>}
second_key valid_from {year <year>}}
second_key valid_from {hour <hour> |
second_key valid_from {minute <minute>}
second_key valid_from {second <second>}
second_key valid_to {day <day>}
second_key valid_to {month <month>}
second_key valid_to {year <year>}}
second_key valid_to {hour <hour> |
second_key valid_to {minute <minute>}
second_key valid_to {second <second>}
```

Mode net-config [dynamic-routing]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
General		
authentication_enable	**Y** or **N**	Enables or disables authentication for RIP-2B or RIP-2M.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description	
direction	**None**, **In-only**, **Out-only**, or **Both**.	Specifies the RIP direction.	
version	**Disabled**, **Rip1**, **Rip2B**, or **Rip2M**	Specifies the RIP version.	
First key			
first_key authentication_id	*authentication key*	The first MD5 authentication key (alphanumeric string).	
first_key id_number	*number*	The first MD5 key ID (integer).	
first_key valid_from day	*day*	The day in the format DD (01 to 31).	The day and time on which the validity of the first MD5 authentication key starts.
first_key valid_from month	*month*	The month in the format MM (01 to 12).	
first_key valid_from year	*year*	The year in the format YYYY (1970 to 2037).	
first_key valid_from hour	*hour*	The hour in the 24-hour format HH (00 to 23).	
first_key valid_from minute	*minute*	The minute in the format MM (00 to 59).	
first_key valid_from second	*second*	The second in the format SS (00 to 59).	
first_key valid_to day	*day*	The day in the format DD (01 to 31).	The day and time on which the validity of the first MD5 authentication key expires.
first_key valid_to month	*month*	The month in the format MM (01 to12).	
first_key valid_to year	*year*	The year in the format YYYY (1970 to 2037).	
first_key valid_to hour	*hour*	The hour in the 24-hour format HH (00 to 23).	
first_key valid_to minute	*minute*	The minute in the format MM (00 to 59).	
first_key valid_to second	*second*	The second in the format SS (00 to 59).	
Second key			
Note: The keywords and parameters for the second key follow the same format as those for the first key.			

Command example:

```
FVS336Gv2> net routing dynamic configure
net-config[dynamic-routing]> authentication_enable Y
net-config[dynamic-routing]> direction Both
net-config[dynamic-routing]> version Rip2M
net-config[dynamic-routing]> first_key authentication_id 2rt!00jkl26ll7Oo0
net-config[dynamic-routing]> first_key id_number 1
net-config[dynamic-routing]> first_key valid_from day 01
net-config[dynamic-routing]> first_key valid_from month 12
net-config[dynamic-routing]> first_key valid_from year 2011
net-config[dynamic-routing]> first_key valid_from hour 07
net-config[dynamic-routing]> first_key valid_from minute 00
net-config[dynamic-routing]> first_key valid_from second 00
net-config[dynamic-routing]> first_key valid_to day 31
net-config[dynamic-routing]> first_key valid_to month 12
net-config[dynamic-routing]> first_key valid_to year 2011
net-config[dynamic-routing]> first_key valid_to hour 23
net-config[dynamic-routing]> first_key valid_to minute 59
net-config[dynamic-routing]> first_key valid_to second 59
net-config[dynamic-routing]> second_key authentication_id 3gry!!99OoiI
net-config[dynamic-routing]> second_key id_number 2
net-config[dynamic-routing]> second_key valid_from day 31
net-config[dynamic-routing]> second_key valid_from month 12
net-config[dynamic-routing]> second_key valid_from year 2011
net-config[dynamic-routing]> second_key valid_from hour 24
net-config[dynamic-routing]> second_key valid_from minute 00
net-config[dynamic-routing]> second_key valid_from second 00
net-config[dynamic-routing]> second_key valid_to day 31
net-config[dynamic-routing]> second_key valid_to month 03
net-config[dynamic-routing]> second_key valid_to year 2012
net-config[dynamic-routing]> second_key valid_to hour 23
net-config[dynamic-routing]> second_key valid_to minute 59
net-config[dynamic-routing]> second_key valid_to second 59
net-config[dynamic-routing]> save
```

Related show command: *show net routing dynamic setup*

IPv6 Routing Commands

This section describes the following commands:

- *net routing static ipv6 configure <route name>*
- *net routing static ipv6 delete <route name>*
- *net routing static ipv6 delete_all*

net routing static ipv6 configure <route name>

This command configures an IPv6 static route. After you issue the **net routing static ipv6 configure** command to specify the name of the new route, you enter the net-config [static-routing-ipv6] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**net routing static ipv6 configure** *<route name>*
	Mode	net
Step 2	**Format**	**active_flag** {**Y** | **N**} **destination_address** *<ipv6-address>* **prefix** *<prefix length>* **gateway_address** {**6to4_gateway** *<ipv6-address>* | **ipv6_gateway** *<ipv6-address>*} **interface** {**WAN1** | **WAN2** | **Sit0-WAN** | **LAN** | **DMZ**} **metric** *<number>*
	Mode	net-config [static-routing-ipv6]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
active_flag	**Y** or **N**	Specifies whether or not the route is an active route.
destination_address	*ipv6-address*	The destination IP address.
prefix	*prefix length*	The IPv6 prefix length (integer). This is a decimal value that indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address.
interface	**WAN1**, **WAN2**, **Sit0-WAN**, **LAN**, or **DMZ**	Specifies the physical or virtual network interface through which the route is accessible: • **WAN1** or **WAN2**. The selected WAN interface. • **Sit0-WAN1**. The 6to4-WAN interface. • **LAN**. The LAN interface. • **DMZ**. The LAN interface.
gateway_address 6to4_gateway	*ipv6-address*	The gateway IP address for a route that uses a 6to4 tunnel. The **6to4_gateway** and **ipv6_gateway** keywords are mutually exclusive.
gateway_address ipv6_gateway	*ipv6-address*	The gateway IP address for a route in an IPv6 to IPv6 network. The **6to4_gateway** and **ipv6_gateway** keywords are mutually exclusive.
metric	*number*	The metric (integer) for this route. The number can be from 2 to 15.

Command example:

```
FVS336Gv2> net routing static ipv6 configure SFO2
net-config[static-routing-ipv6]> active_flag Y
net-config[static-routing-ipv6]> destination_address 2002:201b:24e2::1001
```

```
net-config[static-routing-ipv6]> prefix 64
net-config[static-routing-ipv6]> interface WAN1
net-config[static-routing-ipv6]> gateway_address ipv6_gateway FE80::2001:5efe:ab23
net-config[static-routing-ipv6]> metric 2
net-config[static-routing-ipv6]> save
```

Related show command: *show net routing static ipv6 setup*

---

net routing static ipv6 delete <route name>

This command deletes a static IPv6 route by deleting its name.

Format	**net routing static ipv6 delete** *<route name>*
Mode	net

Related show command: *show net routing static ipv6 setup*

---

net routing static ipv6 delete_all

This command deletes all static IPv6 routes.

Format	**net routing static ipv6 delete_all**
Mode	net

Related show command: *show net routing static ipv6 setup*

Security Mode Configuration Commands

4

This chapter explains the configuration commands, keywords, and associated parameters in the security mode. The chapter includes the following sections:

- *Security Services Commands*
- *Security Schedules Command*
- *IPv4 Add Firewall Rule and Edit Firewall Rule Commands*
- *IPv4 General Firewall Commands*
- *IPv6 Firewall Commands*
- *Attack Check and IGMP Passthrough Commands*
- *Session Limit, Time-Out, and Advanced Commands*
- *Address Filter and IP/MAC Binding Commands*
- *Port Triggering Commands*
- *UPnP Command*
- *Bandwidth Profile Commands*
- *Content Filtering Commands*

IMPORTANT:

After you issue a command that includes the word `configure`, `add`, or `edit`, you must save (or cancel) your changes. For more information, see *Configuration Commands: Save Commands* on page 13.

Security Services Commands

This section describes the following commands:

- *security services add*
- *security services edit <row id>*
- *security services delete <row id>*
- *security services service_group add*
- *security services service_group edit <row id>*
- *security services service_group delete <row id>*
- *security services qos_profile add*
- *security services qos_profile edit <row id>*
- *security services qos_profile delete <row id>*
- *security services ip_group add*
- *security services ip_group edit <row id>*
- *security services ip_group delete <row id>*
- *security services ip_group add_ip_to <group name>*
- *security services ip_group delete_ip <row id>*

security services add

This command configures a new firewall custom service. After you issue the **`security services add`** command, you enter the security-config [custom-service] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**`security services add`**
	Mode	security
Step 2	**Format**	**`name`** <service *name*> **`protocol`** {**`TCP`** {**`start_port`** <*number*>} {**`finish_port`** <*number*>} | **`UDP`** {**`start_port`** <*number*>} {**`finish_port`** <*number*>} | **`ICMP`** {**`icmp_type`** <*number*> | **`ICMPv6`** {**`icmp_type`** <*number*>}}
	Mode	security-config [custom-service]

Keyword	Associated Keyword to Select or Parameter to Type	Description
`name`	*`service name`*	The name (alphanumeric string) of the service.
`protocol`	**`TCP`**, **`UDP`**, **`ICMP`**, or **`ICMPv6`**	Specifies the protocol type that applies to the service.
`start_port`	*`number`*	For TCP and UDP, the start port number (integer) of the range used by the destination user. Valid numbers are from 1 to 65,535.

Keyword	Associated Keyword to Select or Parameter to Type	Description
finish_port	*number*	For TCP and UDP, the end port number (integer) of the range used by the destination user. Valid numbers are from 1 to 65,535.
icmp_type	*number*	The ICMP type (integer) used by the destination user.

Command example:

```
FVS336Gv2> security services add
security-config[custom-service]> name Traceroute
security-config[custom-service]> protocol ICMP
security-config[custom-service]> icmp_type 20
security-config[custom-service]> save
```

Related show command: *show security services setup*

security services edit <row id>

This command configures an existing firewall custom service. After you issue the **security services edit** command to specify the row to be edited, you enter the security-config [custom-service] mode and then you can edit the service. You cannot change the service name.

Step 1

Format **security services edit** <*row id*>

Mode security

Step 2

Format **protocol** {**TCP** {**start_port** <*number*>} {**finish_port** <*number*>} |
UDP {**start_port** <*number*>} {**finish_port** <*number*>} |
ICMP {**icmp_type** <*number*> | **ICMPv6** {**icmp_type** <*number*>}}

Mode security-config [custom-service]

Keyword	Associated Keyword to Select or Parameter to Type	Description
protocol	**TCP**, **UDP**, **ICMP**, or **ICMPv6**	Specifies the protocol type that applies to the service.
start_port	*number*	For TCP and UDP, the start port number (integer) of the range used by the destination user. Valid numbers are from 1 to 65,535.
finish_port	*number*	For TCP and UDP, the end port number (integer) of the range used by the destination user. Valid numbers are from 1 to 65,535.
icmp_type	*number*	The ICMP type (integer) used by the destination user.

Related show command: *show security services setup*

security services delete <row id>

This command deletes a custom security service by deleting its row ID.

Format	**security services delete** *<row id>*
Mode	security

Related show command: *show security services setup*

---

security services service_group add

This command configures a new service group. After you issue the **security services service_group add** command, you enter the security-config [service-group] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**security services service_group add**
	Mode	security
Step 2	**Format**	**service_group_name** *<name>* **service_add** *<name>* **service_remove** *<name>*
	Mode	security-config [service-group]

Keyword	Associated Parameter to Type	Description
service_group_name	*name*	The name for the service group.
service_add	*name*	The name of the service to add to the service group. You add multiple services to one service group.
service_remove	*name*	The name of the service to remove from the service group.

Related show command: *show security services service_group setup*

---

security services service_group edit <row id>

This command configures an existing service group. After you issue the **security services service_group edit** command to specify the row to be edited, you enter the security-config [service-group] mode and then you can edit the service group.

Step 1	**Format**	**security services service_group edit** *<row id>*
	Mode	security

Step 2	**Format**	**service_group_name** *<name>* **service_add** *<name>* **service_remove** *<name>*
	Mode	security-config [service-group]

Keyword	Associated Parameter to Type	Description
service_group_name	*name*	The name for the service group.
service_add	*name*	The name of the service to add to the service group. You add multiple services to one service group.
service_remove	*name*	The name of the service to remove from the service group.

Related show command: *show security services service_group setup*

security services service_group delete <row id>

This command deletes a custom security service by deleting its row ID.

Format	**security services delete** *<row id>*
Mode	security

Related show command: *show security services service_group setup*

security services qos_profile add

This command configures a new Quality of Service (QoS) profile that you can associate with a nonblocking inbound or outbound IPv4 firewall rule. After you issue the **security services qos_profile add** command, you enter the security-config [qos-profile] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**security services qos_profile add**
	Mode	security
Step 2	**Format**	**profile_name** *<profile name>* **remark** {**N** | **Y** {**qos_type** {**IP-Precedence** | **DSCP**} {**qos_value** *<number>*}}} **qos_priority** {**Default** | **High** | **Medium-high** | **Medium** | **Low**}
	Mode	security-config [qos-profile]

Keyword	Associated Keyword to Select or Parameter to Type	Description
profile_name	*profile name*	The name (alphanumeric string) of the profile.
remark	**Y** or **N**	Specifies whether or not packets are remarked. If you select **Y**, you also must issue the **qos_type** keyword to specify the traffic classification method and the **qos_value** keyword to specify the associated value.
qos_type	**IP-Precedence** or **DSCP**	Specifies the traffic classification method: • **IP-Precedence**. A legacy method that sets the priority in the ToS byte of an IP header. You must issue the **qos_value** keyword to specify the IP precedence value. • **DSCP**. A method that sets the Differentiated Services Code Point (DSCP) in the Differentiated Services (DS) field (which is the same as the ToS byte) of an IP header. You must issue the **qos_value** keyword to specify the DSCP value.
qos_value	*number*	The following two options are available: • If the **qos_type** keyword is set to **IP-Precedence**, the IP precedence value, from 0 through 7. Packets are remarked with this value. • If the **qos_type** keyword is set to **DSCP**, the DSCP value, from 1 through 63. Packets are remarked with this value.
qos_priority	**Default**, **High**, **Medium-high**, **Medium**, or **Low**	Specifies the priority queue that determines the allocation of excess bandwidth and the classification level of the packets among other priority queues on the VPN firewall: • **Default**. Traffic is mapped based on the ToS field in the packet's IP header. • **High**. This queue includes the following DSCP values: AF41, AF42, AF43, AF44, and CS4. • **Medium-high**. This queue includes the following DSCP values: AF31, AF32, AF33, AF34, and CS3. • **Medium**. This queue includes the following DSCP values: AF21, AF22, AF23, AF24, and CS2. • **Low**. This queue includes the following DSCP values: AF11, AF12, AF13, AF14, CS1, 0, and all other values.

Command example:

```
FVS336Gv2> security services qos_profile add
security-config[qos-profile]> profile name Voice
security-config[qos-profile]> remark Y
security-config[qos-profile]> qos_type DSCP
security-config[qos-profile]> qos_value 24
security-config[qos-Profile]> qos_priority High
security-config[qos-Profile]> save
```

Related show command: *show security services qos_profile setup*

security services qos_profile edit <row id>

This command configures an existing Quality of Service (QoS) profile that you can associate with a nonblocking inbound or outbound IPv4 firewall rule. After you issue the **security services qos_profile edit** command to specify the row to be edited, you enter the security-config [qos-profile] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. You cannot change the name of the profile.

Step 1	**Format**	**security services qos_profile edit** *<row id>*
	Mode	security
Step 2	**Format**	**remark** {**N** | **Y** {**qos_type** {**IP-Precedence** | **DSCP**} {**qos_value** *<number>*}}} **qos_priority** {**Default** | **High** | **Medium-high** | **Medium** | **Low**}
	Mode	security-config [qos-profile]

Keyword	Associated Keyword to Select or Parameter to Type	Description
remark	**Y** or **N**	Specifies whether or not packets are remarked. If you select **Y**, you also must issue the **qos_type** keyword to specify the traffic classification method and the **qos_value** keyword to specify the associated value.
qos_type	**IP-Precedence** or **DSCP**	Specifies the traffic classification method: • **IP-Precedence**. A legacy method that sets the priority in the ToS byte of an IP header. You must issue the **qos_value** keyword to specify the IP precedence value. • **DSCP**. A method that sets the Differentiated Services Code Point (DSCP) in the Differentiated Services (DS) field (which is the same as the ToS byte) of an IP header. You must issue the **qos_value** keyword to specify the DSCP value.
qos_value	*number*	The following two options are available: • If the **qos_type** keyword is set to **IP-Precedence**, the IP precedence value, from 0 through 7. Packets are remarked with this value. • If the **qos_type** keyword is set to **DSCP**, the DSCP value, from 1 through 63. Packets are remarked with this value.

Keyword	Associated Keyword to Select or Parameter to Type	Description
qos_priority	**Default**, **High**, **Medium-high**, **Medium**, or **Low**	Specifies the priority queue that determines the allocation of excess bandwidth and the classification level of the packets among other priority queues on the VPN firewall: • **Default**. Traffic is mapped based on the ToS field in the packet's IP header. • **High**. This queue includes the following DSCP values: AF41, AF42, AF43, AF44, and CS4. • **Medium-high**. This queue includes the following DSCP values: AF31, AF32, AF33, AF34, and CS3. • **Medium**. This queue includes the following DSCP values: AF21, AF22, AF23, AF24, and CS2. • **Low**. This queue includes the following DSCP values: AF11, AF12, AF13, AF14, CS1, 0, and all other values.

Related show command: *show security services qos_profile setup*

security services qos_profile delete <row id>

This command deletes a QoS profile by deleting its row ID.

Format	**security services qos_profile delete** *<row id>*
Mode	security

Related show command: *show security services qos_profile setup*

security services ip_group add

This command configures a new LAN or WAN IP group. After you issue the **security services ip_group add** command, you enter the security-config [ip-group] mode and then you can configure the group type and name in the order that you prefer.

Step 1	**Format**	**security services ip_group add**
	Mode	security
Step 2	**Format**	**ip_group_type** {**LAN-Group** | **WAN-Group**} **ip_group_name** *<group name>*
	Mode	security-config [ip-group]

Keyword	Associated Keyword to Select or Parameter to Type	Description
ip_group_type	**LAN-Group** or **WAN-Group**	Specifies the type of IP group: • **LAN-Group**. The group can be used as a firewall object in an IPv4 LAN firewall rule. • **WAN-Group**. The group can be used as a firewall object in an IPv4 WAN firewall rule.
ip_group_name	*group name*	The name (alphanumeric string) of the group.

Command example:

```
FVS336Gv2> security services ip_group add
security-config[ip-group]> ip_group_type LAN-Group
security-config[ip-group]> ip_group_name TechSupport
security-config[ip-group]> save
```

Related show command: *show security services ip_group ip_setup*

security services ip_group edit <row id>

This command configures an existing LAN or WAN IP group. After you issue the **security services ip_group edit** command to specify the row to be edited, you enter the security-config [ip-group] mode and then you can configure the group type and name in the order that you prefer.

Step 1	**Format**	**security services ip_group edit** *<row id>*
	Mode	security
Step 2	**Format**	**ip_group_type** {**LAN-Group** | **WAN-Group**} **ip_group_name** *<group name>*
	Mode	security-config [ip-group]

Keyword	Associated Keyword to Select or Parameter to Type	Description
ip_group_type	**LAN-Group** or **WAN-Group**	Specifies the type of IP group: • **LAN-Group**. The group can be used as a firewall object in an IPv4 LAN firewall rule. • **WAN-Group**. The group can be used as a firewall object in an IPv4 WAN firewall rule.
ip_group_name	*group name*	The name (alphanumeric string) of the group.

Related show command: *show security services ip_group ip_setup*

security services ip_group delete <row id>

This command deletes a LAN or WAN IP group by deleting its row ID.

Format	**security services ip_group delete** *<row id>*
Mode	security

Related show command: *show security services ip_group ip_setup*

---

security services ip_group add_ip_to <group name>

This command adds an IPv4 address to a LAN or WAN IP group. After you issue the **security services ip_group add_ip_to** command to specify the LAN IP or WAN IP group name to which an IP address is to be added, you enter the security-config [ip-group-add-ip] mode and then you can add the IP address.

Step 1	**Format**	**security services ip_group add_ip_to** *<group name>*
	Mode	security
Step 2	**Format**	**ip_address** *<ipaddress>*
	Mode	security-config [ip-group-add-ip]

Keyword	Associated Parameter to Type	Description
ip_address	*ipaddress*	The IPv4 address to be assigned to the IP group.

Command example:

```
FVS336Gv2> security services ip_group add_ip_to TechSupport
security-config[ipGroup-Ip]> ip_address 10.55.3.201
security-config[ipGroup-Ip]> save
```

Related show command: *show security services ip_group ip_setup*

---

security services ip_group delete_ip <row id>

This command removes an IP address from a LAN or WAN IP group by deleting the row ID of the IP address.

Format	**security services ip_group delete_ip** *<row id>*
Mode	security

Related show command: *show security services ip_group ip_setup*

Security Schedules Command

This section describes the **security schedules edit {1 | 2 | 3}** command.

security schedules edit {1 | 2 | 3}

This command configures one of the three security schedules. After you issue the **security schedule edit** command to specify the row (that is, the schedule: 1, 2, or 3) to be edited, you enter the security-config [schedules] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1 **Format** **security schedules edit {1 | 2 | 3}**

Mode security

Step 2 **Format** **{days all {Y | N {[days sunday {Y | N}] [days monday {Y | N}] [days tuesday {Y | N}] [days wednesday {Y | N}] [days thursday {Y | N}] [days friday {Y | N}] [days saturday {Y | N}]}}}**

{time_of-day all_enable {Y | N {time_of-day start hours <hour>**}**
{time_of-day start mins <*minute*>**} {time_of-day start meridiem {AM | PM}} {time_of-day end hours** <*hour*>**}**
{time_of-day day end mins <*minute*>**} {time_of-day end meridiem {AM | PM}}}}**

Mode security-config [schedules}

Keyword (consists of two separate words)	Associated Keyword to Select or Parameter to Type	Description
days all	**Y** or **N**	Specifies whether or not the schedule is active on all days.
days sunday	**Y** or **N**	Specifies whether or not the schedule is active on Sundays.
days monday	**Y** or **N**	Specifies whether or not the schedule is active on Mondays.
days tuesday	**Y** or **N**	Specifies whether or not the schedule is active on Tuesdays.
days wednesday	**Y** or **N**	Specifies whether or not the schedule is active on Wednesdays.
days thursday	**Y** or **N**	Specifies whether or not the schedule is active on Thursdays.
days friday	**Y** or **N**	Specifies whether or not the schedule is active on Fridays.
days saturday	**Y** or **N**	Specifies whether or not the schedule is active on Saturdays.

Keyword (consists of two separate words)	Associated Keyword to Select or Parameter to Type	Description
time_of_day all_enable	**Y** or **N**	Specifies whether or not the schedule is active all day.
time_of_day start hours	*hour*	The schedule starts at the specified hour in the 12-hour format HH (00 to 12).
time_of_day start mins	*minute*	The schedule starts at the specified minute in the format MM (00 to 59).
time_of_day start meridiem	**AM** or **PM**	Specifies the meridiem for the start time.
time_of_day end hours	*hour*	The schedule ends at the specified hour in the 12-hour format HH (00 to 12).
time_of_day end mins	*minute*	The schedule ends at the specified minute in the format MM (00 to 59).
time_of_day end meridiem	**AM** or **PM**	Specifies the meridiem for the end time.

Command example:

```
FVS336Gv2> security schedule edit 1
security-config[schedules]> days monday Y
security-config[schedules]> days tuesday Y
security-config[schedules]> days wednesday Y
security-config[schedules]> days thursday Y
security-config[schedules]> days friday Y
security-config[schedules]> time_of_day start hours 07
security-config[schedules]> time_of_day start mins 30
security-config[schedules]> time_of_day start meridiem AM
security-config[schedules]> time_of_day end hours 08
security-config[schedules]> time_of_day end mins 00
security-config[schedules]> time_of_day end meridiem PM
security-config[schedules]> save
```

Related show command: *show security schedules setup*

IPv4 Add Firewall Rule and Edit Firewall Rule Commands

This section describes the following commands:

- *security firewall ipv4 add_rule lan_wan outbound*
- *security firewall ipv4 edit_rule lan_wan outbound <row id>*
- *security firewall ipv4 add_rule lan_wan inbound*
- *security firewall ipv4 edit_rule lan_wan inbound <row id>*
- *security firewall ipv4 add_rule dmz_wan outbound*
- *security firewall ipv4 edit_rule dmz_wan outbound <row id>*
- *security firewall ipv4 add_rule dmz_wan inbound*
- *security firewall ipv4 edit_rule dmz_wan inbound <row id>*
- *security firewall ipv4 add_rule lan_dmz outbound*
- *security firewall ipv4 edit_rule lan_dmz outbound <row id>*
- *security firewall ipv4 add_rule lan_dmz inbound*
- *security firewall ipv4 edit_rule lan_dmz inbound <row id>*

security firewall ipv4 add_rule lan_wan outbound

This command configures a new IPv4 LAN WAN outbound firewall rule. After you issue the **security firewall ipv4 add_rule lan_wan outbound** command, you enter the security-config [firewall-ipv4-lan-wan-outbound] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the **action** keyword determines which other keywords and parameters you can apply to a rule.

Step 1	**Format**	**security firewall ipv4 add_rule lan_wan outbound**
	Mode	security
Step 2	**Format**	**service_name** {**default_services** *<default service name>* | {**custom_services** *<custom service name>*} **action** {**ALWAYS_BLOCK** | **ALWAYS_ALLOW** | **BLOCK_BY_SCHEDULE_ELSE_ALLOW** {**schedule** {**Schedule1** | **Schedule2** | **Schedule3**}} | **ALLOW_BY_SCHEDULE_ELSE_BLOCK** {**schedule** {**Schedule1** | **Schedule2** | **Schedule3**}}} **lan_users** {{**address_wise** {**ANY** | **SINGLE_ADDRESS** {**lan_user_start_ip** *<ipaddress>*} | **ADDRESS_RANGE** {**lan_user_start_ip** *<ipaddress>*} {**lan_user_end_ip** *<ipaddress>*}} | **group_wise** *<group name>*}} **wan_users** {{**address_wise** {**ANY** | **SINGLE_ADDRESS** {**wan_user_start_ip** *<ipaddress>*} | **ADDRESS_RANGE** {**wan_user_start_ip** *<ipaddress>*} {**wan_user_end_ip** *<ipaddress>*}} | **group_wise** *<group name>*}}

```
qos_profile <profile name>
log {NEVER | ALWAYS}
bandwidth_profile <profile name>
nat_ip {type {Auto | WAN1 | WAN2} | address <ipaddress>}
```

Mode security-config [firewall-ipv4-lan-wan-outbound]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Service name, action, and schedule		
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the firewall rule applies.
action	**ALWAYS_BLOCK**, **ALWAYS_ALLOW**, **BLOCK_BY_SCHEDULE_ELSE_ALLOW**, or **ALLOW_BY_SCHEDULE_ELSE_BLOCK**	Specifies the type of action to be enforced by the rule.
schedule	**Schedule1**, **Schedule2**, or **Schedule3**	Specifies the schedule, if any, that applies to the rule.
LAN user addresses or LAN group and WAN user addresses		
lan_users address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of LAN address. The **address_wise** and **group_wise** keywords are mutually exclusive.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
lan_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **lan_users address_wise** keywords are set to **SINGLE_ADDRESS**. • The start IP address if the **lan_users address_wise** keywords are set to **ADDRESS_RANGE**.
lan_user_end_ip	*ipaddress*	The end IP address if the **lan_users address_wise** keywords are set to **ADDRESS_RANGE**.
lan_users group_wise	*group name*	The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specify with the *net lan lan_groups edit <row id> <new group name>* command. The LAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.
wan_users address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN address. The **address_wise** and **group_wise** keywords are mutually exclusive.
wan_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **wan_users** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **wan_users** keyword is set to **ADDRESS_RANGE**.
wan_user_end_ip	*ipaddress*	The end IP address if the **wan_users** keyword is set to **ADDRESS_RANGE**.
wan_users group_wise	*group name*	The name of the WAN IP group. The WAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
QoS profile, logging, bandwidth profile, and NAT IP address		
qos_profile	*profile name*	The name of the QoS profile that you specify with the *security services qos_profile add* command.
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.
bandwidth_profile	*profile name*	The name of the bandwidth profile that you specify with the *security bandwidth profile add* command.
nat_ip type	**Auto**, **WAN1**, or **WAN2**	Specifies the type of NAT IP address for a nonblocking rule: • **Auto**. The source address of the outgoing packets is autodetected through the configured routing and load balancing rules. • **WAN1** or **WAN2**. The IP address of the selected WAN interface. **Note:** The **nat_ip type** and **nat_ip address** keywords are mutually exclusive.
nat_ip address	*ipaddress*	The NAT IP address, if the address is different from the IP address of a WAN interface, for example, a secondary WAN IP address. **Note:** The **nat_ip type** and **nat_ip address** keywords are mutually exclusive.

Command example:

```
FVS336Gv2> security firewall ipv4 add_rule lan_wan outbound
security-config[firewall-ipv4-lan-wan-outbound]> service_name default_services HTTP
security-config[firewall-ipv4-lan-wan-outbound]> action ALWAYS_ALLOW
security-config[firewall-ipv4-lan-wan-outbound]> lan_users group_wise SalesAmericas
security-config[firewall-ipv4-lan-wan-outbound]> wan_users address_wise ANY
security-config[firewall-ipv4-lan-wan-outbound]> bandwidth profile PriorityQueue
security-config[firewall-ipv4-lan-wan-outbound]> nat_ip type Auto
security-config[firewall-ipv4-lan-wan-outbound]> log NEVER
security-config[firewall-ipv4-lan-wan-outbound]> save
```

Related show command: *show security firewall ipv4 setup lan_wan*

security firewall ipv4 edit_rule lan_wan outbound <row id>

This command configures an existing IPv4 LAN WAN outbound firewall rule. After you issue the **security firewall ipv4 edit_rule lan_wan outbound** command to specify the row to be edited (for row information, see the output of the *show security firewall ipv4 setup lan_wan* command), you enter the security-config [firewall-ipv4-lan-wan-outbound] mode. You can then edit one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the **action** keyword determines which other keywords and parameters you can apply to a rule.

Step 1

Format **security firewall ipv4 edit_rule lan_wan outbound** *<row id>*

Mode security

Step 2

Format

```
service_name {default_services <default service name> |
   {custom_services <custom service name>}
action {ALWAYS_BLOCK | ALWAYS_ALLOW |
   BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 |
   Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK
   {schedule {Schedule1 | Schedule2 | Schedule3}}}

lan_users {{address_wise {ANY | SINGLE_ADDRESS
   {lan_user_start_ip <ipaddress>} | ADDRESS_RANGE
   {lan_user_start_ip <ipaddress>} {lan_user_end_ip
   <ipaddress>}} | group_wise <group name>}}
wan_users {{address_wise {ANY | SINGLE_ADDRESS
   {wan_user_start_ip <ipaddress>} | ADDRESS_RANGE
   {wan_user_start_ip <ipaddress>} {wan_user_end_ip
   <ipaddress>}} | group_wise <group name>}}

qos_profile <profile name>
log {NEVER | ALWAYS}
bandwidth_profile <profile name>
nat_ip {type {Auto | WAN1 | WAN2} | address <ipaddress>}
```

Mode security-config [firewall-ipv4-lan-wan-outbound]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Service name, action, and schedule		
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the firewall rule applies.
action	**ALWAYS_BLOCK**, **ALWAYS_ALLOW**, **BLOCK_BY_SCHEDULE_ELSE_ALLOW**, or **ALLOW_BY_SCHEDULE_ELSE_BLOCK**	Specifies the type of action to be enforced by the rule.
schedule	**Schedule1**, **Schedule2**, or **Schedule3**	Specifies the schedule, if any, that applies to the rule.
LAN user addresses or LAN group and WAN user addresses		
lan_users address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of LAN address. The **address_wise** and **group_wise** keywords are mutually exclusive.
lan_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **lan_users address_wise** keywords are set to **SINGLE_ADDRESS**. • The start IP address if the **lan_users address_wise** keywords are set to **ADDRESS_RANGE**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
lan_user_end_ip	*ipaddress*	The end IP address if the **lan_users address_wise** keywords are set to **ADDRESS_RANGE**.
lan_users group_wise	*group name*	The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specify with the *net lan lan_groups edit <row id> <new group name>* command. The LAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.
wan_users address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN address. The **address_wise** and **group_wise** keywords are mutually exclusive.
wan_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **wan_users** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **wan_users** keyword is set to **ADDRESS_RANGE**.
wan_user_end_ip	*ipaddress*	The end IP address if the **wan_users** keyword is set to **ADDRESS_RANGE**.
wan_users group_wise	*group name*	The name of the WAN IP group. The WAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.
QoS profile, logging, bandwidth profile, and NAT IP address		
qos_profile	*profile name*	The name of the QoS profile that you specify with the *security services qos_profile add* command.
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
bandwidth_profile	*profile name*	The name of the bandwidth profile that you specify with the *security bandwidth profile add* command.
nat_ip type	**Auto**, **WAN1**, or **WAN2**	Specifies the type of NAT IP address for a nonblocking rule: • **Auto**. The source address of the outgoing packets is autodetected through the configured routing and load balancing rules. • **WAN1** or **WAN2**. The IP address of the selected WAN interface. **Note:** The **nat_ip type** and **nat_ip address** keywords are mutually exclusive.
nat_ip address	*ipaddress*	The NAT IP address, if the address is different from the IP address of a WAN interface, for example, a secondary WAN IP address. **Note:** The **nat_ip type** and **nat_ip address** keywords are mutually exclusive.

Command example: See the command example for the *security firewall ipv4 add_rule lan_wan outbound* command.

Related show command: *show security firewall ipv4 setup lan_wan*

security firewall ipv4 add_rule lan_wan inbound

This command configures a new IPv4 LAN WAN outbound firewall rule. After you issue the **security firewall ipv4 add_rule lan_wan inbound** command, you enter the security-config [firewall-ipv4-lan-wan-inbound] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the **action** keyword determines which other keywords and parameters you can apply to a rule.

Step 1	**Format**	**security firewall ipv4 add_rule lan_wan inbound**
	Mode	security

Step 2 **Format**

```
service_name {default_services <default service name> |
   {custom_services <custom service name>}
action {ALWAYS_BLOCK | ALWAYS_ALLOW |
   BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 |
   Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK
   {schedule {Schedule1 | Schedule2 | Schedule3}}}

send_to_lan_server {SINGLE_ADDRESS {send_to_lan_server_start_ip
   <ipaddress>} | ADDRESS_RANGE {send_to_lan_server_start_ip
   <ipaddress>} {send_to_lan_server_end_ip <ipaddress>}}
translate_to_port_number enable {N | Y
   {translate_to_port_number port <number>}}
{wan_destination_ip_address {WAN1 | WAN2} | RANGE
   {wan_destination_ip_address_start <ipaddress>}
   {wan_destination_ip_address_end <ipaddress>} | OTHER
   {wan_destination_ip_address_start <ipaddress>}}

lan_user {address_wise {ANY | SINGLE_ADDRESS {lan_user_start_ip
   <ipaddress>} | ADDRESS_RANGE {lan_user_start_ip <ipaddress>}
   {lan_user_end_ip <ipaddress>}} | group_wise <group name>}
wan_users {address_wise {ANY | SINGLE_ADDRESS {wan_user_start_ip
   <ipaddress>} | ADDRESS_RANGE {wan_user_start_ip <ipaddress>}
   {wan_user_end_ip <ipaddress>}} | group_wise <group name>}

qos_profile <profile name>
log {NEVER | ALWAYS}
bandwidth_profile <profile name>
```

Mode security-config [firewall-ipv4-lan-wan-inbound]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Service name, action, and schedule		
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the firewall rule applies.
action	**ALWAYS_BLOCK**, **ALWAYS_ALLOW**, **BLOCK_BY_SCHEDULE_ELSE_ALLOW**, or **ALLOW_BY_SCHEDULE_ELSE_BLOCK**	Specifies the type of action to be enforced by the rule.
schedule	**Schedule1**, **Schedule2**, or **Schedule3**	Specifies the schedule, if any, that applies to the rule.
LAN server addresses, port number translation, and WAN destination addresses		
send_to_lan_server	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of LAN address.
send_to_lan_server_start_ip	*ipaddress*	The following two options are available: • The IP address if the **send_to_lan_server** keyword is to **SINGLE_ADDRESS**. • The start IP address if the **send_to_lan_server** keyword is set to **ADDRESS_RANGE**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
send_to_lan_server_end_ip	*ipaddress*	The end IP address if the **send_to_lan_server** keyword is set to **ADDRESS_RANGE**.
translate_to_port_number enable	**Y** or **N**	Enables or disables port forwarding.
translate_to_port_number port	*number*	The port number (integer) if port forwarding is enabled. Valid numbers are 0 through 65,535.
wan_destination_ip_address	**WAN1**, **WAN2**, **RANGE**, or **OTHER**	Specifies the type of destination WAN address for an inbound rule: • **WAN1** or **WAN2**. The IP address of the selected WAN interface. • **RANGE**. A range of public IP addresses, which you must configure by issuing the **wan_destination_ip_address_start** and **wan_destination_ip_address_end** keywords and specifying IPv4 addresses. • **OTHER**. If the IP address is a single IP address that is different from the IP address of a WAN interface, for example, a secondary WAN IP address, issue the **wan_destination_ip_address_start** keyword to specify the address.
wan_destination_ip_address _start	*ipaddress*	The following two options are available: • The start IP address if the **wan_destination_ip_address** keyword is set to **RANGE**. • The IP address if the **wan_destination_ip_address** keyword is set to **OTHER**.
wan_destination_ip_address _end	*ipaddress*	The end IP address if the **wan_destination_ip_address** keyword is set to **RANGE**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
LAN user addresses or LAN group and WAN user addresses		
lan_user address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of LAN address. The **address_wise** and **group_wise** keywords are mutually exclusive. For an inbound rule, this option is available only when the WAN mode is Classical Routing.
lan_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **lan_user address_wise** keywords are set to **SINGLE_ADDRESS**. • The start IP address if the **lan_user address_wise** keywords are set to **ADDRESS_RANGE**.
lan_user_end_ip	*ipaddress*	The end IP address if the **lan_user address_wise** keywords are set to **ADDRESS_RANGE**.
lan_user group_wise	*group name*	The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specify with the *net lan lan_groups edit <row id> <new group name>* command. The LAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive. For an inbound rule, this option is available only when the WAN mode is Classical Routing.
wan_users address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN address. The **address_wise** and **group_wise** keywords are mutually exclusive.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
wan_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **wan_user** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **wan_user** keyword is set to **ADDRESS_RANGE**.
wan_user_end_ip	*ipaddress*	The end IP address if the **wan_user** keyword is set to **ADDRESS_RANGE**.
wan_users group_wise	*group name*	The name of the WAN IP group. The WAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.
QoS profile, logging, and bandwidth profile		
qos_profile	*profile name*	The name of the QoS profile that you specify with the *security services qos_profile add* command.
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.
bandwidth_profile	*profile name*	The name of the bandwidth profile that you specify with the *security bandwidth profile add* command.

Command example:

```
FVS336Gv2> security firewall ipv4 add_rule lan_wan inbound
security-config[firewall-ipv4-lan-wan-inbound]> service_name default_services FTP
security-config[firewall-ipv4-lan-wan-inbound]> action ALWAYS_ALLOW
security-config[firewall-ipv4-lan-wan-inbound]> send_to_lan_server SINGLE_ADDRESS
security-config[firewall-ipv4-lan-wan-inbound]> send_to_lan_server_start_ip 192.168.5.71
security-config[firewall-ipv4-lan-wan-inbound]> wan_destination_ip_address_start 10.168.50.1
security-config[firewall-ipv4-lan-wan-inbound]> wan_user ANY
security-config[firewall-ipv4-lan-wan-inbound]> qos_profile Standard
security-config[firewall-ipv4-lan-wan-inbound]> log NEVER
security-config[firewall-ipv4-lan-wan-inbound]> save
```

Related show command: *show security firewall ipv4 setup lan_wan*

security firewall ipv4 edit_rule lan_wan inbound <row id>

This command configures an existing IPv4 LAN WAN inbound firewall rule. After you issue the **security firewall ipv4 edit_rule lan_wan inbound** command to specify the row to be edited (for row information, see the output of the *show security firewall ipv4 setup lan_wan* command), you enter the security-config [firewall-ipv4-lan-wan-outbound] mode. You can then edit one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the **action** keyword determines which other keywords and parameters you can apply to a rule.

Step 1

Format `security firewall ipv4 edit_rule lan_wan inbound <row id>`

Mode security

Step 2

Format

```
service_name {default_services <default service name> |
   {custom_services <custom service name>}
action {ALWAYS_BLOCK | ALWAYS_ALLOW |
   BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 |
   Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK
   {schedule {Schedule1 | Schedule2 | Schedule3}}}

send_to_lan_server {SINGLE_ADDRESS {send_to_lan_server_start_ip
   <ipaddress>} | ADDRESS_RANGE {send_to_lan_server_start_ip
   <ipaddress>} {send_to_lan_server_end_ip <ipaddress>}}
translate_to_port_number enable {N | Y
   {translate_to_port_number port <number>}}
{wan_destination_ip_address {WAN1 | WAN2} | RANGE
   {wan_destination_ip_address_start <ipaddress>}
   {wan_destination_ip_address_end <ipaddress>} | OTHER
   {wan_destination_ip_address_start <ipaddress>}}

lan_user {address_wise {ANY | SINGLE_ADDRESS {lan_user_start_ip
   <ipaddress>} | ADDRESS_RANGE {lan_user_start_ip <ipaddress>}
   {lan_user_end_ip <ipaddress>}} | group_wise <group name>}
wan_users {address_wise {ANY | SINGLE_ADDRESS {wan_user_start_ip
   <ipaddress>} | ADDRESS_RANGE {wan_user_start_ip <ipaddress>}
   {wan_user_end_ip <ipaddress>}} | group_wise <group name>}

qos_profile <profile name>
log {NEVER | ALWAYS}
bandwidth_profile <profile name>
```

Mode security-config [firewall-ipv4-lan-wan-inbound]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Service name, action, and schedule		
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the firewall rule applies.
action	**ALWAYS_BLOCK**, **ALWAYS_ALLOW**, **BLOCK_BY_SCHEDULE_ELSE_ALLOW**, or **ALLOW_BY_SCHEDULE_ELSE_BLOCK**	Specifies the type of action to be enforced by the rule.
schedule	**Schedule1**, **Schedule2**, or **Schedule3**	Specifies the schedule, if any, that applies to the rule.
LAN server addresses, port number translation, and WAN destination addresses		
send_to_lan_server	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of LAN address.
send_to_lan_server_start_ip	*ipaddress*	The following two options are available: • The IP address if the **send_to_lan_server** keyword is to **SINGLE_ADDRESS**. • The start IP address if the **send_to_lan_server** keyword is set to **ADDRESS_RANGE**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
send_to_lan_server_end_ip	*ipaddress*	The end IP address if the **send_to_lan_server** keyword is set to **ADDRESS_RANGE**.
translate_to_port_number enable	**Y** or **N**	Enables or disables port forwarding.
translate_to_port_number port	*number*	The port number (integer) if port forwarding is enabled. Valid numbers are 0 through 65,535.
wan_destination_ip_address	**WAN1**, **WAN2**, or **RANGE**	Specifies the type of destination WAN address for an inbound rule: • **WAN1** or **WAN2**. The IP address of the selected WAN interface. • **RANGE**. A range of public IP addresses, which you must configure by issuing the **wan_destination_ip_address_start** and **wan_destination_ip_address_end** keywords and specifying IPv4 addresses. • **OTHER**. If the IP address is a single IP address that is different from the IP address of a WAN interface, for example, a secondary WAN IP address, issue the **wan_destination_ip_address_start** keyword to specify the address.
wan_destination_ip_address _start	*ipaddress*	The following two options are available: • The start IP address if the **wan_destination_ip_address** keyword is set to **RANGE**. • The IP address if the **wan_destination_ip_address** keyword is set to **OTHER**.
wan_destination_ip_address _end	*ipaddress*	The end IP address if the **wan_destination_ip_address** keyword is set to **RANGE**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
LAN user addresses or LAN group and WAN user addresses		
lan_user address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of LAN address. The **address_wise** and **group_wise** keywords are mutually exclusive. For an inbound rule, this option is available only when the WAN mode is Classical Routing.
lan_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **lan_user address_wise** keywords are set to **SINGLE_ADDRESS**. • The start IP address if the **lan_user address_wise** keywords are set to **ADDRESS_RANGE**.
lan_user_end_ip	*ipaddress*	The end IP address if the **lan_user address_wise** keywords are set to **ADDRESS_RANGE**.
lan_user group_wise	*group name*	The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specify with the *net lan lan_groups edit <row id> <new group name>* command. The LAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive. For an inbound rule, this option is available only when the WAN mode is Classical Routing.
wan_users address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN address. The **address_wise** and **group_wise** keywords are mutually exclusive.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
wan_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **wan_user** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **wan_user** keyword is set to **ADDRESS_RANGE**.
wan_user_end_ip	*ipaddress*	The end IP address if the **wan_user** keyword is set to **ADDRESS_RANGE**.
wan_users group_wise	*group name*	The name of the WAN IP group. The WAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.
QoS profile, logging, and bandwidth profile		
qos_profile	*profile name*	The name of the QoS profile that you specify with the *security services qos_profile add* command.
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.
bandwidth_profile	*profile name*	The name of the bandwidth profile that you specify with the *security bandwidth profile add* command.

Command example: See the command example for the *security firewall ipv4 add_rule lan_wan inbound* command.

Related show command: *show security firewall ipv4 setup lan_wan*

security firewall ipv4 add_rule dmz_wan outbound

This command configures a new IPv4 DMZ WAN outbound firewall rule. After you issue the **security firewall ipv4 add_rule dmz_wan outbound** command, you enter the security-config [firewall-ipv4-dmz-wan-outbound] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the **action** keyword determines which other keywords and parameters you can apply to a rule.

Step 1	**Format**	**security firewall ipv4 add_rule dmz_wan outbound**
	Mode	security

Step 2 **Format**

```
service_name {default_services <default service name> |
   {custom_services <custom service name>}
action {ALWAYS_BLOCK | ALWAYS_ALLOW |
   BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 |
   Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK
   {schedule {Schedule1 | Schedule2 | Schedule3}}}

dmz_users {ANY | SINGLE_ADDRESS {dmz_user_start_ip <ipaddress>}
   | ADDRESS_RANGE {dmz_user_start_ip <ipaddress>}
   {dmz_user_end_ip <ipaddress>}}
wan_users {address_wise {ANY | SINGLE_ADDRESS {wan_user_start_ip
   <ipaddress>} | ADDRESS_RANGE {wan_user_start_ip <ipaddress>}
   {wan_user_end_ip <ipaddress>}} | group_wise <group name>}

qos_profile <profile name>
log {NEVER | ALWAYS}
nat_ip {type {Auto | WAN1 | WAN2}} | address <ipaddress>}
```

Mode security-config [firewall-ipv4-dmz-wan-outbound]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Service name, action, and schedule		
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the firewall rule applies.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
action	**ALWAYS_BLOCK**, **ALWAYS_ALLOW**, **BLOCK_BY_SCHEDULE_ELSE_ALLOW**, or **ALLOW_BY_SCHEDULE_ELSE_BLOCK**	Specifies the type of action to be enforced by the rule.
schedule	**Schedule1**, **Schedule2**, or **Schedule3**	Specifies the schedule, if any, that applies to the rule.
DMZ user addresses and WAN user addresses		
dmz_users	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of DMZ address.
dmz_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **dmz_users** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **dmz_users** keyword is set to **ADDRESS_RANGE**.
dmz_user_end_ip	*ipaddress*	The end IP address if the **dmz_users** keyword is set to **ADDRESS_RANGE**.
wan_users address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN address. The **address_wise** and **group_wise** keywords are mutually exclusive.
wan_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **wan_user** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **wan_user** keyword is set to **ADDRESS_RANGE**.
wan_user_end_ip	*ipaddress*	The end IP address if the **wan_user** keyword is set to **ADDRESS_RANGE**.
wan_users group_wise	*group name*	The name of the WAN IP group. The WAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
QoS profile, logging, and NAT IP address		
qos_profile	*profile name*	The name of the QoS profile that you specify with the *security services qos_profile add* command.
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.
nat_ip type	**Auto**, **WAN1**, or **WAN2**	Specifies the type of NAT IP address for a nonblocking rule: • **Auto**. The source address of the outgoing packets is autodetected through the configured routing and load balancing rules. • **WAN1** or **WAN2**. The IP address of the selected WAN interface. **Note:** The **nat_ip type** and **nat_ip address** keywords are mutually exclusive.
nat_ip address	*ipaddress*	The NAT IP address, if the address is different from the IP address of a WAN interface, for example, a secondary WAN IP address. **Note:** The **nat_ip type** and **nat_ip address** keywords are mutually exclusive.

Command example:

```
FVS336Gv2> security firewall ipv4 add_rule dmz_wan outbound
security-config[firewall-ipv4-dmz-wan-outbound]> service_name default_services CU-SEEME:TCP
security-config[firewall-ipv4-dmz-wan-outbound]> action BLOCK_BY_SCHEDULE_ELSE_BLOCK
security-config[firewall-ipv4-dmz-wan-outbound]> schedule Schedule2
security-config[firewall-ipv4-dmz-wan-outbound]> dmz_users ANY
security-config[firewall-ipv4-dmz-wan-outbound]> wan_users ANY
security-config[firewall-ipv4-dmz-wan-outbound]> qos_profile Video
security-config[firewall-ipv4-dmz-wan-outbound]> log Never
security-config[firewall-ipv4-dmz-wan-outbound]> nat_ip type WAN1
security-config[firewall-ipv4-dmz-wan-outbound]> save
```

Related show command: *show security firewall ipv4 setup dmz_wan*

security firewall ipv4 edit_rule dmz_wan outbound <row id>

This command configures an existing IPv4 DMZ WAN outbound firewall rule. After you issue the **security firewall ipv4 edit_rule dmz_wan outbound** command to specify the row to be edited (for row information, see the output of the *show security firewall ipv4 setup dmz_wan* command), you enter the security-config [firewall-ipv4-dmz-wan-outbound] mode. You can then edit one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the **action** keyword determines which other keywords and parameters you can apply to a rule.

Step 1

Format

```
security firewall ipv4 edit_rule dmz_wan outbound <row id>
```

Mode security

Step 2

Format

```
service_name {default_services <default service name> |
   {custom_services <custom service name>}
action {ALWAYS_BLOCK | ALWAYS_ALLOW |
   BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 |
   Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK
   {schedule {Schedule1 | Schedule2 | Schedule3}}}

dmz_users {ANY | SINGLE_ADDRESS {dmz_user_start_ip <ipaddress>}
   | ADDRESS_RANGE {dmz_user_start_ip <ipaddress>}
   {dmz_user_end_ip <ipaddress>}}
wan_users {address_wise {ANY | SINGLE_ADDRESS {wan_user_start_ip
   <ipaddress>} | ADDRESS_RANGE {wan_user_start_ip <ipaddress>}
   {wan_user_end_ip <ipaddress>}} | group_wise <group name>}

qos_profile <profile name>
log {NEVER | ALWAYS}
nat_ip {type {Auto | WAN1 | WAN2}} | address <ipaddress>}
```

Mode security-config [firewall-ipv4-dmz-wan-outbound]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Service name, action, and schedule		
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the firewall rule applies.
action	**ALWAYS_BLOCK**, **ALWAYS_ALLOW**, **BLOCK_BY_SCHEDULE_ELSE_ALLOW**, or **ALLOW_BY_SCHEDULE_ELSE_BLOCK**	Specifies the type of action to be enforced by the rule.
schedule	**Schedule1**, **Schedule2**, or **Schedule3**	Specifies the schedule, if any, that applies to the rule.
DMZ user addresses and WAN user addresses		
dmz_users	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of DMZ address.
dmz_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **dmz_users** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **dmz_users** keyword is set to **ADDRESS_RANGE**.
dmz_user_end_ip	*ipaddress*	The end IP address if the **dmz_users** keyword is set to **ADDRESS_RANGE**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
wan_users address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN address. The **address_wise** and **group_wise** keywords are mutually exclusive.
wan_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **wan_user** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **wan_user** keyword is set to **ADDRESS_RANGE**.
wan_user_end_ip	*ipaddress*	The end IP address if the **wan_user** keyword is set to **ADDRESS_RANGE**.
wan_users group_wise	*group name*	The name of the WAN IP group. The WAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.
QoS profile, logging, and NAT IP address		
qos_profile	*profile name*	The name of the QoS profile that you specify with the *security services qos_profile add* command.
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
nat_ip type	**Auto**, **WAN1**, or **WAN2**	Specifies the type of NAT IP address for a nonblocking rule: • **Auto**. The source address of the outgoing packets is autodetected through the configured routing and load balancing rules. • **WAN1** or **WAN2**. The IP address of the selected WAN interface. **Note:** The **nat_ip type** and **nat_ip address** keywords are mutually exclusive.
nat_ip address	*ipaddress*	The NAT IP address, if the address is different from the IP address of a WAN interface, for example, a secondary WAN IP address. **Note:** The **nat_ip type** and **nat_ip address** keywords are mutually exclusive.

Command example: See the command example for the *security firewall ipv4 add_rule dmz_wan outbound* command.

Related show command: *show security firewall ipv4 setup dmz_wan*

security firewall ipv4 add_rule dmz_wan inbound

This command configures a new IPv4 DMZ WAN inbound firewall rule. After you issue the **security firewall ipv4 add_rule dmz_wan inbound** command, you enter the security-config [firewall-ipv4-dmz-wan-inbound] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the **action** keyword determines which other keywords and parameters you can apply to a rule.

Step 1	**Format**	**security firewall ipv4 add_rule dmz_wan inbound**
	Mode	security
Step 2	**Format**	**service_name** {**default_services** *<default service name>* | {**custom_services** *<custom service name>*} **action** {**ALWAYS_BLOCK** | **ALWAYS_ALLOW** | **BLOCK_BY_SCHEDULE_ELSE_ALLOW** {**schedule** {**Schedule1** | **Schedule2** | **Schedule3**}} | **ALLOW_BY_SCHEDULE_ELSE_BLOCK** {**schedule** {**Schedule1** | **Schedule2** | **Schedule3**}}}

```
send_to_dmz_server_ip <ipaddress>
translate_to_port_number enable {N | Y
   {translate_to_port_number port <number>}}
wan_destination_ip_address {WAN1 | WAN2}

dmz_users {ANY | SINGLE_ADDRESS {dmz_user_start_ip <ipaddress>}
   | ADDRESS_RANGE {dmz_user_start_ip <ipaddress>}
   {dmz_user_end_ip <ipaddress>}}
wan_users {address_wise {ANY | SINGLE_ADDRESS {wan_user_start_ip
   <ipaddress>} | ADDRESS_RANGE {wan_user_start_ip <ipaddress>}
   {wan_user_end_ip <ipaddress>}} | group_wise <group name>}

qos_profile <profile name>
log {NEVER | ALWAYS}
```

Mode security-config [firewall-ipv4-dmz-wan-inbound]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Service name, action, and schedule		
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the firewall rule applies.
action	**ALWAYS_BLOCK**, **ALWAYS_ALLOW**, **BLOCK_BY_SCHEDULE_ELSE_ALLOW**, or **ALLOW_BY_SCHEDULE_ELSE_BLOCK**	Specifies the type of action to be enforced by the rule.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
schedule	**Schedule1**, **Schedule2**, or **Schedule3**	Specifies the schedule, if any, that applies to the rule.
DMZ server address, port number translation, and WAN destination address		
send_to_dmz_server_ip	*ipaddress*	The IP address of the DMZ server.
translate_to_port_number enable	**Y** or **N**	Enables or disables port forwarding.
translate_to_port_number port	*number*	The port number (integer) if port forwarding is enabled. Valid numbers are 0 through 65,535.
wan_destination_ip_address	**WAN1** or **WAN2**	Specifies the selected WAN interface as the destination address.
DMZ user addresses and WAN user addresses		
dmz_users	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of DMZ address. For an inbound rule, this option is available only when the WAN mode is Classical Routing.
dmz_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **dmz_users** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **dmz_users** keyword is set to **ADDRESS_RANGE**.
dmz_user_end_ip	*ipaddress*	The end IP address if the **dmz_users** keyword is set to **ADDRESS_RANGE**.
wan_users address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN address. The **address_wise** and **group_wise** keywords are mutually exclusive.
wan_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **wan_user** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **wan_user** keyword is set to **ADDRESS_RANGE**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
wan_user_end_ip	*ipaddress*	The end IP address if the **wan_user** keyword is set to **ADDRESS_RANGE**.
wan_users group_wise	*group name*	The name of the WAN IP group. The WAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.
QoS profile and logging		
qos_profile	*profile name*	The name of the QoS profile that you specify with the *security services qos_profile add* command.
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.

Command example:

```
FVS336Gv2> security firewall ipv4 add_rule dmz_wan inbound
security-config[firewall-ipv4-dmz-wan-inbound]> service_name custom_services
BOOTP_CLIENT
security-config[firewall-ipv4-dmz-wan-inbound]> action ALWAYS_ALLOW
security-config[firewall-ipv4-dmz-wan-inbound]> send_to_dmz_server_ip 192.168.24.112
security-config[firewall-ipv4-dmz-wan-inbound]> translate_to_port_number enable Y
security-config[firewall-ipv4-dmz-wan-inbound]> translate_to_port_number port 6700
security-config[firewall-ipv4-dmz-wan-inbound]> wan_destination_ip_address WAN1
security-config[firewall-ipv4-dmz-wan-inbound]> wan_users Single_Address
security-config[firewall-ipv4-dmz-wan-inbound]> wan_user_start_ip 10.132.215.4
security-config[firewall-ipv4-dmz-wan-inbound]> log Always
security-config[firewall-ipv4-dmz-wan-inbound]> save
```

Related show command: *show security firewall ipv4 setup dmz_wan*

security firewall ipv4 edit_rule dmz_wan inbound <row id>

This command configures an existing IPv4 DMZ WAN inbound firewall rule. After you issue the **security firewall ipv4 edit_rule dmz_wan inbound** command to specify the row to be edited (for row information, see the output of the *show security firewall ipv4 setup dmz_wan* command), you enter the security-config [firewall-ipv4-dmz-wan-inbound] mode. You can then edit one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the **action** keyword determines which other keywords and parameters you can apply to a rule.

Step 1	**Format**	**security firewall ipv4 edit_rule dmz_wan inbound** *<row id>*
	Mode	security

Step 2 **Format**

```
service_name {default_services <default service name> |
   {custom_services <custom service name>}
action {ALWAYS_BLOCK | ALWAYS_ALLOW |
   BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 |
   Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK
   {schedule {Schedule1 | Schedule2 | Schedule3}}}

send_to_dmz_server_ip <ipaddress>
translate_to_port_number enable {N | Y
   {translate_to_port_number port <number>}}
wan_destination_ip_address {WAN1 | WAN2}

dmz_users {ANY | SINGLE_ADDRESS {dmz_user_start_ip <ipaddress>}
   | ADDRESS_RANGE {dmz_user_start_ip <ipaddress>}
   {dmz_user_end_ip <ipaddress>}}
wan_users {address_wise {ANY | SINGLE_ADDRESS {wan_user_start_ip
   <ipaddress>} | ADDRESS_RANGE {wan_user_start_ip <ipaddress>}
   {wan_user_end_ip <ipaddress>}} | group_wise <group name>}

log {NEVER | ALWAYS}
```

Mode security-config [firewall-ipv4-dmz-wan-inbound]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Service name, action, and schedule		
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the firewall rule applies.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the firewall rule applies.
action	**ALWAYS_BLOCK**, **ALWAYS_ALLOW**, **BLOCK_BY_SCHEDULE_ELSE_ALLOW**, or **ALLOW_BY_SCHEDULE_ELSE_BLOCK**	Specifies the type of action to be enforced by the rule.
schedule	**Schedule1**, **Schedule2**, or **Schedule3**	Specifies the schedule, if any, that applies to the rule.
DMZ server address, port number translation, and WAN destination address		
send_to_dmz_server_ip	*ipaddress*	The IP address of the DMZ server.
translate_to_port_number enable	**Y** or **N**	Enables or disables port forwarding.
translate_to_port_number port	*number*	The port number (integer) if port forwarding is enabled. Valid numbers are 0 through 65,535.
wan_destination_ip_address	**WAN1** or **WAN2**	Specifies the selected WAN interface as the destination address.
DMZ user addresses and WAN user addresses		
dmz_users	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of DMZ address. For an inbound rule, this option is available only when the WAN mode is Classical Routing.
dmz_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **dmz_users** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **dmz_users** keyword is set to **ADDRESS_RANGE**.
dmz_user_end_ip	*ipaddress*	The end IP address if the **dmz_users** keyword is set to **ADDRESS_RANGE**.
wan_users address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN address. The **address_wise** and **group_wise** keywords are mutually exclusive.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
wan_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **wan_user** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **wan_user** keyword is set to **ADDRESS_RANGE**.
wan_user_end_ip	*ipaddress*	The end IP address if the **wan_user** keyword is set to **ADDRESS_RANGE**.
wan_users group_wise	*group name*	The name of the WAN IP group. The WAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.
QoS profile and logging		
qos_profile	*profile name*	The name of the QoS profile that you specify with the *security services qos_profile add* command.
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.

Command example: See the command example for the *security firewall ipv4 add_rule dmz_wan inbound* command.

Related show command: *show security firewall ipv4 setup dmz_wan*

security firewall ipv4 add_rule lan_dmz outbound

This command configures a new IPv4 LAN DMZ outbound firewall rule. After you issue the **security firewall ipv4 add_rule lan_dmz outbound** command, you enter the security-config [firewall-ipv4-lan-dmz-outbound] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the **action** keyword determines which other keywords and parameters you can apply to a rule.

Step 1	**Format**	**security firewall ipv4 add_rule lan_dmz outbound**
	Mode	security

Step 2 **Format**

```
service_name {default_services <default service name> |
   {custom_services <custom service name>}
action {ALWAYS_BLOCK | ALWAYS_ALLOW |
   BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 |
   Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK
   {schedule {Schedule1 | Schedule2 | Schedule3}}}

lan_users {address_wise {ANY | SINGLE_ADDRESS {lan_user_start_ip
   <ipaddress>} | ADDRESS_RANGE {lan_user_start_ip <ipaddress>}
   {lan_user_end_ip <ipaddress>}} | group_wise <group name>}
dmz_users {ANY | SINGLE_ADDRESS {dmz_user_start_ip <ipaddress>}
   | ADDRESS_RANGE {dmz_user_start_ip <ipaddress>}
   {dmz_user_end_ip <ipaddress>}}

log {NEVER | ALWAYS}
```

Mode security-config [firewall-ipv4-lan-dmz-outbound]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Service name, action, and schedule		
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the firewall rule applies.
action	**ALWAYS_BLOCK**, **ALWAYS_ALLOW**, **BLOCK_BY_SCHEDULE_ELSE_ALLOW**, or **ALLOW_BY_SCHEDULE_ELSE_BLOCK**	Specifies the type of action to be enforced by the rule.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
schedule	**Schedule1**, **Schedule2**, or **Schedule3**	Specifies the schedule, if any, that applies to the rule.
LAN user addresses or LAN group and DMZ user addresses		
lan_users address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of LAN address. The **address_wise** and **group_wise** keywords are mutually exclusive.
lan_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **lan_users address_wise** keywords are set to **SINGLE_ADDRESS**. • The start IP address if the **lan_users address_wise** keywords are set to **ADDRESS_RANGE**.
lan_user_end_ip	*ipaddress*	The end IP address if the **lan_users address_wise** keywords are set to **ADDRESS_RANGE**.
lan_users group_wise	*group name*	The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specify with the *net lan lan_groups edit <row id> <new group name>* command. The LAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.
dmz_users	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of DMZ address.
dmz_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **dmz_users** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **dmz_users** keyword is set to **ADDRESS_RANGE**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
dmz_user_end_ip	*ipaddress*	The end IP address if the **dmz_users** keyword is set to **ADDRESS_RANGE**.
Logging		
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.

Command example:

```
FVS336Gv2> security firewall ipv4 add_rule lan_dmz outbound
security-config[firewall-ipv4-lan-dmz-outbound]> service_name default_services FTP
security-config[firewall-ipv4-lan-dmz-outbound]> action ALWAYS_ALLOW
security-config[firewall-ipv4-lan-dmz-outbound]> lan_users group_wise GROUP4
security-config[firewall-ipv4-lan-dmz-outbound]> dmz_users ADDRESS_RANGE
security-config[firewall-ipv4-lan-dmz-outbound]> dmz_user_start_ip 176.14.2.30
security-config[firewall-ipv4-lan-dmz-outbound]> dmz_user_end_ip 176.14.2.79
security-config[firewall-ipv4-lan-dmz-outbound]> log Never
security-config[firewall-ipv4-lan-dmz-outbound]> save
```

Related show command: *show security firewall ipv4 setup lan_dmz*

security firewall ipv4 edit_rule lan_dmz outbound <row id>

This command configures an existing IPv4 LAN DMZ outbound firewall rule. After you issue the **security firewall ipv4 edit_rule lan_dmz outbound** command to specify the row to be edited (for row information, see the output of the *show security firewall ipv4 setup lan_dmz* command), you enter the security-config [firewall-ipv4-lan-dmz-outbound] mode. You can then edit one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the **action** keyword determines which other keywords and parameters you can apply to a rule.

Step 1	**Format**	**security firewall ipv4 edit_rule lan_dmz outbound** *<row id>*
	Mode	security
Step 2	**Format**	**service_name** {**default_services** *<default service name>* | {**custom_services** *<custom service name>*} **action** {**ALWAYS_BLOCK** | **ALWAYS_ALLOW** | **BLOCK_BY_SCHEDULE_ELSE_ALLOW** {**schedule** {**Schedule1** | **Schedule2** | **Schedule3**}} | **ALLOW_BY_SCHEDULE_ELSE_BLOCK** {**schedule** {**Schedule1** | **Schedule2** | **Schedule3**}}}

```
lan_users {address_wise {ANY | SINGLE_ADDRESS {lan_user_start_ip
   <ipaddress>} | ADDRESS_RANGE {lan_user_start_ip <ipaddress>}
   {lan_user_end_ip <ipaddress>}} | group_wise <group name>}
dmz_users {ANY | SINGLE_ADDRESS {dmz_user_start_ip <ipaddress>}
   | ADDRESS_RANGE {dmz_user_start_ip <ipaddress>}
   {dmz_user_end_ip <ipaddress>}}

log {NEVER | ALWAYS}
```

Mode security-config [firewall-ipv4-lan-dmz-outbound]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Service name, action, and schedule		
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the firewall rule applies.
action	**ALWAYS_BLOCK**, **ALWAYS_ALLOW**, **BLOCK_BY_SCHEDULE_ELSE_ALLOW**, or **ALLOW_BY_SCHEDULE_ELSE_BLOCK**	Specifies the type of action to be enforced by the rule.
schedule	**Schedule1**, **Schedule2**, or **Schedule3**	Specifies the schedule, if any, that applies to the rule.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
LAN user addresses or LAN group and DMZ user addresses		
lan_users address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of LAN address. The **address_wise** and **group_wise** keywords are mutually exclusive.
lan_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **lan_users address_wise** keywords are set to **SINGLE_ADDRESS**. • The start IP address if the **lan_users address_wise** keywords are set to **ADDRESS_RANGE**.
lan_user_end_ip	*ipaddress*	The end IP address if the **lan_users address_wise** keywords are set to **ADDRESS_RANGE**.
lan_users group_wise	*group name*	The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specify with the *net lan lan_groups edit <row id> <new group name>* command. The LAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.
dmz_users	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of DMZ address.
dmz_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **dmz_users** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **dmz_users** keyword is set to **ADDRESS_RANGE**.
dmz_user_end_ip	*ipaddress*	The end IP address if the **dmz_users** keyword is set to **ADDRESS_RANGE**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Logging		
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.

Command example: See the command example for the *security firewall ipv4 add_rule lan_dmz outbound* command.

Related show command: *show security firewall ipv4 setup lan_dmz*

security firewall ipv4 add_rule lan_dmz inbound

This command configures a new IPv4 LAN DMZ inbound firewall rule. After you issue the **security firewall ipv4 add_rule lan_dmz inbound** command, you enter the security-config [firewall-ipv4-lan-dmz-outbound] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the **action** keyword determines which other keywords and parameters you can apply to a rule.

Step 1

Format

```
security firewall ipv4 add_rule lan_dmz inbound
```

Mode security

Step 2

Format

```
service_name {default_services <default service name> |
   {custom_services <custom service name>}
action {ALWAYS_BLOCK | ALWAYS_ALLOW |
   BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 |
   Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK
   {schedule {Schedule1 | Schedule2 | Schedule3}}}

lan_users {address_wise {ANY | SINGLE_ADDRESS {lan_user_start_ip
   <ipaddress>} | ADDRESS_RANGE {lan_user_start_ip <ipaddress>}
   {lan_user_end_ip <ipaddress>}} | group_wise <group name>}
dmz_users {ANY | SINGLE_ADDRESS {dmz_user_start_ip <ipaddress>}
   | ADDRESS_RANGE {dmz_user_start_ip <ipaddress>}
   {dmz_user_end_ip <ipaddress>}}

log {NEVER | ALWAYS}
```

Mode security-config [firewall-ipv4-lan-dmz-inbound]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Service name, action, and schedule		
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	Specifies the custom service that you configure with the *security services add* command and to which the firewall rule applies.
action	**ALWAYS_BLOCK**, **ALWAYS_ALLOW**, **BLOCK_BY_SCHEDULE_ELSE_ALLOW**, or **ALLOW_BY_SCHEDULE_ELSE_BLOCK**	Specifies the type of action to be enforced by the rule.
schedule	**Schedule1**, **Schedule2**, or **Schedule3**	Specifies the schedule, if any, that is applicable to the rule.
LAN user addresses or LAN group and DMZ user addresses		
lan_users address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of LAN address. The **address_wise** and **group_wise** keywords are mutually exclusive.
lan_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **lan_users address_wise** keywords are set to **SINGLE_ADDRESS**. • The start IP address if the **lan_users address_wise** keywords are set to **ADDRESS_RANGE**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
lan_user_end_ip	*ipaddress*	The end IP address if the **lan_users address_wise** keywords are set to **ADDRESS_RANGE**.
lan_users group_wise	*group name*	The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specify with the *net lan lan_groups edit <row id> <new group name>* command. The LAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.
dmz_users	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of DMZ address.
dmz_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **dmz_users** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **dmz_users** keyword is set to **ADDRESS_RANGE**.
dmz_user_end_ip	*ipaddress*	The end IP address if the **dmz_users** keyword is set to **ADDRESS_RANGE**.
Logging		
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.

Command example:

```
FVS336Gv2> security firewall ipv4 add_rule lan_dmz inbound
security-config[firewall-ipv4-lan-dmz-inbound]> service_name default_services SSH:UDP
security-config[firewall-ipv4-lan-dmz-inbound]> action BLOCK_BY_SCHEDULE_ELSE_ALLOW
security-config[firewall-ipv4-lan-dmz-inbound]> schedule Schedule1
security-config[firewall-ipv4-lan-dmz-inbound]> lan_users address_wise SINGLE_ADDRESS
security-config[firewall-ipv4-lan-dmz-inbound]> lan_user_start_ip 192.168.5.108
security-config[firewall-ipv4-lan-dmz-inbound]> dmz_users SINGLE_ADDRESS
security-config[firewall-ipv4-lan-dmz-inbound]> dmz_user_start_ip 176.16.2.101
security-config[firewall-ipv4-lan-dmz-inbound]> log Always
security-config[firewall-ipv4-lan-dmz-inbound]> save
```

Related show command: *show security firewall ipv4 setup lan_dmz*

security firewall ipv4 edit_rule lan_dmz inbound <row id>

This command configures an existing IPv4 LAN DMZ inbound firewall rule. After you issue the **security firewall ipv4 edit_rule lan_dmz inbound** command to specify the row to be edited (for row information, see the output of the *show security firewall ipv4 setup lan_dmz* command), you enter the security-config [firewall-ipv4-lan-dmz-outbound] mode. You can then edit one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the **action** keyword determines which other keywords and parameters you can apply to a rule.

Step 1	**Format**	**security firewall ipv4 edit_rule lan_dmz inbound** *<row id>*
	Mode	security
Step 2	**Format**	**service_name** {**default_services** *<default service name>* | {**custom_services** *<custom service name>*} **action** {**ALWAYS_BLOCK** | **ALWAYS_ALLOW** | **BLOCK_BY_SCHEDULE_ELSE_ALLOW** {**schedule** {**Schedule1** | **Schedule2** | **Schedule3**}} | **ALLOW_BY_SCHEDULE_ELSE_BLOCK** {**schedule** {**Schedule1** | **Schedule2** | **Schedule3**}}} **lan_users** {**address_wise** {**ANY** | **SINGLE_ADDRESS** {**lan_user_start_ip** *<ipaddress>*} | **ADDRESS_RANGE** {**lan_user_start_ip** *<ipaddress>*} {**lan_user_end_ip** *<ipaddress>*}} | **group_wise** *<group name>*} **dmz_users** {**ANY** | **SINGLE_ADDRESS** {**dmz_user_start_ip** *<ipaddress>*} | **ADDRESS_RANGE** {**dmz_user_start_ip** *<ipaddress>*} {**dmz_user_end_ip** *<ipaddress>*}} **log** {**NEVER** | **ALWAYS**}
	Mode	security-config [firewall-ipv4-lan-dmz-inbound]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Service name, action, and schedule		
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the firewall rule applies.
action	**ALWAYS_BLOCK**, **ALWAYS_ALLOW**, **BLOCK_BY_SCHEDULE_ELSE_ALLOW**, or **ALLOW_BY_SCHEDULE_ELSE_BLOCK**	Specifies the type of action to be enforced by the rule.
schedule	**Schedule1**, **Schedule2**, or **Schedule3**	Specifies the schedule, if any, that is applicable to the rule.
LAN user addresses or LAN group and DMZ user addresses		
lan_users address_wise	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of LAN address. The **address_wise** and **group_wise** keywords are mutually exclusive.
lan_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **lan_users address_wise** keywords are set to **SINGLE_ADDRESS**. • The start IP address if the **lan_users address_wise** keywords are set to **ADDRESS_RANGE**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
lan_user_end_ip	*ipaddress*	The end IP address if the **lan_users address_wise** keywords are set to **ADDRESS_RANGE**.
lan_users group_wise	*group name*	The name of the LAN group or LAN IP group. The LAN group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specify with the *net lan lan_groups edit <row id> <new group name>* command. The LAN IP group name is a name that you specify with the *security services ip_group add* command. The **address_wise** and **group_wise** keywords are mutually exclusive.
dmz_users	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of DMZ address.
dmz_user_start_ip	*ipaddress*	The following two options are available: • The IP address if the **dmz_users** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **dmz_users** keyword is set to **ADDRESS_RANGE**.
dmz_user_end_ip	*ipaddress*	The end IP address if the **dmz_users** keyword is set to **ADDRESS_RANGE**.
Logging		
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.

Command example: See the command example for the *security firewall ipv4 add_rule lan_dmz inbound* command.

Related show command: *show security firewall ipv4 setup lan_dmz*

IPv4 General Firewall Commands

This section describes the following commands:

- *security firewall ipv4 default_outbound_policy {Allow | Block}*
- *security firewall ipv4 delete <row id>*
- *security firewall ipv4 disable <row id>*
- *security firewall ipv4 enable <row id>*

security firewall ipv4 default_outbound_policy {Allow | Block}

This command allows or blocks the IPv4 firewall default outbound policy.

Format	**security firewall ipv4 default_outbound_policy** {**Allow** | **Block**}
Mode	security

Related show commands: *show security firewall ipv4 setup lan_wan*, *show security firewall ipv4 setup dmz_wan*, and *show security firewall ipv4 setup lan_dmz*

---

security firewall ipv4 delete <row id>

This command deletes an IPv4 firewall rule by deleting its row ID.

Format	**security firewall ipv4 delete** *<row id>*
Mode	security

Related show commands: *show security firewall ipv4 setup lan_wan*, *show security firewall ipv4 setup dmz_wan*, and *show security firewall ipv4 setup lan_dmz*

---

security firewall ipv4 disable <row id>

This command disables an IPv4 firewall rule by specifying its row ID.

Format	**security firewall ipv4 disable** *<row id>*
Mode	security

Related show commands: *show security firewall ipv4 setup lan_wan*, *show security firewall ipv4 setup dmz_wan*, and *show security firewall ipv4 setup lan_dmz*

---

security firewall ipv4 enable <row id>

This command enables an IPv4 firewall rule by specifying its row ID.

Format	**security firewall ipv4 enable** *<row id>*
Mode	security

Related show commands: *show security firewall ipv4 setup lan_wan*, *show security firewall ipv4 setup dmz_wan*, and *show security firewall ipv4 setup lan_dmz*

IPv6 Firewall Commands

This section describes the following commands:

- *security firewall ipv6 default_outbound_policy {Allow | Block}*
- *security firewall ipv6 configure*
- *security firewall ipv6 edit <row id>*
- *security firewall ipv6 delete <row id>*
- *security firewall ipv6 disable <row id>*
- *security firewall ipv6 enable <row id>*

security firewall ipv6 default_outbound_policy {Allow | Block}

This command allows or blocks the IPv6 firewall default outbound policy.

Format	**security firewall ipv6 default_outbound_policy** {**Allow** | **Block**}
Mode	security

Related show command: *show security firewall ipv6 setup*

---

security firewall ipv6 configure

This command configures a new IPv6 firewall rule. After you issue the **security firewall ipv6 configure** command, you enter the security-config [firewall-ipv6] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the **action** keyword determines which other keywords and parameters you can apply to a rule.

Step 1 **Format** `security firewall ipv6 configure`

Mode security

Step 2 **Format**

```
from_zone {LAN | WAN | DMZ}
to_zone {LAN | WAN | DMZ}
service_name {default_services <default service name> |
   custom_services <custom service name>}
action {ALWAYS_BLOCK | ALWAYS_ALLOW |
   BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 |
   Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK
   {schedule {Schedule1 | Schedule2 | Schedule3}}}

source_address_type {ANY | SINGLE_ADDRESS {source_start_address
   <ipv6-address>} | ADDRESS_RANGE {source_start_address
   <ipv6-address>} {source_end_address <ipv6-address>}}
destination_address_type {ANY | SINGLE_ADDRESS
   {destination_start_address <ipv6-address>} | ADDRESS_RANGE
   {destination_start_address <ipv6-address>}
   {destination_end_address <ipv6-address>}}

qos_priority {Normal-Service | Minimize-Cost |
   Maximize-Reliability | Maximize-Throughput | Minimize-Delay}
log {NEVER | ALWAYS}
```

Mode security-config [firewall-ipv6]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Direction of service, service name, action, and schedule		
`from_zone`	**LAN**, **WAN**, or **DMZ**	Specifies the outbound direction: • **LAN**. From the LAN. • **WAN**. From the WAN. • **DMZ**. From the DMZ.
`to_zone`	**LAN**, **WAN**, or **DMZ**	Specifies the inbound direction: • **LAN**. To the LAN. • **WAN**. To the WAN. • **DMZ**. To the DMZ.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the firewall rule applies.
action	**ALWAYS_BLOCK**, **ALWAYS_ALLOW**, **BLOCK_BY_SCHEDULE_ELSE_ALLOW**, or **ALLOW_BY_SCHEDULE_ELSE_BLOCK**	Specifies the type of action to be taken by the rule.
schedule	**Schedule1**, **Schedule2**, or **Schedule3**	Specifies the schedule, if any, that is applicable to the rule.
LAN, WAN, and DMZ source and destination IP addresses		
source_address_type	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of source address.
source_start_address	*ipv6-address*	The following two options are available: • The IPv6 address if the **source_address_type** keyword is set to **SINGLE_ADDRESS**. • The start IPv6 address if the **source_address_type** keyword is set to **ADDRESS_RANGE**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
source_end_address	*ipv6-address*	The end IPv6 address if the **source_address_type** keyword is set to **ADDRESS_RANGE**.
destination_address_type	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of destination address.
destination_start_address	*ipv6-address*	The following two options are available: • The IPv6 address if the **destination_address_type** keyword is set to **SINGLE_ADDRESS**. • The start IPv6 address if the **destination_address_type** keyword is set to **ADDRESS_RANGE**.
destination_end_address	*ipv6-address*	The end IPv6 address if the **destination_address_type** keyword is set to **ADDRESS_RANGE**.
QoS priority and logging		
qos_priority	**Normal-Service**, **Minimize-Cost**, **Maximize-Reliability**, **Maximize-Throughput**, or **Minimize-Delay**	Specifies the type of QoS that applies to the rule. You can apply QoS to LAN WAN and DMZ WAN outbound rules only.
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.

Command example:

```
FVS336Gv2> security firewall ipv6 configure
security-config[firewall-ipv6]> from_zone WAN
security-config[firewall-ipv6]> to_zone LAN
security-config[firewall-ipv6]> service_name default_services RTELNET
security-config[firewall-ipv6]> action ALWAYS_ALLOW
security-config[firewall-ipv6]> source_address_type SINGLE_ADDRESS
security-config[firewall-ipv6]> source_start_address 2002::B32:AAB1:fD41
security-config[firewall-ipv6]> destination_address_type SINGLE_ADDRESS
security-config[firewall-ipv6]> destination_start_address FEC0::db8:145
security-config[firewall-ipv6]> log ALWAYS
security-config[firewall-ipv6]> save
```

Related show command: *show security firewall ipv6 setup*

security firewall ipv6 edit <row id>

This command configures an existing IPv6 firewall rule. After you issue the **security firewall ipv6 edit** command to specify the row to be edited (for row information, see the output of the *show security firewall ipv6 setup* command), you enter the security-config [firewall-ipv6] mode.You can then edit one keyword and associated parameter or associated keyword at a time in the order that you prefer. However, note that the setting of the **action** keyword determines which other keywords and parameters you can apply to a rule.

Step 1 **Format** **security firewall ipv6 edit** *<row id>*

Mode security

Step 2 **Format**

```
from_zone {LAN | WAN | DMZ}
to_zone {LAN | WAN | DMZ}
service_name {default_services <default service name> |
   custom_services <custom service name>}
action {ALWAYS_BLOCK | ALWAYS_ALLOW |
   BLOCK_BY_SCHEDULE_ELSE_ALLOW {schedule {Schedule1 |
   Schedule2 | Schedule3}} | ALLOW_BY_SCHEDULE_ELSE_BLOCK
   {schedule {Schedule1 | Schedule2 | Schedule3}}}

source_address_type {ANY | SINGLE_ADDRESS {source_start_address
   <ipv6-address>} | ADDRESS_RANGE {source_start_address
   <ipv6-address>} {source_end_address <ipv6-address>}}
destination_address_type {ANY | SINGLE_ADDRESS
   {destination_start_address <ipv6-address>} | ADDRESS_RANGE
   {destination_start_address <ipv6-address>}
   {destination_end_address <ipv6-address>}}

qos_priority {Normal-Service | Minimize-Cost |
   Maximize-Reliability | Maximize-Throughput | Minimize-Delay}
log {NEVER | ALWAYS}
```

Mode security-config [firewall-ipv6]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Direction of service, service name, action, and schedule		
from_zone	**LAN**, **WAN**, or **DMZ**	Specifies the outbound direction: • **LAN**. From the LAN. • **WAN**. From the WAN. • **DMZ**. From the DMZ.
to_zone	**LAN**, **WAN**, or **DMZ**	Specifies the inbound direction: • **LAN**. To the LAN. • **WAN**. To the WAN. • **DMZ**. To the DMZ.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
service_name default_services	**ANY**, **AIM**, **BGP**, **BOOTP_CLIENT**, **BOOTP_SERVER**, **CU-SEEME:UDP**, **CU-SEEME:TCP**, **DNS:UDP**, **DNS:TCP**, **FINGER**, **FTP**, **HTTP**, **HTTPS**, **ICMP-TYPE-3**, **ICMP-TYPE-4**, **ICMP-TYPE-5**, **ICMP-TYPE-6**, **ICMP-TYPE-7**, **ICMP-TYPE-8**, **ICMP-TYPE-9**, **ICMP-TYPE-10**, **ICMP-TYPE-11**, **ICMP-TYPE-13**, **ICQ**, **IMAP2**, **IMAP3**, **IRC**, **NEWS**, **NFS**, **NNTP**, **PING**, **POP3**, **PPTP**, **RCMD**, **REAL-AUDIO**, **REXEC**, **RLOGIN**, **RTELNET**, **RTSP:TCP**, **RTSP:UDP**, **SFTP**, **SMTP**, **SNMP:TCP**, **SNMP:UDP**, **SNMP-TRAPS:TCP**, **SNMP-TRAPS:UDP**, **SQL-NET**, **SSH:TCP**, **SSH:UDP**, **STRMWORKS**, **TACACS**, **TELNET**, **TFTP**, **RIP**, **IKE**, **SHTTPD**, **IPSEC-UDP-ENCAP**, **IDENT**, **VDOLIVE**, **SSH**, **SIP-TCP**, **SIP-UDP**, **NFS-TCP**, or **RPC-TCP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you configure with the *security services add* command and to which the firewall rule applies.
action	**ALWAYS_BLOCK**, **ALWAYS_ALLOW**, **BLOCK_BY_SCHEDULE_ELSE_ALLOW**, or **ALLOW_BY_SCHEDULE_ELSE_BLOCK**	Specifies the type of action to be taken by the rule.
schedule	**Schedule1**, **Schedule2**, or **Schedule3**	Specifies the schedule, if any, that is applicable to the rule.
LAN, WAN, and DMZ source and destination IP addresses		
source_address_type	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of source address.
source_start_address	*ipv6-address*	The following two options are available: • The IPv6 address if the **source_address_type** keyword is set to **SINGLE_ADDRESS**. • The start IPv6 address if the **source_address_type** keyword is set to **ADDRESS_RANGE**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
source_end_address	*ipv6-address*	The end IPv6 address if the **source_address_type** keyword is set to **ADDRESS_RANGE**.
destination_address_type	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of destination address.
destination_start_address	*ipv6-address*	The following two options are available: • The IPv6 address if the **destination_address_type** keyword is set to **SINGLE_ADDRESS**. • The start IPv6 address if the **destination_address_type** keyword is set to **ADDRESS_RANGE**.
destination_end_address	*ipv6-address*	The end IPv6 address if the **destination_address_type** keyword is set to **ADDRESS_RANGE**.
QoS profile and logging		
qos_priority	**Normal-Service**, **Minimize-Cost**, **Maximize-Reliability**, **Maximize-Throughput**, or **Minimize-Delay**	Specifies the type of QoS that applies to the rule. You can apply QoS to LAN WAN and DMZ WAN outbound rules only.
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.

Command example: See the command example for the *security firewall ipv6 configure* command.

Related show command: *show security firewall ipv6 setup*

security firewall ipv6 delete <row id>

This command deletes an IPv6 firewall rule by deleting its row ID.

Format	**security firewall ipv6 delete** *<row id>*
Mode	security

Related show command: *show security firewall ipv6 setup*

security firewall ipv6 disable <row id>

This command disables an IPv6 firewall rule by specifying its row ID.

Format	**security firewall ipv6 disable** *<row id>*
Mode	security

Related show command: *show security firewall ipv6 setup*

---

security firewall ipv6 enable <row id>

This command enables an IPv6 firewall rule by specifying its row ID.

Format	**security firewall ipv6 enable** *<row id>*
Mode	security

Related show command: *show security firewall ipv6 setup*

Attack Check and IGMP Passthrough Commands

This section describes the following commands:

- *security firewall attack_checks configure ipv4*
- *security firewall attack_checks vpn_passthrough configure*
- *security firewall attack_checks configure ipv6*
- *security firewall igmp configure*
- *security firewall igmp alternate_networks add*
- *security firewall igmp alternate_networks delete*

security firewall attack_checks configure ipv4

This command configures ipv4 WAN and LAN security attack checks. After you issue the **security firewall attack_checks configure ipv4** command, you enter the security-config [attack-checks-ipv4] mode and then you can edit one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**security firewall attack_checks configure ipv4**
	Mode	security

Step 2 **Format** `respond_to_ping_on_internet_ports enable {N | Y {respond_to_ping_on_internet_ports address_type {Any | IP_address {respond_to_ping_on_internet_ports ip_address <ipaddress>}}}}`
`enable_stealth_mode {Y | N}`
`block_tcp_flood {Y | N}`
`block_udp_flood {N | Y {udp_connection_limit <number>}}`
`disable_ping_reply_on_lan {Y | N}`

Mode security-config [attack-checks-ipv4]

Keyword (might consist of two separate words)	Associated Keyword to Select	Description
WAN security checks		
respond_to_ping_on_internet_ports enable	**Y** or **N**	Allows a WAN port to respond to a ping or prevents a WAN port from responding to a ping.
respond_to_ping_on_internet_ports address_type	**Any** or **IP_Address**	Specifies if a WAN port can respond to a ping from any WAN IP address or from a specific IP address only: • **Any**. A WAN port can respond to a ping from any IP address. • **IP_Address**. A WAN port can respond to a ping from a specific IP address only. Issue the **respond_to_ping_on_internet_ports ip_address** keywords to specify the IP address.
respond_to_ping_on_internet_ports ip_address	*ipaddress*	The IP address if the **respond_to_ping_on_internet_ports address_type** keywords are set to **IP_Address**.
enable_stealth_mode	**Y** or **N**	Enables or disables stealth mode.
block_tcp_flood	**Y** or **N**	Blocks or allows TCP floods on the WAN port.
LAN security checks		
block_udp_flood	**Y** or **N**	Blocks or allows UDP floods on LAN ports.
udp_connection_limit	*number*	If UDP floods on LAN ports are allowed, specifies the number of connections that are allowed per second.
disable_ping_reply_on_lan	**Y** or **N**	Allows LAN ports to reply to a ping or prevents LAN ports from replying to a ping.

Command example:

```
FVS336Gv2> security firewall attack_checks configure ipv4
security-config[attack-checks-ipv4]> respond_to_ping_on_internet_ports enable N
security-config[attack-checks-ipv4]> enable_stealth_mode Y
security-config[attack-checks-ipv4]> block_tcp_flood Y
security-config[attack-checks-ipv4]> block_udp_flood N
security-config[attack-checks-ipv4]> disable_ping_reply_on_lan Y
security-config[attack-checks-ipv4]> save
```

Related show command: *show security firewall attack_checks setup ipv4*

security firewall attack_checks vpn_passthrough configure

This command configures VPN pass-through for IPv4 traffic. After you issue the **security firewall attack_checks vpn_passthrough configure** command, you enter the security-config [vpn-passthrough] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**security firewall attack_checks vpn_passthrough configure**
	Mode	security
Step 2	**Format**	**ipsec_enable** {**Y** | **N**} **l2tp_enable** {**Y** | **N**} **pptp_enable** {**Y** | **N**}
	Mode	security-config [vpn-passthrough]

Keyword	Associated Keyword to Select	Description
ipsec_enable	**Y** or **N**	Enables or disables IPSec pass-through.
l2tp_enable	**Y** or **N**	Enables or disables L2TP pass-through.
pptp_enable	**Y** or **N**	Enables or disables PPTP pass-through.

Command example:

```
FVS336Gv2> security firewall attack_checks vpn_passthrough configure
security-config[vpn-passthrough]> ipsec_enable Y
security-config[vpn-passthrough]> l2tp_enable Y
security-config[vpn-passthrough]> pptp_enable N
security-config[vpn-passthrough]> save
```

Related show command: *show security firewall attack_checks vpn_passthrough setup*

security firewall attack_checks configure ipv6

This command configures ipv6 WAN security attack checks. After you issue the **security firewall attack_checks configure ipv6** command, you enter the security-config [attack-checks-ipv6] mode and then you can edit one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**security firewall attack_checks configure ipv6**
	Mode	security
Step 2	**Format**	**respond_to_ping_on_internet_ports enable** {**N** | **Y** {**respond_to_ping_on_internet_ports address_type** {**Any** | **IP_address** {**respond_to_ping_on_internet_ports ip_address** *<ipv6-address>*}}}} **vpn_ipsec_passthrough** {**Y** | **N**}
	Mode	security-config [attack-checks-ipv6]

Keyword (might consist of two separate words)	Associated Keyword to Select	Description
respond_to_ping_on_internet_ports enable	**Y** or **N**	Allows a WAN port to respond to a ping or prevents a WAN port from responding to a ping.
respond_to_ping_on_internet_ports address_type	**Any** or **IP_Address**	Specifies if a WAN port can respond to a ping from any WAN IP address or from a specific IP address only: • **Any**. A WAN port can respond to a ping from any IP address. • **IP_Address**. A WAN port can respond to a ping from a specific IP address only. Issue the **respond_to_ping_on_internet_ports ip_address** keywords to specify the IPv6 address.
respond_to_ping_on_internet_ports ip_address	*ipv6-address*	The IPv6 address if the **respond_to_ping_on_internet_ports address_type** keywords are set to **IP_Address**.
vpn_ipsec_passthrough	**Y** or **N**	Irrespective of the default firewall outbound policy and custom firewall rules, allows IPSec VPN traffic that is initiated from the LAN to reach the WAN or prevents IPSec VPN traffic that is initiated from the LAN from reaching the WAN.

Command example:

```
FVS336Gv2> security firewall attack_checks configure ipv6
security-config[attack-checks-ipv6]> respond_to_ping_on_internet_ports enable N
security-config[attack-checks-ipv6]> vpn_ipsec_passthrough Y
security-config[attack-checks-ipv6]> save
```

Related show command: *show security firewall attack_checks setup ipv6*

security firewall igmp configure

This command enables or disables multicast pass-through by enabling or disabling the IGMP proxy for IPv4 traffic. After you issue the **security firewall igmp configure** command, you enter the security-config [igmp-passthrough] mode and then you can enable or disable the IGMP proxy and select the WAN interface to which the upstream interface must be bound.

Step 1	**Format**	**security firewall igmp configure**
	Mode	security
Step 2	**Format**	**enable_igmp_proxy** {**Y** | **N**} **up_stream_interface** {**WAN1** | **WAN2**}
	Mode	security-config [igmp-passthrough]

Related show command: *show security firewall attack_checks igmp*

security firewall igmp alternate_networks add

This command adds an IP address and subnet mask for a multicast originator that is in a different subnet from the VPN firewall. Specifying a multicast originator in a different subnet is required if the ISP connection is PPPoE or PPTP. After you issue the **security firewall igmp alternate_networks add** command, you enter the security-config [igmp-allowed-networks] mode and then you can add an IP address and subnet mask.

Step 1	**Format**	**security firewall igmp alternate_networks add**
	Mode	security
Step 2	**Format**	**ip_address** *<ipaddress>* **subnet_mask** *<subnet mask>*
	Mode	security-config [igmp-allowed-networks]

Keyword	Associated Parameter to Type	Description
ip_address	*ipaddress*	The IP address of the multicast originator.
subnet_mask	*subnet mask*	The subnet mask of the multicast originator.

Command example:

```
FVS336Gv2> security firewall igmp alternate_networks add
security-config[igmp-allowed-networks]> ip address 192.0.2.1
security-config[igmp-allowed-networks]> subnet_mask 255.255.255.0
security-config[igmp-allowed-networks]> save
```

Related show command: *show security firewall igmp allowed_networks*

security firewall igmp alternate_networks delete

This command deletes an IP address and subnet mask for a multicast originator by deleting its row ID.

Format	**security firewall igmp alternate_networks delete** *<row id>*
Mode	security

Related show command: *show security firewall igmp allowed_networks*

Session Limit, Time-Out, and Advanced Commands

This section describes the following commands:

- *security firewall session_limit configure*
- *security firewall session_settings configure*
- *security firewall advanced algs*

security firewall session_limit configure

This command configures global session limits. After you issue the **security firewall session_limit configure** command, you enter the security-config [session-limit] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**security firewall session_limit configure**
	Mode	security
Step 2	**Format**	**enable** {**Y** | **N**} **session_limit_control** {**Single_IP_cannot_Exceed** | **When_Single_IP_Exceed**} **conn_limit_type** {**Percentage_Of_MaxSessions** | **Number_Of_Sessions**} **user_limit** *<number>* **block_new_session** {**Block_IP_to_add_new_session** {**block_IP_to_add_new_session_for_time** *<seconds>*} | **Block_IPs_all_connections** {**block_IPs_all_connections_for_time** *<seconds>*}}
	Mode	security-config [session-limit]

Keyword	Associated Keyword to Select or Parameter to Type	Description
enable	**Y** or **N**	Enforces or ignores session limits.
session_limit_control	**When_Single_IP_Exceed** or **Single_IP_cannot_Exceed**	Specifies how limit control is implemented: • **When_Single_IP_Exceed**. When the limit is reached, no new session is allowed from the IP address for a specified period, or all sessions from the IP address are terminated and new sessions are blocked for a specified period. Issue the **conn_limit_type** keyword to specify the type of session limit and issue the **block_new_session** keyword to specify the type of blockage. • **Single_IP_cannot_Exceed**. When the limit is reached, no new session is allowed from the IP address. A new session is allowed only when an existing session is terminated or times out. Issue the **conn_limit_type** keyword to specify the type of session limit.
conn_limit_type	**Percentage_Of_MaxSessions** or **Number_Of_Sessions**	Specifies the type of session limits: • **Percentage_Of_MaxSessions**. Specifies a percentage of the total session-connection capacity on the VPN firewall. Issue the **user_limit** keyword to specify a percentage of the total session connection. • **Number_Of_Sessions**. Specifies an absolute number of maximum sessions. Issue the **user_limit** keyword to specify an absolute number of maximum sessions.
user_limit	*number*	The percentage of the total session-connection capacity on the VPN firewall or an absolute number of maximum sessions.

Keyword	Associated Keyword to Select or Parameter to Type	Description
block_new_session	**Block_IP_to_add_new_session** or **Block_IPs_all_connections**	Specifies the type of blockage: • **Block_IP_to_add_new_session**. No new session is allowed from the IP address for a period. Issue the **block_IP_to_add_new_session_for_time** keyword to specify the period in seconds. • **Block_IPs_all_connections**. All sessions from the IP address are terminated, and new sessions are blocked for a period. Issue the **block_IPs_all_connections_for_time** keyword to specify the period in seconds. These options are available only if the **session_limit_control** keyword is set to **When_Single_IP_Exceed**.
block_IP_to_add_new_session_for_time	*seconds*	The period during which no new session is allowed from the IP address.
block_IPs_all_connections_for_time	*seconds*	The period during which all sessions are blocked from the IP address.

Command example:

```
FVS336Gv2> security firewall session_limit configure
security-config[session-limit]> enable Y
security-config[session-limit]> session_limit_control When_Single_IP_Exceed
security-config[session-limit]> conn_limit_type Percentage_Of_MaxSessions
security-config[session-limit]> user_limit 80
security-config[session-limit]> block_new_session Block_IP_to_add_new_session
security-config[session-limit]> block_IP_to_add_new_session_for_time 60
security-config[session-limit]> save
```

Related show command: *show security firewall session_limit*

security firewall session_settings configure

This command configures global session time-outs. After you issue the **security firewall session_settings configure** command, you enter the security-config [session-settings] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**security firewall session_settings configure**
	Mode	security

Step 2	**Format**	**tcp_session_timeout** *<seconds>* **udp_session_timeout** *<seconds>* **icmp_session_timeout** *<seconds>*
	Mode	security-config [session-settings]

Keyword	Associated Parameter to Type	Description
tcp_session_timeout	*seconds*	Specifies the TCP session time-out period (integer) in seconds.
udp_session_timeout	*seconds*	Specifies the UDP session time-out period (integer) in seconds.
icmp_session_timeout	*seconds*	Specifies the ICMP session time-out period (integer) in seconds.

Command example:

```
FVS336Gv2> security firewall session_settings configure
security-config[session-settings]> tcp_session_timeout 1000
security-config[session-settings]> udp_session_timeout 120
security-config[session-settings]> icmp_session_timeout 6
security-config[session-settings]> save
```

Related show command: *show security firewall session_settings*

security firewall advanced algs

This command configures Session Initiation Protocol (SIP) support for the application level gateway (ALG). After you issue the **security firewall advanced algs** command, you enter the security-config [firewall-alg] mode and then you can enable or disable SIP support.

Step 1	**Format**	**security firewall advanced algs**
	Mode	security
Step 2	**Format**	**sip** {**Y** | **N**}
	Mode	security-config [firewall-alg]

Keyword	Associated Keyword to Select	Description
sip	**Y** or **N**	Enables or disables SIP for the ALG.

Command example:

```
FVS336Gv2> security firewall advanced algs
security-config[firewall-alg]> sip N
security-config[firewall-alg]> save
```

Related show command: *show security firewall advanced algs*

Address Filter and IP/MAC Binding Commands

This section describes the following commands:

- *security address_filter mac_filter configure*
- *security address_filter mac_filter source add*
- *security address_filter mac_filter source delete <row id>*
- *security address_filter ip_or_mac_binding add*
- *security address_filter ip_or_mac_binding edit <row id>*
- *security address_filter ip_or_mac_binding delete <row id>*
- *security address_filter ip_or_mac_binding enable_email_log <ip version>*

security address_filter mac_filter configure

This command configures the source MAC address filter. After you issue the **security address_filter mac_filter configure** command, you enter the security-config [mac-filter] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**security address_filter mac_filter configure**
	Mode	security
Step 2	**Format**	**enable** {**N** | **Y** {**policy** {**Permit-And-Block-Rest** | **Block-And-Permit-Rest**}}
	Mode	security-config [mac-filter]

Keyword	Associated Keyword to Select	Description
enable	**Y** or **N**	Enables or disables the source MAC address filter.
policy	**Permit-And-Block-Rest** or **Block-And-Permit-Rest**	Specifies the policy of the source MAC address filter.

Command example:

```
FVS336Gv2> security address_filter mac_filter configure
security-config[mac-filter]> enable Y
security-config[mac-filter]> policy Block-And-Permit-Rest
security-config[mac-filter]> save
```

Related show command: *show security address_filter mac_filter setup*

security address_filter mac_filter source add

This command adds a new MAC address to the MAC address table for the source MAC address filter. After you issue the **security address_filter mac_filter source add** command, you enter the security-config [mac-filter-source] mode and then you can add a MAC address.

Step 1	**Format**	**security address_filter mac_filter source add**
	Mode	security
Step 2	**Format**	**address** *<mac address>*
	Mode	security-config [mac-filter-source]

Keyword	Associated Parameter to Type	Description
address	*mac address*	The MAC address to be added to the MAC address table for the source MAC address filter.

Command example:

```
FVS336Gv2> security address_filter mac_filter source add
security-config[mac-filter-source]> address a1:b2:c3:de:11:22
security-config[mac-filter-source]> save
security-config[mac-filter-source]> address a1:b2:c3:de:11:25
security-config[mac-filter-source]> save
```

Related show command: *show security address_filter mac_filter setup*

---

security address_filter mac_filter source delete <row id>

This command deletes a MAC address from the MAC address table by deleting its row ID.

Format	**security address_filter mac_filter source delete** *<row id>*
Mode	security

Related show command: *show security address_filter mac_filter setup*

---

security address_filter ip_or_mac_binding add

This command configures a new IP/MAC binding rule. After you issue the **security address_filter ip_or_mac_binding add** command, you enter the security-config [ip-or-mac-binding] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**security address_filter ip_or_mac_binding add**
	Mode	security
Step 2	**Format**	**name** *<rule name>* **mac_address** *<mac address>* **ip_version** {**IPv4** {**ip_address** *<ipaddress>*} | **IPv6** {**ip_address6** *<ipv6-address>*}} **log_dropped_packets** {**Y** | **N**}
	Mode	security-config [ip-or-mac-binding]

Keyword	Associated Keyword to Select or Parameter to Type	Description
name	*rule name*	The name (alphanumeric string) of the IP/MAC binding rule.
mac_address	*mac address*	The MAC address to which the IP/MAC binding rule applies.
ip_version	**IPv4** or **IPv6**	Specifies the type of IP address to which the IP/MAC binding rule applies: • **IPv4**. You must issue the **ip_address** keyword and specify an IPv4 address. • **IPv6**. You must issue the **ip_address6** keyword and specify an IPv6 address.
ip_address	*ipaddress*	The IPv4 address to which the IP/MAC binding rule applies.
ip_address6	*ipv6-address*	The IPv6 address to which the IP/MAC binding rule applies.
log_dropped_packets	**Y** or **N**	Enables or disables packet logging for the IP/MAC binding rule.

Command example:

```
FVS336Gv2> security address_filter ip_or_mac_binding add
security-config[ip-or-mac-binding]> name PhoneConfRoom52
security-config[ip-or-mac-binding]> mac_address d1:e1:55:54:8e:7f
security-config[ip-or-mac-binding]> ip_version IPv4
security-config[ip-or-mac-binding]> ip_address 192.151.1.107
security-config[ip-or-mac-binding]> log_dropped_packets N
security-config[ip-or-mac-binding]> save
```

Related show command: *show security address_filter ip_or_mac_binding setup*

security address_filter ip_or_mac_binding edit <row id>

This command configures an existing IP/MAC binding rule. After you issue the **security address_filter ip_or_mac_binding edit** command to specify the row to be edited, you enter the security-config [ip-or-mac-binding] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. You cannot change the name of the rule.

Step 1	**Format**	**security address_filter ip_or_mac_binding edit** *<row id>*
	Mode	security
Step 2	**Format**	**mac_address** *<mac address>* **ip_version** {**IPv4** {**ip_address** *<ipaddress>*} | **IPv6** {**ip_address6** *<ipv6-address>*}} **log_dropped_packets** {**Y** | **N**}
	Mode	security-config [ip-or-mac-binding]

Keyword	Associated Keyword to Select or Parameter to Type	Description
mac_address	*mac address*	The MAC address to which the IP/MAC binding rule applies.
ip_version	**IPv4** or **IPv6**	Specifies the type of IP address to which the IP/MAC binding rule applies: • **IPv4**. You must issue the **ip_address** keyword and specify an IPv4 address. • **IPv6**. You must issue the **ip_address6** keyword and specify an IPv6 address.
ip_address	*ipaddress*	The IPv4 address to which the IP/MAC binding rule applies.
ip_address6	*ipv6-address*	The IPv6 address to which the IP/MAC binding rule applies.
log_dropped_packets	**Y** or **N**	Enables or disables packet logging for the IP/MAC binding rule.

Related show command: *show security address_filter ip_or_mac_binding setup*

security address_filter ip_or_mac_binding delete <row id>

This command deletes an IP/MAC binding rule by deleting its row ID.

Format	**security address_filter ip_or_mac_binding delete** *<row id>*
Mode	security

Related show command: *show security address_filter ip_or_mac_binding setup*

security address_filter ip_or_mac_binding enable_email_log <ip version>

This command configures the email log for IP/MAC binding violations. After you issue the **security address_filter ip_or_mac_binding enable_email_log** command to specify the IP version, you enter the security-config [ip-or-mac-binding] mode and then you can configure the email log setting.

Step 1	**Format**	**security address_filter ip_or_mac_binding enable_email_log {IPv4 | IPv6}**
	Mode	security
Step 2	**Format**	**enable_email_logs {Y | N}**
	Mode	security-config [ip-or-mac-binding]

Keyword	Associated Keyword to Select	Description
enable_email_logs	**Y** or **N**	Enables or disables the email log for IP/MAC binding violations.

Command example:

```
FVS336Gv2> security address_filter ip_or_mac_binding enable_email_log IPv4
security-config[ip-or-mac-binding]> enable_email_logs Y
security-config[ip-or-mac-binding]> save
```

Related show command: *show security address_filter enable_email_log*

Port Triggering Commands

This section describes the following commands:

- *security porttriggering_rules add*
- *security porttriggering_rules edit <row id>*
- *security porttriggering_rules delete <row id>*

security porttriggering_rules add

This command configures a new port triggering rule. After you issue the **security porttriggering_rules add** command, you enter the security-config [porttriggering-rules] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**security porttriggering_rules add**
	Mode	security

Step 2 **Format** **name** <*rule name*>
enable_rule {**Y** | **N**}
protocol {**TCP** | **UDP**}
outgoing_start_port <*number*>
outgoing_end_port <*number*>
incoming_start_port <*number*>
incoming_end_port <*number*>

Mode security-config [porttriggering-rules]

Keyword	Associated Keyword to Select or Parameter to Type	Description
name	*rule name*	The name (alphanumeric string) of the port triggering rule.
enable_rule	**Y** or **N**	Enables or disables the port triggering rule.
protocol	**TCP** or **UDP**	Specifies whether the port uses the TCP or UDP protocol.
outgoing_start_port	*number*	The start port number (integer) of the outgoing traffic range. Valid numbers are from 1025 to 65,535.
outgoing_end_port	*number*	The end port number (integer) of the outgoing traffic range. Valid numbers are from 1025 to 65,535.
incoming_start_port	*number*	The start port number (integer) of the incoming traffic range. Valid numbers are from 1025 to 65,535.
incoming_end_port	*number*	The end port number (integer) of the incoming traffic range. Valid numbers are from 1025 to 65,535.

Command example:

```
FVS336Gv2> security porttriggering_rules add
security-config[porttriggering-rules]> name Skype
security-config[porttriggering-rules]> enable_rule Y
security-config[porttriggering-rules]> protocol TCP
security-config[porttriggering-rules]> outgoing_start_port 61196
security-config[porttriggering-rules]> outgoing_end_port 61196
security-config[porttriggering-rules]> incoming_start_port 61197
security-config[porttriggering-rules]> incoming_end_port 61197
security-config[porttriggering-rules]> save
```

Related show commands: *show security porttriggering_rules setup* and *show security porttriggering_rules status*

security porttriggering_rules edit <row id>

This command configures an existing port triggering rule. After you issue the **security porttriggering_rules edit** command to specify the row to be edited, you enter the security-config [porttriggering-rules] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. You cannot change the name of the rule.

Step 1	**Format**	**security porttriggering_rules edit** *<row id>*
	Mode	security
Step 2	**Format**	**enable_rule** {**Y** | **N**} **protocol** {**TCP** | **UDP**} **outgoing_start_port** *<number>* **outgoing_end_port** *<number>* **incoming_start_port** *<number>* **incoming_end_port** *<number>*
	Mode	security-config [porttriggering-rules]

Keyword	Associated Keyword to Select or Parameter to Type	Description
enable_rule	**Y** or **N**	Enables or disables the port triggering rule.
protocol	**TCP** or **UDP**	Specifies whether the port uses the TCP or UDP protocol.
outgoing_start_port	*number*	The start port number (integer) of the outgoing traffic range. Valid numbers are from 1025 to 65,535.
outgoing_end_port	*number*	The end port number (integer) of the outgoing traffic range. Valid numbers are from 1025 to 65,535.
incoming_start_port	*number*	The start port number (integer) of the incoming traffic range. Valid numbers are from 1025 to 65,535.
incoming_end_port	*number*	The end port number (integer) of the incoming traffic range. Valid numbers are from 1025 to 65,535.

Related show commands: *show security porttriggering_rules setup* and *show security porttriggering_rules status*

security porttriggering_rules delete <row id>

This command deletes a port triggering rule by deleting its row.

Format	**security porttriggering_rules delete** *<row id>*
Mode	security

Related show commands: *show security porttriggering_rules setup* and *show security porttriggering_rules status*

UPnP Command

This section describes the **security upnp configure** command.

security upnp configure

This command configures Universal Plug and Play (UPnP). After you issue the **security upnp configure** command, you enter the security-config [upnp] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**security upnp configure**
	Mode	security
Step 2	**Format**	**enable** {**Y** | **N**} **advertisement period** *<seconds>* **advertisement time_to_live** *<number>*
	Mode	security-config [upnp]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
enable	**Y** or **N**	Enables or disables UPnP.
advertisement period	*seconds*	The advertisement period in seconds, from 1 to 1440 seconds.
advertisement time_to_live	*number*	The advertisement time-to-live period in hops, from 1 to 255 hops.

Command example:

```
FVS336Gv2> security upnp configure
security-config[upnp]> enable Y
security-config[upnp]> advertisement period 60
security-config[upnp]> advertisement time_to_live 6
security-config[upnp]> save
```

Related show commands: *show security upnp setup* and *show security upnp portmap*

Bandwidth Profile Commands

This section describes the following commands:

- *security bandwidth enable_bandwidth_profiles {Y | N}*
- *security bandwidth profile add*
- *security bandwidth profile edit <row id>*
- *security bandwidth profile delete <row id>*

security bandwidth enable_bandwidth_profiles {Y | N}

This command enables or disables bandwidth profiles globally. Select **Y** to enable bandwidth profiles globally or **N** to disable bandwidth profiles globally.

Format	**security bandwidth enable_bandwidth_profiles** {**Y** | **N**}
Mode	security

Related show command: *show security bandwidth profile setup*

---

security bandwidth profile add

This command configures a new bandwidth profile. After you issue the **security bandwidth profile add** command, you enter the security-config [bandwidth-profile] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**security bandwidth profile add**
	Mode	security
Step 2	**Format**	**name** <*profile name*> **direction** {**Inbound** | **Outbound** | **Both _Directions**} **inbound_minimum_rate** <*kbps*> **inbound_maximum_rate** <*kbps*> **outbound_minimum_rate** <*kbps*> **outbound_maximum_rate** <*kbps*> **is_group** {**Individual** {**max_instances** <*number*>}| **Group**}
	Mode	security-config [bandwidth-profile]

Keyword	Associated Keyword to Select or Parameter to Type	Description
name	*profile name*	The profile name (alphanumeric string).
direction	**Inbound, Outbound**, or **Both_Directions**	Specifies the direction to which the bandwidth profile applies.

Keyword	Associated Keyword to Select or Parameter to Type	Description
inbound_minimum_rate	*kbps*	The minimum inbound bandwidth in kbps (0 to 100,000) provided to the group or individual user.
inbound_maximum_rate	*kbps*	The maximum inbound bandwidth in kbps (100 to 100,000) provided to the group or individual user.
outbound_minimum_rate	*kbps*	The minimum outbound bandwidth in kbps (0 to 100,000) provided to the group or individual user.
outbound_maximum_rate	*kbps*	The maximum outbound bandwidth in kbps (100 to 100,000) provided to the group or individual user.
is_group	**Individual** or **Group**	Specifies the type for the bandwidth profile: • **Individual**. The profile applies to an individual user. Issue the **max_instances** keyword to specify the maximum number of users. • **Group**. The profile applies to a group.
max_instances	*number*	If the **is_group** keyword is set to **Individual,** specify the maximum number of class instances that can be created by the individual bandwidth profile.

Command example:

```
FVS336Gv2> security bandwidth profile add
security-config[bandwidth-profile]> name BusinessLevelI
security-config[bandwidth-profile]> direction Both _Directions
security-config[bandwidth-profile]> inbound_minimum_rate 7500
security-config[bandwidth-profile]> inbound_maximum_rate 25000
security-config[bandwidth-profile]> outbound_minimum_rate 5000
security-config[bandwidth-profile]> outbound_maximum_rate 10000
security-config[bandwidth-profile]> is_group Individual
security-config[bandwidth-profile]> max_instances 4
security-config[bandwidth-profile]> save
```

Related show command: *show security bandwidth profile setup*

security bandwidth profile edit <row id>

This command configures an existing bandwidth profile. After you issue the **security bandwidth profile edit** command to specify the row to be edited, you enter the security-config [bandwidth-profile] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. You cannot change the name of the profile.

Step 1	**Format**	**security bandwidth profile edit** *<row id>*
	Mode	security

Step 2	**Format**	**direction** {**Inbound** | **Outbound** | **Both _Directions**} **inbound_minimum_rate** <*kbps*> **inbound_maximum_rate** <*kbps*> **outbound_minimum_rate** <*kbps*> **outbound_maximum_rate** <*kbps*> **is_group** {**Individual** {**max_instances** <*number*>}| **Group**}
	Mode	security-config [bandwidth-profile]

Keyword	Associated Keyword to Select or Parameter to Type	Description
direction	**Inbound, Outbound**, or **Both_Directions**	Specifies the direction to which the bandwidth profile applies.
inbound_minimum_rate	*kbps*	The minimum inbound bandwidth in kbps (0 to 100,000) provided to the group or individual user.
inbound_maximum_rate	*kbps*	The maximum inbound bandwidth in kbps (100 to 100,000) provided to the group or individual user.
outbound_minimum_rate	*kbps*	The minimum outbound bandwidth in kbps (0 to 100,000) provided to the group or individual user.
outbound_maximum_rate	*kbps*	The maximum outbound bandwidth in kbps (100 to 100,000) provided to the group or individual user.
is_group	**Individual** or **Group**	Specifies the type for the bandwidth profile: • **Individual**. The profile applies to an individual user. Issue the **max_instances** keyword to specify the maximum number of users. • **Group**. The profile applies to a group.
max_instances	*number*	If the **is_group** keyword is set to **Individual,** specify the maximum number of class instances that can be created by the individual bandwidth profile.

Related show command: *show security bandwidth profile setup*

security bandwidth profile delete <row id>

This command deletes a bandwidth profile by deleting its row ID.

Format	**net bandwidth profile delete** <*row id*>
Mode	security

Related show command: *show security bandwidth profile setup*

Content Filtering Commands

This section describes the following commands:

- *security content_filter content_filtering configure*
- *security content_filter block_group enable*
- *security content_filter block_group disable*
- *security content_filter blocked_keywords add*
- *security content_filter blocked_keywords edit <row id>*
- *security content_filter blocked_keywords delete <row id>*
- *security content_filter trusted_domain add*
- *security content_filter trusted_domain edit <row id>*
- *security content_filter trusted_domain delete <row id>*

security content_filter content_filtering configure

This command globally enables or disables content filtering and configures web components. After you issue the **`security content_filter content_filtering configure`** command, you enter the security-config [content-filtering] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**`security content_filter content_filtering configure`**
	Mode	security
Step 2	**Format**	**`content_filtering {Y | N}`** **`activex_enable {Y | N}`** **`cookies_enable {Y | N}`** **`java_enable {Y | N}`** **`proxy_enable {Y | N}`**
	Mode	security-config [content-filtering]

Keyword	Associated Keyword to Select	Description
`content_filtering`	**`Y`** or **`N`**	Enables or disables content filtering globally.
`activex_enable`	**`Y`** or **`N`**	Enables or disables ActiveX.
`cookies_enable`	**`Y`** or **`N`**	Enables or disables cookies.
`java_enable`	**`Y`** or **`N`**	Enables or disables Java.
`proxy_enable`	**`Y`** or **`N`**	Enables or disables the proxy server.

Command example:

```
FVS336Gv2> security content_filter content_filtering configure
security-config[content-filtering]> content_filtering Y
security-config[content-filtering]> activex_enable Y
security-config[content-filtering]> cookies_enable Y
security-config[content-filtering]> java_enable Y
security-config[content-filtering]> proxy_enable N
security-config[content-filtering]> save
```

Related show command: *show security content_filter content_filtering*

security content_filter block_group enable

This command applies content filtering to selected groups or to all groups. After you issue the **security content_filter block_group enable** command, you enter the security-config [block-group-enable] mode and then you can select a group, several groups, or all groups.

Step 1	**Format**	**security content_filter block_group enable**
	Mode	security
Step 2	**Format**	**group all** {**Y**} **group group1** {**Y**} **group group2** {**Y**} **group group3** {**Y**} **group group4** {**Y**} **group group5** {**Y**} **group group6** {**Y**} **group group7** {**Y**} **group group8** {**Y**}
	Mode	security-config [block-group-enable]

Keyword (might consist of two separate words)	Associated Keyword to Select	Description
group all	**Y**	Enables content filtering for all groups.

Keyword (might consist of two separate words)	Associated Keyword to Select	Description
group group1	**Y**	Enables content filtering for the selected group.
group group2	**Y**	
group group3	**Y**	
group group4	**Y**	
group group5	**Y**	
group group6	**Y**	
group group7	**Y**	
group group8	**Y**	

Command example:

```
FVS336Gv2> security content_filter blocked_group enable
security-config[block-group-enable]> group group1 Y
security-config[block-group-enable]> group group2 Y
security-config[block-group-enable]> group group3 Y
security-config[block-group-enable]> group group8 Y
security-config[block-group-enable]> save
```

Related show command: *show security content_filter block_group*

security content_filter block_group disable

This command removes content filtering from selected groups or from all groups. After you issue the **security content_filter block_group disable** command, you enter the security-config [block-group-disable] mode and then you can select a group, several groups, or all groups.

Step 1	**Format**	**security content_filter block_group disable**
	Mode	security
Step 2	**Format**	**group all** {**Y**} **group group1** {**Y**} **group group2** {**Y**} **group group3** {**Y**} **group group4** {**Y**} **group group5** {**Y**} **group group6** {**Y**} **group group7** {**Y**} **group group8** {**Y**}
	Mode	security-config [block-group-disable]

Keyword (might consist of two separate words)	Associated Keyword to Select	Description
group all	**Y**	Disables content filtering for all groups.
group group1	**Y**	Disables content filtering for the selected group.
group group2	**Y**	
group group3	**Y**	
group group4	**Y**	
group group5	**Y**	
group group6	**Y**	
group group7	**Y**	
group group8	**Y**	

Command example:

```
FVS336Gv2> security content_filter blocked_group disable
security-config[block-group-disable]> group group3 Y
security-config[block-group-disable]> group group8 Y
security-config[block-group-disable]> save
```

Related show command: *show security content_filter block_group*

security content_filter blocked_keywords add

This command configures a new blocked keyword for content filtering. After you issue the **security content_filter blocked_keywords add** command, you enter the security-config [blocked-keywords] mode and then you can configure one keyword a time.

Step 1	**Format**	**security content_filter blocked_keywords add**
	Mode	security
Step 2	**Format**	**blocked_keyword** *<keyword>*
	Mode	security-config [blocked-keywords]

Keyword	Associated Parameter to Type	Description
blocked_keyword	*keyword*	The keyword (string) to be blocked.

Command example:

```
FVS336Gv2> security content_filter blocked_keywords add
security-config[blocked-keywords]> blocked_keyword casino
security-config[blocked-keywords]> save
security-config[blocked-keywords]> blocked_keyword gambl*
security-config[blocked-keywords]> save
```

Related show command: *show security content_filter blocked_keywords*

security content_filter blocked_keywords edit <row id>

This command configures an existing blocked keyword for content filtering. After you issue the **security content_filter blocked_keywords edit** command to specify the row to be edited, you enter the security-config [blocked-keywords] mode and then you can edit the keyword.

Step 1	**Format**	**security content_filter blocked_keywords edit**
	Mode	security
Step 2	**Format**	**blocked_keyword** *<keyword>*
	Mode	security-config [blocked-keywords]

Keyword	Associated Parameter to Type	Description
blocked_keyword	*keyword*	The keyword (string) to be blocked.

Related show command: *show security content_filter blocked_keywords*

security content_filter blocked_keywords delete <row id>

This command deletes a blocked keyword by deleting its row ID.

Format	**security content_filter blocked_keywords delete** *<row id>*
Mode	security

Related show command: *show security content_filter blocked_keywords*

security content_filter trusted_domain add

This command configures a new trusted domain for content filtering. After you issue the **security content_filter trusted_domain add** command, you enter the security-config [approved-urls] mode and then you can add a URL or domain name.

Step 1	**Format**	**security content_filter trusted_domain add**
	Mode	security
Step 2	**Format**	**url** *<url>*
	Mode	security-config [approved-urls]

Keyword	Associated Parameter to Type	Description
url	*url*	The URL or domain name to be blocked.

Command example:

```
FVS336Gv2> security content_filter trusted_domain add
security-config[approved-urls]> url netgear
security-config[approved-urls]> save
security-config[approved-urls]> url google.com
security-config[approved-urls]> save
security-config[approved-urls]> url www.irs.gov
security-config[approved-urls]> save
```

Related show command: *show security content_filter trusted_domains*

security content_filter trusted_domain edit <row id>

This command configures an existing trusted domain for content filtering. After you issue the **security content_filter trusted_domain edit** command to specify the row to be edited, you enter the security-config [approved-urls] mode and then you can edit the URL or domain name.

Step 1	**Format**	**security content_filter trusted_domain edit** *<row id>*
	Mode	security
Step 2	**Format**	**url** *<url>*
	Mode	security-config [approved-urls]

Keyword	Associated Parameter to Type	Description
url	*url*	The URL or domain name to be blocked.

Related show command: *show security content_filter trusted_domains*

security content_filter trusted_domain delete <row id>

This command deletes a trusted domain by deleting its row ID.

Format	**security content_filter trusted_domain delete** *<row id>*
Mode	security

Related show command: *show security content_filter trusted_domains*

System Mode Configuration Commands

5

This chapter explains the configuration commands, keywords, and associated parameters in the system mode. The chapter includes the following sections:

- *Remote Management Commands*
- *SNMP Commands*
- *Time Zone Command*
- *WAN Traffic Meter Command*
- *Firewall Logs and Email Alerts Commands*
- *System Reboot Command*

IMPORTANT:

After you issue a command that includes the word `configure`, `add`, or `edit`, you must save (or cancel) your changes. For more information, see *Configuration Commands: Save Commands* on page 13.

Remote Management Commands

This section describes the following commands:

- *system remote_management https configure*
- *system remote_management telnet configure*

system remote_management https configure

This command configures remote management over HTTPS. After you issue the **system remote_management https configure** command, you enter the system-config [https] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Note: You can configure remote management over HTTPS for both IPv4 and IPv6 connections because these connections are not mutually exclusive.

Step 1

Format `system remote_management https configure`

Mode system

Step 2

Format

```
ip_version {IPv4 | IPv6}

enable_ipv4 {Y | N}
access_type {Everyone | IP_Range {from_address <ipaddress>}
   {end_address <ipaddress>} | To_this_PC_only {only_this_pc_ip
   <ipaddress>}}
port <number>

enable_ipv6 {Y | N}
access_type6 {Everyone | IP_Range {from_address6
   <ipv6-address>} {end_address6 <ipv6-address>} |
   To_this_PC_only {only_this_pc_ipv6 <ipv6-address>}}
port <number>
```

Mode system-config [https]

Keyword	Associated Keyword to Select or Parameter to Type	Description
`ip_version`	**IPv4** or **IPv6**	Specifies the configuration of IPv4 or IPv6.
HTTPS over an IPv4 connection		
`enable_ipv4`	**Y** or **N**	Allows or blocks remote management over HTTPS for an IPv4 connection.

Keyword	Associated Keyword to Select or Parameter to Type	Description
access_type	**Everyone**, **IP_Range**, or **To_this_PC_only**	Specifies the type of access: • **Everyone**. Enables access to all IP addresses. You do not need to configure any IP address. • **IP_Range**. Enables access to a range of IP addresses. You also must configure the **from_address** and **end_address** keywords and associated parameters. • **To_this_PC_only**. Enables access to a single IP address. You also must configure the **only_this_pc_ip** keyword and associated parameter.
from_address	*ipaddress*	The start IP address if you set the **access_type** keyword to **IP_Range**.
end_address	*ipaddress*	The end IP address if you set the **access_type** keyword to **IP_Range**.
only_this_pc_ip	*ipaddress*	The single IP address if you set the **access_type** keyword to **To_this_PC_only**.
port	*number*	The number of the port through which access is allowed.
HTTPS over an IPv6 connection		
enable_ipv6	**Y** or **N**	Allows or blocks remote management over HTTPS for an IPv6 connection.
access_type6	**Everyone**, **IP_Range**, or **To_this_PC_only**	Specifies the type of access: • **Everyone**. Enables access to all IP addresses. You do not need to configure any IP address. • **IP_Range**. Enables access to a range of IP addresses. You also must configure the **from_address6** and **end_address6** keywords and associated parameters. • **To_this_PC_only**. Enables access to a single IP address. You also must configure the **only_this_pc_ipv6** keyword and associated parameter.
from_address6	*ipv6-address*	The start IP address if you set the **access_type6** keyword to **IP_Range**.
end_address6	*ipv6-address*	The end IP address if you set the **access_type6** keyword to **IP_Range**.
only_this_pc_ipv6	*ipaddress*	The single IP address if you set the **access_type6** keyword to **To_this_PC_only**.
port	*number*	The number of the port through which access is allowed.

Command example:

```
FVS336Gv2> system remote_management https configure
system-config[https]> ip_version IPv4
system-config[https]> enable_ipv4 Y
system-config[https]> access_type Everyone
system-config[https]> port 445
system-config[https]> save
```

Related show command: *show system remote_management setup*

system remote_management telnet configure

This command configures remote management over Telnet. After you issue the **system remote_management telnet configure** command, you enter the system-config [telnet] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Note: You can configure remote management over Telnet for both IPv4 and IPv6 connections because these connections are not mutually exclusive.

Step 1

Format `system remote_management telnet configure`

Mode system

Step 2

Format

```
ip_version {IPv4 | IPv6}

enable_ipv4 {Y | N}
access_type {Everyone | IP_Range {from_address <ipaddress>}
   {to_address <ipaddress>} | To_this_PC_only {only_this_pc_ip
   <ipaddress>}}

enable_ipv6 {Y | N}
access_type6 {Everyone | IP_Range {from_address6
   <ipv6-address>} {to_address6 <ipv6-address>} |
   To_this_PC_only {only_this_pc_ip6 <ipv6-address>}}
```

Mode system-config [telnet]

Keyword	Associated Keyword to Select or Parameter to Type	Description
ip_version	**IPv4** or **IPv6**	Specifies the configuration of IPv4 or IPv6.
Telnet over an IPv4 connection		
enable_ipv4	**Y** or **N**	Allows or blocks remote management over Telnet for an IPv4 connection.

Keyword	Associated Keyword to Select or Parameter to Type	Description
access_type	**Everyone**, **IP_Range**, or **To_this_PC_only**	Specifies the type of access: • **Everyone**. Enables access to all IP addresses. You do not need to configure any IP address. • **IP_Range**. Enables access to a range of IP addresses. You also must configure the **from_address** and **to_address** keywords and associated parameters. • **To_this_PC_only**. Enables access to a single IP address. You also must configure the **only_this_pc_ip** keyword and associated parameter.
from_address	*ipaddress*	The start IP address if you set the **access_type** keyword to **IP_Range**.
to_address	*ipaddress*	The end IP address if you set the **access_type** keyword to **IP_Range**.
only_this_pc_ip	*ipaddress*	The single IP address if you set the **access_type** keyword to **To_this_PC_only**.
Telnet over an IPv6 connection		
enable_ipv6	**Y** or **N**	Allows or blocks remote management over Telnet for an IPv6 connection.
access_type6	**Everyone**, **IP_Range**, or **To_this_PC_only**	Specifies the type of access: • **Everyone**. Enables access to all IP addresses. You do not need to configure any IP address. • **IP_Range**. Enables access to a range of IP addresses. You also must configure the **from_address6** and **to_address6** keywords and associated parameters. • **To_this_PC_only**. Enables access to a single IP address. You also must configure the **only_this_pc_ip6** keyword and associated parameter.
from_address6	*ipv6-address*	The start IP address if you set the **access_type6** keyword to **IP_Range**.
to_address6	*ipv6-address*	The end IP address if you set the **access_type6** keyword to **IP_Range**.
only_this_pc_ip6	*ipaddress*	The single IP address if you set the **access_type6** keyword to **To_this_PC_only**.

Command example:

```
FVS336Gv2> system remote_management telnet configure
system-config[telnet]> ip_version IPv6
system-config[telnet]> enable_ipv6 Y
system-config[telnet]> access_type6 IP_Range
system-config[telnet]> from_address6 FEC0::3001
```

```
system-config[telnet]> end_address6 FEC0::3100
system-config[telnet]> save
```

Related show command: *show system remote_management setup*

SNMP Commands

This section describes the following commands:

- *system snmp trap configure <ip address>*
- *system snmp trap delete <ipaddress>*
- *system snmp remote_snmp enable*
- *system snmp trapevent edit*
- *system snmp sys configure*
- *system snmp v3_users edit*

system snmp trap configure <ip address>

This command configures a new or existing SNMP agent to which trap information is forwarded. After you issue the **system snmp trap configure** command to specify the IP address of the agent, you enter the system-config [snmp-trap] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**system snmp trap configure** *<ipaddress>*
	Mode	system
Step 2	**Format**	**agent** *<ipaddress>* **subnet_mask** *<subnet mask>* **port** *<number>* **snmp_version** {**v1** | **v2c** | **v3**} **community** *<community name>*
	Mode	system-config [snmp-trap]

Keyword	Associated Keyword to Select or Parameter to Type	Description
agent	*ipaddress*	This keyword and parameter allow you to change the existing agent IP address that you issued to enter the system-config [snmp-trap] mode.
subnet_mask	*subnet mask*	The subnet mask used to determine the list of allowed SNMP agents that are part of the subnet. To allow any IP address on the network to manage the device, specify **255.255.255.0**. For a specific host, specify **255.255.255.255**. To allow global access, specify **0.0.0.0**.

Keyword	Associated Keyword to Select or Parameter to Type	Description
port	*number*	The SNMP port (integer) to which the trap messages are forwarded. Valid numbers are from 0 to 65,535.
snmp_version	**v1**, **v2c**, or **v3**	The SNMP version. For information about configuring SNMPv3 users, see *system snmp v3_users edit*.
community	*community name*	The string that represents the community to which the agent belongs. Most agents are configured to listen for traps in the public community.

Command example:

```
FVS336Gv2> system snmp trap configure 10.118.33.245
system-config[snmp-trap]> subnet_mask 255.255.255.0
system-config[snmp-trap]> port 162
system-config[snmp-trap]> community public
system-config[snmp-trap]> snmp_version v2c
system-config[snmp-trap]> save
```

Related show command: *show system snmp trap [agent ipaddress]*

---

system snmp trap delete <ipaddress>

This command deletes an SNMP agent by deleting its IP address.

Format	**system snmp trap delete** *<ipaddress>*
Mode	system

Related show command: *show system snmp trap [agent ipaddress]*

---

system snmp remote_snmp enable

This command allows or blocks SNMP access from the WAN.

Format	**system snmp remote_snmp enable** {**Y** | **N**}
Mode	security

Related show command: *show system snmp remote_snmp status*

---

system snmp trapevent edit

This command changes the default SNMP trap events. After you issue the **system snmp trapevent edit** command, you enter the system-config [snmp-trapevents] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**system snmp trapevent edit**
	Mode	system
Step 2	**Format**	**Wan_Configuration_Failure** {**Y** | **N**} **Firewall_Event** {**Y** | **N**} **ipsecVPN_Event** {**Y** | **N**} **SSlVPN_Event** {**Y** | **N**} **Login_Events** {**Y** | **N**} **LoginFailure_Events** {**Y** | **N**} **WAN_Failover_Events** {**Y** | **N**} **Config_Change_Events** {**Y** | **N**}
	Mode	system-config [snmp-trapevents]

Keyword	Associated Keyword to Select	Description
Wan_Configuration_Failure	**Y** or **N**	Allows or blocks the generation of a trap when a WAN connection fails.
Firewall_Event	**Y** or **N**	Allows or blocks the generation of a trap when a new connection is initiated through addition of a custom firewall rule.
ipsecVPN_Event	**Y** or **N**	Allows or blocks the generation of a trap when an IPSec VPN tunnel is established or disconnected.
SSlVPN_Event	**Y** or **N**	Allows or blocks the generation of a trap when an SSL VPN tunnel is established or disconnected.
Login_Events	**Y** or **N**	Allows or blocks the generation of a trap when a user logs in to the VPN firewall.
LoginFailure_Events	**Y** or **N**	Allows or blocks the generation of a trap when a user attempts to log in to the VPN firewall but fails to do so.
WAN_Failover_Events	**Y** or **N**	Allows or blocks the generation of a trap when an auto-rollover occurs from one WAN interface to another.
Config_Change_Events	**Y** or **N**	Allows or blocks the generation of a trap when the configuration of the VPN firewall changes.

Command example:

```
FVS336Gv2> system snmp trapevent edit
system-config[snmp-trapevents]> Login_Events N
system-config[snmp-trapevents]> WAN_Failover_Events Y
```

```
system-config[snmp-trapevents]> Config_Change_Events Y
system-config[snmp-trapevents]> save
```

Related show command: *show system snmp trap_events*

system snmp sys configure

This command configures the SNMP system information. After you issue the **system snmp sys configure** command, you enter the system-config [snmp-system] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**system snmp sys configure**
	Mode	system
Step 2	**Format**	**sys_contact** *<contact name>* **sys_location** *<location name>* **sys_name** *<system name>*
	Mode	system-config [snmp-system]

Keyword	Associated Parameter to Type	Description
sys_contact	*contact name*	The system contact name (alphanumeric string).
sys_location	*location name*	The system location name (alphanumeric string).
sys_name	*system name*	The system name (alphanumeric string).

Command example:

```
FVS336Gv2> system snmp sys configure
system-config[snmp-system]> sys_contact AdminFVS@netgear.com
system-config[snmp-system]> sys_location San Jose
system-config[snmp-system]> sys_name FVS336Gv2-Bld3
system-config[snmp-system]> save
```

Related show command: *show system snmp sys*

system snmp v3_users edit

This command configures the default SNMPv3 users. After you issue the **system snmp v3_users edit** command to select either the admin or guest default SNMPv3 user, you enter the system-config [snmpv3-users] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Note: Use the *system snmp trap configure <ip address>* command to configure an SNMPv3 agent.

Step 1	**Format**	**system snmp v3_users edit** [**admin** | **guest**]
	Mode	system
Step 2	**Format**	**security_level** [**NoAuthNoPriv** | **AuthNoPriv** | **AuthPriv**] **auth_algo** [**MD5** | **SHA1**] **auth_pass** <*password*> **priv_algo** [**DES** | **AES**] **priv_pass** <*password*>
	Mode	system-config [snmpv3-users]

Keyword	Associated Parameter to Type	Description
security_level	**NoAuthNoPriv**, **AuthNoPriv**, or **AuthPriv**	Specifies the level of SNMPv3 security: • **NoAuthNoPriv**. No authorization and no privacy (encryption) settings. This is the default setting. • **AuthNoPriv**. Authorization settings but not privacy (encryption) settings. You must issue the **auth_algo** keyword to specify the type of authorization and the **auth_pass** keyword to specify the authorization password. • **AuthPriv**. Authorization settings and privacy (encryption) settings. You must issue the following keywords: - **auth_algo** keyword to specify the type of authorization and the **auth_pass** keyword to specify the authorization password. - **priv_alg** keyword to specify the type of encryption and the **priv_pass** keyword to specify the encryption password.
auth_algo	**MD5** or **SHA1**	If the **security_level** keyword is set to **AuthNoPriv**, or **AuthPriv**, the type of authorization.
auth_pass	*password*	If the **security_level** keyword is set to **AuthNoPriv**, or **AuthPriv**, the authorization password (alphanumeric string).
priv_alg	**DES** or **AES**	If the **security_level** keyword is set to **AuthPriv**, the type of privacy (encryption).
priv_pass	*password*	If the **security_level** keyword is set to **AuthPriv**, the privacy (encryption) password (alphanumeric string).

ommand example:

```
FVS336Gv2> system snmp v3_users edit admin
system-config[snmpv3-users]> security_level AuthNoPriv
system-config[snmpv3-users]> auth_algo MD5
system-config[snmpv3-users]> auth_pass xt5ROOT37ggZ
system-config[snmpv3-users]> save
```

Related show command: *show system snmp snmpv3_users*

Time Zone Command

This section describes the **system time configure** command.

system time configure

This command configures the system time, date, and NTP servers. After you issue the **system time configure** command, you enter the system-config [time] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1 **Format** **system time configure**

Mode system

Step 2 **Format** **timezone** <*timezone*>
auto_daylight {**Y** | **N**}
resolve_ipv6_address {**Y** | **N**}
ntp_mode {**Authoritative_Mode** {**stratum** <*number*>} |
Sync_to_NTP_Servers_on_Internet | **Sync_to_NTP_Servers_on_VPN**}
{**vpn_policy** <*vpn policy name*>}}
set_date_time_manually {**N** | **Y** {**ntp_hour** <*hour*> | **ntp_minutes** <*minutes*> | **ntp_seconds** <*seconds*> | **ntp_day** <*day*> | **ntp_month** <*month*> | **ntp_year** <*year*>}}
ntp_server_type {**DEFAULT** | **CUSTOM** {**ntp_server1** {<*ipaddress*> | <*domain name*>}} {**ntp_server2** {<*ipaddress*> | <*domain name*>}}}

Mode system-config [time]

Keyword	Associated Keyword to Select or Parameter to Type	Description
timezone	*timezone*	For a list of time zones that you can enter, see *Table 11*.
auto_daylight	**Y** or **N**	Allows or blocks automatic adjustment for daylight saving time.
resolve_ipv6_address	**Y** or **N**	Specifies whether or not the VPN firewall automatically resolves a domain name for an NTP server to an IPv6 address: • **Y**. A domain name is resolved to an IPv6 address. • **N**. A domain name is resolved to an IPv4 address.

Keyword	Associated Keyword to Select or Parameter to Type	Description
ntp_mode	**Authoritative_Mode**, **Sync_to_NTP_Servers_on_Internet**, or **Sync_to_NTP_Servers_on_VPN**	Specifies the NTP mode: • **Authoritative_Mode**. The VPN firewall synchronizes its clock with the specified NTP server or servers on the Internet. If external servers are unreachable, the VPN firewall's real-time clock (RTC) provides time service to clients. Issue the **stratum** keyword to specify the stratum value. As an option, issue the **set_date_time_manually** value keyword to enable manual configuration of the date and time. • **Sync_to_NTP_Servers_on_Internet**. The VPN firewall synchronizes its clock with the specified NTP server or servers on the Internet. If external servers are unreachable, the VPN firewall does *not* use its RTC. • **Sync_to_NTP_Servers_on_VPN**. The VPN firewall synchronizes its clock with the specified NTP server on the VPN. If the server is unreachable, the VPN firewall does *not* use its RTC. Issue the **vpn_policy** keyword to specify a VPN policy that enables the VPN firewall to contact the NTP server on the VPN.
stratum	*number*	If the **ntp_mode** keyword is set to **Authoritative_Mode**, the stratum value. This value indicates the distance between the RTC of the VPN firewall and a reference clock.
set_date_time_manually	**Y** or **N**	Allows or blocks manual configuration of the date and time. If you enable manual configuration, issue the **ntp_hour**, **ntp_minutes**, **ntp_seconds**, **ntp_day**, **ntp_month**, and **ntp_year** keywords to specify the date and time manually.
ntp_hour	*hour*	The hour in the format HH (00 to 24) for manual configuration.
ntp_minutes	*minutes*	The minutes in the format MM (00 to 59) for manual configuration.
ntp_seconds	*seconds*	The seconds in the format SS (00 to 59) for manual configuration.
ntp_day	*day*	The day in the format DD (00 to 31) for manual configuration.
ntp_month	*month*	The month in the format MM (01 to 12) for manual configuration.

Keyword	Associated Keyword to Select or Parameter to Type	Description
ntp_year	*year*	The year in the format YYYY for manual configuration.
vpn_policy	*vpn policy name*	If the **ntp_mode** keyword is set to **Sync_to_NTP_Servers_on_VPN**, the name of the VPN policy that enables the VPN firewall to contact the NTP server on the VPN.
ntp_server_type	**CUSTOM** or **DEFAULT**	Specifies the use of custom or default NTP servers: • **CUSTOM**. The VPN firewall uses custom NTP servers. Issue the **ntp_server1** and **ntp_server2** keywords to specify the server IP addresses or domain names. • **DEFAULT**. The VPN firewall uses the default NTP servers.
ntp_server1	*ipaddress* or *domain name*	The IP address of domain name of the first custom NTP server.
ntp_server2	*ipaddress* or *domain name*	The IP address of domain name of the second custom NTP server.

Table 11. Time zone keywords

GMT time and location **Note:** Enter the keywords exactly as stated (you can use autocompletion keys). If a time zone has more than one location, enter the location exactly as stated. For example, either enter **GMT-11:00::Samoa** or enter **GMT-10:00::Hawaii**.
GMT::Greenwich-Mean-Time:Edinburgh,London
GMT-12:00::Eniwetok
GMT-12:00::Kwajalein
GMT-11:00::Midway_Island
GMT-11:00::Samoa
GMT-10:00::Hawaii
GMT-09:30::Marquesas_Is
GMT-09:00::Alaska
GMT-08:30::Pitcairn_Is
GMT-08:00::Pacific_Time-Canada
GMT-08:00::Pacific_Time-US

Table 11. Time zone keywords (continued)

GMT time and location **Note:** Enter the keywords exactly as stated (you can use autocompletion keys). If a time zone has more than one location, enter the location exactly as stated. For example, either enter **GMT-11:00::Samoa** or enter **GMT-10:00::Hawaii**.
GMT-08:00::Tijuana
GMT-07:00::Mountain_Time-Canada
GMT-07:00::Mountain_Time-US
GMT-06:00::Central_Time-Canada
GMT-06:00::Central_Time-US
GMT-05:00::Eastern_Time-Canada
GMT-05:00::Eastern_Time-Lima
GMT-05:00::Eastern_Time-US
GMT-04:30::Caracas
GMT-04:00::Atlantic_Time-Canada
GMT-03:30::Newfoundland
GMT-03:00::Brasilia,Buenos_Aires
GMT-02:00::Mid-Atlantic
GMT-01:00::Azores
GMT-01:00::Cape_Verde_Is
GMT+01:00::Europe
GMT+02:00::Athens
GMT+02:00::Istanbul
GMT+02:00::Minsk
GMT+02:00::Cairo
GMT+03:00::Baghdad
GMT+03:00::Kuwait
GMT+03:00::Moscow
GMT+03:30::Tehran
GMT+04:00::Abu-Dhabi
GMT+04:00::Muscat
GMT+04:00::Baku

Table 11. Time zone keywords (continued)

GMT time and location **Note:** Enter the keywords exactly as stated (you can use autocompletion keys). If a time zone has more than one location, enter the location exactly as stated. For example, either enter **GMT-11:00::Samoa** or enter **GMT-10:00::Hawaii**.
GMT+04:30::Kabul
GMT+05:00::Ekaterinburg
GMT+05:00::Islamabad
GMT+05:00::Karachi
GMT+05:30::Bombay,Calcutta,Madras,Delhi
GMT+05:30::Colombo
GMT+06:00::Almaty
GMT+06:00::Dhaka
GMT+06:30::Burma
GMT+07:00::Bangkok
GMT+07:00::Hanoi
GMT+07:00::Jakarta
GMT+08:00::Beijing,Chongqing,Hong_Kong
GMT+08:00::AWST-Perth
GMT+09:00::Osaka,Sapporo,Tokyo
GMT+09:00::Seoul
GMT+09:30::ACST-Adelaide
GMT+09:30::ACST-Darwin
GMT+09:30::ACST--Broken_Hill,NSW
GMT+10:00::AEST-Brisbane
GMT+10:00::Guam
GMT+10:00::Port_Moresby
GMT+10:00::AEST-Canberra
GMT+10:00::AEST-Melbourne
GMT+10:00::AEST-Sydney
GMT+10:00::AEST-Hobart
GMT+10:30::Lord_Howe_Is

Table 11. Time zone keywords (continued)

GMT time and location **Note:** Enter the keywords exactly as stated (you can use autocompletion keys). If a time zone has more than one location, enter the location exactly as stated. For example, either enter **GMT-11:00::Samoa** or enter **GMT-10:00::Hawaii**.
GMT+11:00::Magadan
GMT+11:00::Solomon_Is
GMT+11:00::New_Caledonia
GMT+11:30::Norfolk_I
GMT+12:00::Auckland
GMT+12:00::Wellington
GMT+12:00::New_Zealand
GMT+12:00::Fiji
GMT+13:00::Tonga
GMT+14:00::Kiribati

Command example:

```
FVS336Gv2> system time configure
system-config[time]> timezone GMT-08:00::Pacific_Time-US
system-config[time]> auto_daylight Y
system-config[time]> resolve_ipv6_address N
system-config[time]> ntp_mode Sync_to_NTP_Servers_on_Internet
system-config[time]> ntp_server_type DEFAULT
system-config[time]> save
```

Related show command: *show system time setup*

WAN Traffic Meter Command

This section describes the **system traffic_meter configure** command.

system traffic_meter configure <wan interface>

This command configures the traffic meter. After you issue the **system traffic_meter configure** command to specify one of the two WAN interfaces (that is, WAN1 or WAN2), you enter the system-config [traffic-meter] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**system traffic_meter configure** {**WAN1** | **WAN2**}
	Mode	system

Step 2 **Format**

```
enable {Y | N}
limit_type {Nolimit | Downloadonly | Directions}
monthly_limit <number>
increase_limit_enable {N | Y {increase_limit_by <number>}}

counter {RestartCounter | SpecificTime {day_of_month <day>}
   {time_hour <hour>} {time_meridiem {AM | PM}} {time_minute
<minute>}}
send_email_report {Y | N}

block_type {Block-all-traffic | Block-all-traffic-except-email}
send_email_alert {Y | N}
```

Mode system-config [traffic-meter]

Keyword	Associated Keyword to Select or Parameter to Type	Description
Traffic meter configuration		
enable	**Y** or **N**	Enables or disables the traffic meter.
limit_type	**Nolimit**, **Downloadonly**, or **Directions**	Specifies the type of traffic limit, if any: • **Nolimit**. Traffic is not limited. • **Downloadonly**. The traffic limit applies to downloaded traffic only. • **Directions**. The traffic limit applies to both downloaded and uploaded traffic.
monthly_limit	*number*	The monthly limit for the traffic meter in MB.
increase_limit_enable	**Y** or **N**	Allows or blocks automatic increase of the limit after the meter exceeds the configured limit. If you allow an automatic increase, issue the **increase_limit_by** keyword to specify the number of MB.
increase_limit_by	*number*	The number in MB to increase the configured limit of the traffic meter.

Keyword	Associated Keyword to Select or Parameter to Type	Description
Traffic counter configuration		
counter	**SpecificTime** or **RestartCounter**	Specifies how the traffic counter is restarted: • **SpecificTime**. Restarts the traffic counter on a specific day and time. You must set the **day_of_month**, **time_hour**, **time_meridiem**, and **time_minute** keywords and associated parameters. • **RestartCounter**. Restarts the traffic counter after you save the command.
day_of_month	*day*	The day in the format DD (01 to 31) that the traffic counter restarts. This keyword applies only if you set the **counter** keyword to **SpecificTime**.
time_hour	*hour*	The hour in the format HH (00 to 12) that the traffic counter restarts. This keyword applies only if you set the **counter** keyword to **SpecificTime**.
time_meridiem	**AM** or **PM**	Specifies the meridiem for the hour that the traffic counter restarts. This keyword applies only if you set the **counter** keyword to **SpecificTime**.
time_minute	*minutes*	The minutes in the format MM (00 to 59) that the traffic counter restarts. This keyword applies only if you set the **counter** keyword to **SpecificTime**.
send_email_report	**Y** or **N**	Specifies whether or not an email report is sent when the traffic counter restarts.
Action when limit is reached		
block_type	**Block-all-traffic**, or **Block-all-traffic-except-email**	Specifies the type of traffic blocking after the meter exceeds the configured limit.
send_email_alert	**Y** or **N**	Specifies whether or not an email alert is sent when the traffic limit is reached.

Command example:

```
FVS336Gv2> system traffic_meter configure WAN1
system-config[traffic-meter]> enable Y
system-config[traffic-meter]> limit_type Downloadonly
system-config[traffic-meter]> monthly_limit 150000
system-config[traffic-meter]> increase_limit_enable Y
system-config[traffic-meter]> increase_limit_by 50000
system-config[traffic-meter]> counter SpecificTime
system-config[traffic-meter]> day_of_month 01
system-config[traffic-meter]> time_hour 00
system-config[traffic-meter]> time_meridiem AM
system-config[traffic-meter]> time_minute 00
system-config[traffic-meter]> send_email_report Y
system-config[traffic-meter]> block_type Block-all-traffic-except-email
system-config[traffic-meter]> send_email_alert Y
system-config[traffic-meter]> save
```

Related show command: *show system traffic_meter setup <wan interface>*

Firewall Logs and Email Alerts Commands

This section describes the following commands:

- *system logging configure*
- *system logging remote configure*

system logging configure

This command configures routing logs for accepted and dropped IPv4 and IPv6 packets, selected system logs, and logs for other events. After you issue the **system logging configure** command, you enter the system-config [logging-ipv4-ipv6] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**system logging configure**
	Mode	system

Step 2 **Format**

```
lan_wan_accept_packet_logs {Y | N}
lan_wan_drop_packet_logs {Y | N}
lan_dmz_accept_packet_logs {Y | N}
lan_dmz_drop_packet_logs {Y | N}
dmz_wan_accept_packet_logs {Y | N}
dmz_wan_drop_packet_logs {Y | N}
wan_lan_accept_packet_logs {Y | N}
wan_lan_drop_packet_logs {Y | N}
dmz_lan_accept_packet_logs {Y | N}
dmz_lan_drop_packet_logs {Y | N}
wan_dmz_accept_packet_logs {Y | N}
wan_dmz_drop_packet_logs {Y | N}

change_of_time_by_NTP_logs {Y | N}
login_attempts_logs {Y | N}
secure_login_attempts_logs {Y | N}
reboot_logs {Y | N}
unicast_traffic_logs {Y | N}
broadcast_or_multicast_traffic_logs {Y | N}
wan_status_logs {Y | N}
resolved_DNS_names_logs {Y | N}
vpn_logs {Y | N}
dhcp_server_logs {Y | N}

source_mac_filter_logs {Y | N}
session_limit_logs {Y | N}
bandwidth_limit_logs {Y | N}
```

Mode system-config [logging-ipv4-ipv6]

Keyword	Associated Keyword to Select	Description
Routing logs		
lan_wan_accept_packet_logs	**Y** or **N**	Enables or disables packet logging for the traffic direction and type of packet (accepted or dropped) that is defined in the keyword.
lan_wan_drop_packet_logs	**Y** or **N**	
lan_dmz_accept_packet_logs	**Y** or **N**	
lan_dmz_drop_packet_logs	**Y** or **N**	
dmz_wan_accept_packet_logs	**Y** or **N**	
dmz_wan_drop_packet_logs	**Y** or **N**	
wan_lan_accept_packet_logs	**Y** or **N**	
wan_lan_drop_packet_logs	**Y** or **N**	
dmz_lan_accept_packet_logs	**Y** or **N**	
dmz_lan_drop_packet_logs	**Y** or **N**	
wan_dmz_accept_packet_logs	**Y** or **N**	
wan_dmz_drop_packet_logs	**Y** or **N**	
System logs		
change_of_time_by_NTP_logs	**Y** or **N**	Enables or disables logging of time changes of the VPN firewall.
login_attempts_logs	**Y** or **N**	Enables or disables logging of login attempts.
secure_login_attempts_logs	**Y** or **N**	Enables or disables logging of secure login attempts.
reboot_logs	**Y** or **N**	Enables or disables logging of rebooting of the VPN firewall.
unicast_traffic_logs	**Y** or **N**	Enables or disables logging of unicast traffic.
broadcast_or_multicast_traffic_logs	**Y** or **N**	Enables or disables logging of broadcast and multicast traffic.
wan_status_logs	**Y** or **N**	Enables or disables logging of WAN link status–related events.
resolved_DNS_names_logs	**Y** or **N**	Enables or disables logging of resolved DNS names.
vpn_logs	**Y** or **N**	Enables or disables logging of VPN negotiation messages.
dhcp_server_logs	**Y** or **N**	Enables or disables logging of DHCP server events.

Keyword	Associated Keyword to Select	Description
Other event logs		
source_mac_filter_logs	**Y** or **N**	Enables or disables logging of packets from MAC addresses that match the source MAC address filter settings.
session_limit_logs	**Y** or **N**	Enables or disables logging of packets that are dropped because the session limit was exceeded.
bandwidth_limit_logs	**Y** or **N**	Enables or disables logging of packets that are dropped because the bandwidth limit was exceeded.

Command example:

```
FVS336Gv2> system logging configure
system-config[logging-ipv4-ipv6]> lan_wan_drop_packet_logs Y
system-config[logging-ipv4-ipv6]> wan_lan_drop_packet_logs Y
system-config[logging-ipv4-ipv6]> change_of_time_by_NTP_logs Y
system-config[logging-ipv4-ipv6]> secure_login_attempts_logs Y
system-config[logging-ipv4-ipv6]> reboot_logs Y
system-config[logging-ipv4-ipv6]> unicast_traffic_logs Y
system-config[logging-ipv4-ipv6]> bandwidth_limit_logs Y
system-config[logging-ipv4-ipv6]> save
```

Related show commands: *show system logging setup* and *show system logs*

system logging remote configure

This command configures email logs and alerts, schedules email logs and alerts, and configures a syslog server. After you issue the **system logging remote configure** command, you enter the system-config [logging-remote] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**system logging remote configure**
	Mode	system
Step 2	**Format**	**log_identifier** *<identifier>*

```
email_logs_enable {Y | N}
email_server {ipaddress | domain name}
return_email <email address>
send_to_email <email address>
smtp_custom_port <number>
smtp_auth type {None | Plain {smtp_auth username <user name>}
   {smtp_auth password <password>} | CRAM-MD5 {smtp_auth
   username <user name>} {smtp_auth password <password>}}
identd_from_smtp_server_enable {Y | N}


schedule unit {Never | Hourly | Daily {schedule time {0:00 |
   1:00 | 2:00 | 3:00 | 4:00 | 5:00 | 6:00 | 7:00 | 8:00 |
   9:00 | 10:00 | 11:00}} {schedule meridiem {AM | PM}} | Weekly
   {schedule day {Sunday | Monday | Tuesday | Wednesday |
   Thursday | Friday | Saturday}} {schedule time {0:00 | 1:00 |
   2:00 | 3:00 | 4:00 | 5:00 | 6:00 | 7:00 | 8:00 | 9:00 |
   10:00 | 11:00}} {schedule meridiem {AM | PM}}}


syslog_enable {Y | N}
syslog_server {ipaddress | domain name}
syslog_severity {LOG_EMERG | LOG_ALERT | LOG_CRITICAL |
   LOG_ERROR | LOG_WARNING | LOG_NOTICE | LOG_INFO | LOG_DEBUG}
```

Mode system-config [logging-remote]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Log identifier		
log_identifier	*identifier*	The log identifier (alphanumeric string).
Email log configuration		
email_logs_enable	**Y** or **N**	Allows or blocks emailing of logs.
email_server	*ipaddress* or *domain name*	The IP address or domain name of the SMTP server.
return_email	*email address*	The email address (alphanumeric string) to which the SMTP server replies are sent.
send_to_email	*email address*	The email address (alphanumeric string) to which the logs and alerts are sent.
smtp_custom_port	*number*	The port number of the SMTP server for the outgoing email. The default port number is 25.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
smtp_auth type	**None**, **Plain**, or **CRAM-MD5**	Specifies the type of authentication for the SMTP server. If you select **Plain** or **CRAM-MD5**, you also must configure the **smtp_auth username** and **smtp_auth password** keywords and associated parameters.
smtp_auth username	*user name*	The user name for SMTP authentication if you set the **smtp_auth type** keyword type to **Plain** or **CRAM-MD5**.
smtp_auth password	*password*	The password for SMTP authentication if you set **smtp_auth type** keyword to **Plain** or **CRAM-MD5**.
identd_from_smtp_server_enable	**Y** or **N**	Allows or rejects Identd protocol messages from the SMTP server.
Email log schedule		
schedule unit	**Never**, **Hourly**, **Daily**, or **Weekly**	Specifies the type of schedule for emailing logs and alerts: • **Never** or **Hourly**. You do not need to further configure the schedule. • **Daily**. You must also configure the **schedule time** and **schedule meridiem** keywords and their associated keywords. • **Weekly**. You must also configure the **schedule day**, **schedule time**, and **schedule meridiem** keywords and their associated keywords.
schedule day	**Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, or **Saturday**	Specifies the scheduled day if you set the **schedule unit** keyword to **Weekly**.
schedule time	**0:00**, **1:00**, **2:00**, **3:00**, **4:00**, **5:00**, **6:00**, **7:00**, **8:00**, **9:00**, **10:00**, or **11:00**	Specifies the scheduled time if you set the **schedule unit** keyword to **Daily** or **Weekly**.
schedule meridiem	**AM** or **PM**	Specifies the meridiem for the start time if you set the **schedule unit** keyword to **Daily** or **Weekly**.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Syslog server		
syslog_enable	**Y** or **N**	Enables or disables the syslog server.
syslog_server	*ipaddress* or *domain name*	The IP address or domain name of the syslog server.
syslog_severity	**LOG_EMERG**, **LOG_ALERT**, **LOG_CRITICAL**, **LOG_ERROR**, **LOG_WARNING**, **LOG_NOTICE**, **LOG_INFO**, or **LOG_DEBUG**	Specifies the syslog severity level. The keywords are self-explanatory. **Note:** All the logs for messages with a severity that is equal to or higher than the severity that you specify are logged on the specified syslog server. For example, if you select **LOG_CRITICAL** as the severity, messages with the severities **LOG_CRITICAL**, **LOG_ALERT**, and **LOG_EMERG** are logged.

Command example:

```
FVS336Gv2> system logging remote configure
system-config[logging-remote]> log_identifier FVS336Gv2-Bld3
system-config[logging-remote]> email_logs_enable Y
system-config[logging-remote]> email_server SMTP.Netgear.com
system-config[logging-remote]> return_email FVS336Gv2@netgear.com
system-config[logging-remote]> send_to_email admin2@netgear.com
system-config[logging-remote]> smtp_custom_port 2025
system-config[logging-remote]> smtp_auth type None
system-config[logging-remote]> schedule unit Weekly
system-config[logging-remote]> schedule day Sunday
system-config[logging-remote]> schedule time 00
system-config[logging-remote]> schedule meridiem AM
system-config[logging-remote]> syslog_enable Y
system-config[logging-remote]> syslog_server fe80::a0ca:f072:127f:b028%21
system-config[logging-remote]> syslog_severity LOG_EMERG
system-config[logging-remote]> save
```

Related show command: *show system logging remote setup*

System Reboot Command

This section describes the **system schedule_reboot configure** command.

system schedule_reboot configure

This command schedules the VPN firewall to be rebooted daily at a specific time. After you issue the **system schedule_reboot configure** command, you enter the system-config [schedule-reboot] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**system schedule_reboot configure**
	Mode	system
Step 2	**Format**	**schedule_reboot_enable** {**Y** | **N**} **schedule_reboot_hour** <*hour*> **schedule_reboot_minute** <*minute*>
	Mode	system-config [schedule-reboot]

Keyword	Associated Parameter to Type	Description
schedule_reboot_enable	**Y** or **N**	Allows the VPN firewall to be rebooted daily or prevents the VPN firewall from being rebooted daily.
schedule_reboot_hour	*hour*	The hour in the format HH (00 to 23) that the VPN firewall reboots.
schedule_reboot_minute	*minute*	The minute in the format MM (00 to 59) that the VPN firewall reboots.

Command example:

```
FVS336Gv2> system schedule_reboot configure
system-config[snmp-system]> schedule_reboot_enable Y
system-config[snmp-system]> schedule_reboot_hour 23
system-config[snmp-system]> schedule_reboot_minute 45
system-config[snmp-system]> save
```

Related show command: *show system schedule_reboot*

VPN Mode Configuration Commands

6

This chapter explains the configuration commands, keywords, and associated parameters in the vpn mode. The chapter includes the following sections:

- *IPSec VPN Wizard Command*
- *IPSec IKE Policy Commands*
- *IPSec VPN Policy Commands*
- *IPSec VPN Mode Config Commands*
- *SSL VPN Wizard Command*
- *SSL VPN Portal Layout Commands*
- *SSL VPN Authentication Domain Commands*
- *SSL VPN Authentication Group Commands*
- *SSL VPN User Commands*
- *SSL VPN Port Forwarding Commands*
- *SSL VPN Client and Client Route Commands*
- *SSL VPN Resource Commands*
- *SSL VPN Policy Commands*
- *RADIUS Server Command*
- *PPTP Server Command*
- *L2TP Server Command*

IMPORTANT:

After you issue a command that includes the word `configure`, `add`, or `edit`, you must save (or cancel) your changes. For more information, see *Configuration Commands: Save Commands* on page 13.

IPSec VPN Wizard Command

This section describes the **vpn ipsec wizard configure** <**Gateway | VPN_Client**> command.

vpn ipsec wizard configure <Gateway | VPN_Client>

This command configures the IPSec VPN wizard for a gateway-to-gateway or gateway-to-VPN client connection. After you issue the **vpn ipsec wizard configure** command to specify the type of peer for which you want to configure the wizard, you enter the vpn-config [wizard] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn ipsec wizard configure** {**Gateway** | **VPN_Client**}
	Mode	vpn
Step 2	**Format**	**ip_version** {**IPv4** | **IPv6**} **conn_name** <*name*> **preshared_key** <*key*> **local_wan_interface** {**WAN1** | **WAN2**} **enable_rollover** {**N** | **Y** {**rollover_gateway** {**WAN1** | **WAN2**}) **remote_wan_ipaddress** {<*ipaddress*> | <*ipv6-address*> | <*domain name*>} **local_wan_ipaddress** {<*ipaddress*> | <*ipv6-address*> | <*domain name*>} **remote_lan_ipaddress** <*ipaddress*> **remote_lan_net_mask** <*subnet mask*> **remote_lan_ipv6_address** <*ipv6-address*> **remote_lan_prefix_length** <*prefix length*>
	Mode	vpn-config [wizard]

Keyword	Associated Keyword to Select or Parameter to Type	Description
ip_version	**IPv4** or **IPv6**	Specifies the IP address version for both the local and remote endpoints: • **IPv4**. Both endpoints use IPv4 addresses. For the remote LAN IP address, you must issue the **remote_lan_ipaddress** and **remote_lan_net_mask** keywords and specify the associated parameters. • **IPv6**. Both endpoints use IPv6 addresses. For the remote LAN IP address, you must issue the **remote_lan_ipv6_address** and **remote_lan_prefix_length** keywords and specify the associated parameters.
conn_name	*connection name*	The unique connection name (alphanumeric string).
preshared_key	*key*	The key (alphanumeric string) to be entered on both peers.
local_wan_interface	**WAN1** or **WAN2**	Specifies the local WAN interface that the VPN tunnel uses as the local endpoint.
enable_rollover	**Y** or **N**	Enables or disables VPN rollover mode. If VPN rollover mode is enabled, you must issue the **rollover_gateway** keyword to specify the WAN interface to which the VPN rollover occurs. **Note:** Rollover mode functions only when the IP version is IPV4.
rollover_gateway	**WAN1** or **WAN2**	If VPN rollover mode is enabled, specifies the WAN interface to which the rollover occurs.
Remote WAN and local WAN address information		
remote_wan_ipaddress	*ipaddress*, *ipv6-address*, or *domain name*	Depending on the setting of the **ip_version** keyword, specifies an IPv4 or IPv6 local WAN address. You can also specify a domain name.
local_wan_ipaddress	*ipaddress*, *ipv6-address*, or *domain name*	Depending on the setting of the **ip_version** keyword, specifies an IPv4 or IPv6 local WAN address. You can also specify a domain name.
Remote LAN IPv4 address information		
remote_lan_ipaddress	*ipaddress*	The IPv4 remote LAN address when the **ip_version** keyword is set to **IPv4**.

Keyword	Associated Keyword to Select or Parameter to Type	Description
remote_lan_net_mask	*subnet mask*	The IPv4 remote LAN subnet mask when the **ip_version** keyword is set to **IPv4**.
Remote LAN IPv6 address information		
remote_lan_ipv6_address	*ipv6-address*	The IPv6 remote LAN address when the **ip_version** keyword is set to **IPv6**.
remote_lan_prefix_length	*prefix length*	The IPv6 remote LAN prefix length when the **ip_version** keyword is set to **IPv6**.

Command example:

```
FVS336Gv2> vpn ipsec wizard configure Gateway
vpn-config[wizard]> ip_version IPv6
vpn-config[wizard]> conn_name FVS336Gv2-to-Peer44
vpn-config[wizard]> preshared_key 2%sgd55%!@GH
vpn-config[wizard]> local_wan_interface WAN1
vpn-config[wizard]> enable_rollover N
vpn-config[wizard]> remote_wan_ipaddress peer44.com
vpn-config[wizard]> local_wan_ipaddress fe80::a8ab:bbff:fe00:2
vpn-config[wizard]> remote_lan_ipv6_address fe80::a4bb:ffdd:fe01:2
vpn-config[wizard]> remote_lan_prefix_length 64
vpn-config[wizard]> save
```

Related show commands: *show vpn ipsec vpnpolicy setup*, *show vpn ipsec ikepolicy setup*, and *show vpn ipsec vpnpolicy status*

To display the VPN policy configuration that the wizard created through the **vpn ipsec wizard configure** command, issue the **show vpn ipsec vpnpolicy setup** command:

```
FVS336Gv2> show vpn ipsec vpnpolicy setup

Status  Name              Type        IPSec Mode  Local                                  Remote                          Auth  Encr
______  ________________  __________  __________  _____________________________________  ______________________________  ____  ____
Enabled FVS336Gv2-to-Peer44 Auto Policy  Tunnel Mode 2002:408b:36e4:a:a8ab:bbff:fe00:1 / 64 fe80::a4bb:ffdd:fe01:2 / 64    SHA-1 3DES
Enabled FVS-to-Paris        Auto Policy  Tunnel Mode 192.168.1.0 / 255.255.255.0          192.168.50.0 / 255.255.255.255 SHA-1 3DES
```

To display the IKE policy configuration that the wizard created through the **vpn ipsec wizard configure** command, issue the **show vpn ipsec ikepolicy setup** command:

```
FVS336Gv2> show vpn ipsec ikepolicy setup

List of IKE Policies
____________________

Name                Mode       Local ID               Remote ID     Encryption Authentication  DH Group
____________________ __________ _____________________ _____________ __________ _____________ ____________
FVS336Gv2-to-Peer44 main       fe80::a8ab:bbff:fe00:2 peer44.com    3DES       SHA-1      Group 2 (1024 bit)
FVS-to-Paris        main       10.139.54.228          10.112.71.154 3DES       SHA-1      Group 2 (1024 bit)
iphone              aggressive 10.139.54.228          0.0.0.0       AES-128    SHA-1      Group 2 (1024 bit)
```

IPSec IKE Policy Commands

This section describes the following commands:

- *vpn ipsec ikepolicy configure <ike policy name>*
- *vpn ipsec ikepolicy delete <ike policy name>*

vpn ipsec ikepolicy configure <ike policy name>

This command configures a new or existing manual IPSec IKE policy. After you issue the **vpn ipsec ikepolicy configure** command to specify the name of a new or existing IKE policy, you enter the vpn-config [ike-policy] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1

Format `vpn ipsec ikepolicy configure <ike policy name>`

Mode vpn

Step 2

Format

```
enable_mode_config {N |Y {mode_config_record <record name>}}
direction_type {Initiator | Responder | Both}
exchange_mode {Main | Aggresive}

ip_version {IPv4 | IPv6}
select_local_gateway {WAN1 | WAN2}
local_ident_type {Local_Wan_IP | FQDN | User-FQDN | DER_ASN1_DN}
   {local_identifier <identifier>}
remote_ident_type {Remote_Wan_IP | FQDN | User-FQDN |
   DER_ASN1_DN}{remote_identifier <identifier>}

encryption_algorithm {DES | 3DES | AES_128 | AES_192 | AES_256}
auth_algorithm {MD5 | SHA-1}
auth_method {Pre_shared_key {pre_shared_key <key>} |
   RSA_Signature}
dh_group {Group1_768_bit | Group2_1024_bit | Group5_1536_bit}
lifetime <seconds>
enable_dead_peer_detection {N | Y {detection_period <seconds>}
   {reconnect_failure_count <number>}}

extended_authentication {None | IPSecHost {xauth_username
   <user name>} {xauth_password <password>} | EdgeDevice
   {extended_authentication_type {User-Database | RadiusPap |
   RadiusChap}}}
```

Mode vpn-config [ike-policy]

Keyword	Associated Keyword to Select or Parameter to Type	Description
Mode Config record selection and general policy settings		
enable_mode_config	**Y** or **N**	Specifies whether or not the IKE policy uses a Mode Config record.
mode_config_record	*record name*	If the **enable_mode_config** keyword is set to **Y**, specifies which Mode Config record to be used. For information about configuring Mode Config records, see the *vpn ipsec mode_config configure <record name>* command.
direction_type	**Initiator**, **Responder**, or **Both**	Specifies the IKE direction type: • **Initiator**. The VPN firewall initiates the connection to the remote endpoint. • **Responder**. The VPN firewall responds only to an IKE request from the remote endpoint. • **Both**. The VPN firewall can both initiate a connection to the remote endpoint and respond to an IKE request from the remote endpoint.
exchange_mode	**Main** or **Aggresive**	Specifies the exchange mode: • **Main**. This mode is slower than the Aggressive mode but more secure. • **Aggressive**. This mode is faster than the Main mode but less secure. When the IKE policy uses a Mode Config record, the exchange mode must be set to **Aggresive**.
Local and remote identifiers		
ip_version	**IPv4** or **IPv6**	If the **local_ident_type** and **remote_ident_type** keywords are set to **Local_Wan_IP**, specifies the IP address version for both the local and remote endpoints: • **IPv4**. Both endpoints use IPv4 addresses. You must specify IPv4 addresses for the **local_identifier** and **remote_identifier** keywords. • **IPv6**. Both endpoints use IPv6 addresses. You must specify IPv6 addresses for the **local_identifier** and **remote_identifier** keywords.
select_local_gateway	**WAN1** or **WAN2**	Specifies the WAN interface for the local gateway.

Keyword	Associated Keyword to Select or Parameter to Type	Description
local_ident_type	**Local_Wan_IP**, **FQDN**, **User-FQDN**, or **DER_ASN1_DN**	Specifies the ISAKMP identifier to be used by the VPN firewall: • **Local_Wan_IP**. The WAN IP address of the VPN firewall. The setting of the **ip_version** keyword determines if you must specify an IPv4 or IPv6 address for the **local_identifier** keyword. • **FQDN**. The domain name for the VPN firewall. • **User-FQDN**. The email address for a local VPN client or the VPN firewall. • **DER_ASN1_DN**. A distinguished name (DN) that identifies the VPN firewall in the DER encoding and ASN.1 format.
local_identifier	*identifier*	The identifier of the VPN firewall. The setting of the **local_ident_type** and **ip_version** keywords determines the type of identifier that you must specify.
remote_ident_type	**Remote_Wan_IP**, **FQDN**, **User-FQDN**, or **DER_ASN1_DN**	Specifies the ISAKMP identifier to be used by the VPN firewall: • **Remote_Wan_IP**. The WAN IP address of the remote endpoint. The setting of the **ip_version** keyword determines if you must specify an IPv4 or IPv6 address for the **local_identifier** keyword. • **FQDN**. The domain name for the VPN firewall. • **User-FQDN**. The email address for a local VPN client or the VPN firewall. • **DER_ASN1_DN**. A distinguished name (DN) that identifies the VPN firewall in the DER encoding and ASN.1 format.
remote_identifier	*identifier*	The identifier of the remote endpoint. The setting of the **remote_ident_type** and **ip_version** keywords determines the type of identifier that you must specify.

Keyword	Associated Keyword to Select or Parameter to Type	Description
IKE SA settings		
encryption_algorithm	**DES**, **3DES**, **AES_128**, **AES_192**, or **AES_256**	Specifies the algorithm to negotiate the security association (SA): • **DES**. Data Encryption Standard (DES). • **3DES**. Triple DES. • **AES_128**. Advanced Encryption Standard (AES) with a 128-bit key size. • **AES_192**. AES with a 192-bit key size. • **AES_256**. AES with a 256-bit key size.
auth_algorithm	**MD5** or **SHA-1**	Specifies the algorithm to be used in the VPN header for the authentication process: • **SHA-1**. Hash algorithm that produces a 160-bit digest. • **MD5**. Hash algorithm that produces a 128-bit digest.
auth_method	**Pre_shared_key** or **RSA_Signature**	Specifies the authentication method: • **Pre_shared_key**. A secret that is shared between the VPN firewall and the remote endpoint. You also must issue the **pre_shared_key** keyword and specify the key. • **RSA_Signature**. Uses the active self-signed certificate that you uploaded on the Certificates screen of the web management interface. **Note:** You cannot upload certificates by using the CLI.
pre_shared_key	*key*	If the **auth_method** keyword is set to **Pre_shared_key**, specifies a key with a minimum length of 8 characters and no more than 49 characters.
dh_group	**Group1_768_bit**, **Group2_1024_bit**, or **Group5_1536_bit**	Specifies the Diffie-Hellman (DH) group, which sets the strength of the algorithm in bits. The higher the group, the more secure the exchange.
lifetime	*seconds*	The period in seconds for which the IKE SA is valid. When the period times out, the next rekeying occurs.

Keyword	Associated Keyword to Select or Parameter to Type	Description
enable_dead_peer_detection	**Y** or **N**	Enables or disables dead peer detection (DPD). When DPD is enabled, you also must issue the **detection_period** and **reconnect_failure_count** keywords and associated parameters.
detection_period	*seconds*	The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle.
reconnect_failure_count	*number*	The maximum number of DPD failures before the VPN firewall tears down the connection and then attempts to reconnect to the peer.
Extended authentication settings		
extended_authentication	**None**, **IPSecHost**, or **EdgeDevice**	Specifies whether or not Extended Authentication (XAUTH) is enabled, and, if enabled, which device is used to verify user account information: • **None**. XAUTH is disabled. This the default setting. • **IPSecHost**. The VPN firewall functions as a VPN client of the remote gateway. In this configuration the VPN firewall is authenticated by a remote gateway. You must issue the **xauth_username** and **xauth_password** keywords and specify the associated parameters. • **EdgeDevice**. The VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. You must issue the **extended_authentication_type** keyword and select an associated keyword.

Keyword	Associated Keyword to Select or Parameter to Type	Description
extended_authentication_type	**User-Database**, **RadiusPap**, or **RadiusChap**	If the **extended_authentication** keyword is set to **EdgeDevice**, specifies the authentication type: • **User-Database**. XAUTH occurs through the VPN firewall's user database. • **RadiusPap**. XAUTH occurs through RADIUS Password Authentication Protocol (PAP). • **RadiusChap**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). **Note:** For information about how to configure a RADIUS server for authentication of VPN connections, see *RADIUS Server Command*.
xauth_username	*user name*	If the **extended_authentication** keyword is set to **IPSecHost**, specifies a user name.
xauth_password	*password*	If the **extended_authentication** keyword is set to **IPSecHost**, specifies a password.

Command example:

```
FVS336Gv2> vpn ipsec ikepolicy configure FVS-to-Paris
vpn-config[ike-policy]> enable_mode_config N
vpn-config[ike-policy]> direction_type Both
vpn-config[ike-policy]> exchange_mode Main
vpn-config[ike-policy]> ip_version ipv4
vpn-config[ike-policy]> select_local_gateway WAN1
vpn-config[ike-policy]> local_ident_type Local_Wan_IP
vpn-config[ike-policy]> local_identifier 10.139.54.228
vpn-config[ike-policy]> remote_ident_type Remote_Wan_IP
vpn-config[ike-policy]> remote_identifier 10.112.71.154
vpn-config[ike-policy]> encryption_algorithm 3DES
vpn-config[ike-policy]> auth_algorithm SHA-1
vpn-config[ike-policy]> auth_method Pre_shared_key
vpn-config[ike-policy]> pre_shared_key 3Tg67!JXL0Oo?
vpn-config[ike-policy]> dh_group Group2_1024_bit
vpn-config[ike-policy]> lifetime 28800
vpn-config[ike-policy]> enable_dead_peer_detection Y
vpn-config[ike-policy]> detection_period 20
vpn-config[ike-policy]> reconnect_failure_count 3
vpn-config[ike-policy]> extended_authentication EdgeDevice
vpn-config[ike-policy]> extended_authentication_type RadiusChap
vpn-config[ike-policy]> save
```

Related show command: *show vpn ipsec ikepolicy setup*

vpn ipsec ikepolicy delete <ike policy name>

This command deletes an IKE policy by specifying the name of the IKE policy.

Format	**vpn ipsec ikepolicy delete** *<ike policy name>*
Mode	vpn

Related show command: *show vpn ipsec ikepolicy setup*

IPSec VPN Policy Commands

This section describes the following commands:

- *vpn ipsec vpnpolicy configure <vpn policy name>*
- *vpn ipsec vpnpolicy delete <vpn policy name>*
- *vpn ipsec vpnpolicy disable <vpn policy name>*
- *vpn ipsec vpnpolicy enable <vpn policy name>*
- *vpn ipsec vpnpolicy connect <vpn policy name>*
- *vpn ipsec vpnpolicy drop <vpn policy name>*

vpn ipsec vpnpolicy configure <vpn policy name>

This command configures a new or existing auto IPSec VPN policy or manual IPSec VPN policy. After you issue the **vpn ipsec vpnpolicy configure** command to specify the name of a new or existing VPN policy, you enter the vpn-config [vpn-policy] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn ipsec vpnpolicy configure** *<vpn policy name>*
	Mode	vpn

Step 2 **Format**

```
general_policy_type {Auto-Policy | Manual-Policy}
general_ip_version {IPv4 | IPv6}
general_select_local_gateway {WAN1 | WAN2}
general_remote_end_point_type {FQDN {general_remote_end_point
   fqdn <domain name> | IP-Address {general_remote_end_point
   ip_address <ipaddress> | {general_remote_end_point
   ipv6_address <ipv6-address>}}
general_enable_netbios {N | Y}
general_enable_rollover {N | Y {general_rollover_gateway {WAN1 |
   WAN2}}
general_enable_auto_initiate_policy {N | Y}
general_enable_keep_alive {N | Y {general_ping_ip_address
   <ipaddress> | {general_ping_ip_address6 <ipv6-address>}
   {general_keep_alive_detection_period <seconds>}
   {general_keep_alive_failure_count <number>}}


general_local_network_type {ANY | SINGLE
   {general_local_start_address <ipaddress> |
   general_local_start_address_ipv6 <ipv6-address>} | RANGE
   {{general_local_start_address <ipaddress>}
   {general_local_end_address <ipaddress>} |
   {general_local_start_address_ipv6 <ipv6-address>}
   {general_local_end_address_ipv6 <ipv6-address>}} | SUBNET
   {{general_local_start_address <ipaddress>}
   {general_local_subnet_mask <subnet mask>} |
   {general_local_start_address_ipv6 <ipv6-address>}
   {general_local_ipv6_prefix_length <prefix length>}}}


general_remote_network_type {ANY | SINGLE
   {general_remote_start_address <ipaddress> |
   general_remote_start_address_ipv6 <ipv6-address>} | RANGE
   {{general_remote_start_address <ipaddress>}
   {general_remote_end_address <ipaddress>} |
   {general_remote_start_address_ipv6 <ipv6-address>}
   {general_remote_end_address_ipv6 <ipv6-address>}} | SUBNET
   {{general_remote_start_address <ipaddress>}
   {general_remote_subnet_mask <subnet mask>} |
   {general_remote_start_address_ipv6 <ipv6-address>}
   {general_remote_ipv6_prefix_length <prefix length>}}}


manual_spi_in <number>
manual_encryption_algorithm {None | DES | 3DES | AES-128 |
   AES-192 | AES-256}
manual_encryption_key_in <key>
manual_encryption_key_out <key>


manual_spi_out <number>
manual_integrity_algorithm {MD5 | SHA-1}
manual_integrity_key_in <key>
manual_integrity_key_out <key>
```

```
auto_sa_lifetime_type {Seconds {auto_sa_lifetime <seconds>} |
   KBytes {auto_sa_lifetime <number>}}
auto_encryption_algorithm {None | DES | 3DES | AES-128 |
   AES-192 | AES-256}
auto_integrity_algorithm {MD5 | SHA-1}
auto_enable_pfskeygroup {N | Y {auto_dh_group {Group1_768_bit |
   Group2_1024_bit | Group5_1536_bit}}}
auto_select_ike_policy <ike policy name>
```

Mode vpn-config [vpn-policy]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
General policy settings		
general_policy_type	**Auto-Policy** or **Manual-Policy**	Species whether the policy type is an auto or manual VPN policy: • **Auto-Policy**. The inbound and outbound policy settings for the VPN tunnel are automatically generated after you issue the keywords and associated parameters that are listed in the Auto policy settings section of this table. You must specify all other VPN policy settings manually. • **Manual-Policy**. You must specify all settings manually, excluding the ones in the Auto policy settings section of this table.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
general_ip_version	**IPv4** or **IPv6**	If the **general_remote_end_point_type** keyword is set to **IP-Address**, specifies the IP address version for the remote endpoint, local address information, and remote address information: • **IPv4**. The IPv4 selection requires you to specify IPv4 addresses for the following keywords: - **general_remote_end_point ip_address** - **general_local_start_address** - **general_local_end_address** - **general_remote_start_address** - **general_remote_end_address** • **IPv6**. The IPv6 selection requires you to specify IPv6 addresses for the following keywords: - **general_remote_end_point ipv6_address** - **general_local_start_address_ipv6** - **general_local_end_address_ipv6** - **general_remote_start_address_ipv6** - **general_remote_end_address_ipv6**
general_select_local_gateway	**WAN1** or **WAN2**	Specifies the local WAN interface that the VPN tunnel uses as the local endpoint.
general_remote_end_point_type	**IP-Address** or **FQDN**	Specifies whether the remote endpoint is defined by an IP address or a domain name: • **IP-Address**. Depending on the setting of the **general_ip_version** keyword, you must either issue the **general_remote_end_point ip_address** keyword and specify an IPv4 address or issue the **general_remote_end_point ipv6_address** keyword and specify an IPv6 address. • **FQDN**. You must issue the **general_remote_end_point fqdn** keyword and specify a domain name.
general_remote_end_point fqdn	*domain name*	If the **general_remote_end_point_type** keyword is set to **FQDN**, the domain name (FQDN) of the remote endpoint.
general_remote_end_point ip_adress	*ipaddress*	If the **general_remote_end_point_type** keyword is set to **IP-Address**, and if the **general_ip_version** keyword is set to **IPv4**, the IPv4 address of the remote endpoint.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
general_remote_end_point ipv6_adress	*ipv6-address*	If the **general_remote_end_point_type** keyword is set to **IP-Address**, and if the **general_ip_version** keyword is set to **IPv6**, the IPv6 address of the remote endpoint.
general_enable_netbios	**Y** or **N**	Allows or blocks NetBIOS broadcasts over the VPN tunnel.
general_enable_rollover	**Y** or **N**	Enables or disables VPN rollover mode. If VPN rollover mode is enabled, you must issue the **general_rollover_gateway** keyword to specify the WAN interface to which the VPN rollover occurs. **Note:** Rollover mode functions only when the IP version is IPV4.
general_rollover_gateway	**WAN1** or **WAN2**	If VPN rollover mode is enabled, specifies the WAN interface to which the rollover occurs.
general_enable_auto_initiate_ policy	**Y** or **N**	Allows or blocks automatic establishment of the VPN tunnel when no traffic is being processed. **Note:** You cannot allow automatic establishment of the VPN tunnel if the **direction_type** keyword under the *vpn ipsec ikepolicy configure <ike policy name>* command is set to **Responder**.
general_enable_keep_alive	**Y** or **N**	Allows the VPN firewall to send keep-alive requests (ping packets) to the remote endpoint to keep the tunnel alive or blocks the VPN firewall from sending keep-alive requests. If you allow keep-alives, you also must issue the following keywords: • Either **general_ping_ip_address** to specify an IPv4 address or **general_ping_ip_address6** to specify an IPv6 address. • **general_keep_alive_detection_period** to specify the detection period. • **general_keep_alive_failue_count** to specify the failure count.
general_ping_ip_address	*ipaddress*	The IPv4 address where keep-alive requests are sent to.
general_ping_ip_address6	*ipv6-address*	The IPv6 address where keep-alive requests are sent to.
general_keep_alive_detection_ period	*seconds*	The period in seconds between consecutive keep-alive requests, which are sent only when the IPSec traffic is idle.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
general_keep_alive_failure_count	*number*	The maximum number of keep-alive request failures before the VPN firewall tears down the connection and then attempts to reconnect to the peer.
Traffic selector settings—Local address information		
general_local_network_type	**ANY**, **SINGLE**, **RANGE**, or **SUBNET**	Specifies the address or addresses that are part of the VPN tunnel on the VPN firewall: • **ANY**. All computers and devices on the network. • **SINGLE**. A single IP address on the network. Depending on the setting of the **general_ip_version** keyword, issue one of the following keywords: - **general_local_start_address** to specify an IPv4 address. - **general_local_start_address_ipv6** to specify an IPv6 address. • **RANGE**. A range of IP addresses on the network. Depending on the setting of the **general_ip_version** keyword, issue one of the following sets of keywords: - **general_local_start_address** and **general_local_end_address** to specify IPv4 addresses. - **general_local_start_address_ipv6** and **general_local_end_address_ipv6** to specify IPv6 addresses. • **SUBNET**. A subnet on the network. Depending on the setting of the **general_ip_version** keyword, issue one of the following sets of keywords: - **general_local_start_address** to specify an IPv4 address and **general_local_subnet_mask** to specify a subnet mask. - **general_local_start_address_ipv6** to specify an IPv6 address and **general_local_ipv6_prefix_length** to specify a prefix length.
general_local_start_address	*ipaddress*	If the **general_local_network_type** keyword is set to **SINGLE**, **RANGE**, or **SUBNET**, and if the **general_ip_version** keyword is set to **IPv4**, specifies the local IPv4 (start) address.
general_local_end_address	*ipaddress*	If the **general_local_network_type** keyword is set to **RANGE**, and if the **general_ip_version** keyword is set to **IPv4**, specifies the local IPv4 end address.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
general_local_subnet_mask	*subnet mask*	If the **general_local_network_type** keyword is set to **SUBNET**, and if the **general_ip_version** keyword is set to **IPv4**, specifies the subnet mask.
general_local_start_address_ipv6	*ipv6-address*	If the **general_local_network_type** keyword is set to **SINGLE**, **RANGE**, or **SUBNET**, and if the **general_ip_version** keyword is set to **IPv6**, specifies the local IPv6 (start) address.
general_local_end_address_ipv6	*ipv6-address*	If the **general_local_network_type** keyword is set to **RANGE**, and if the **general_ip_version** keyword is set to **IPv6**, specifies the local IPv6 end address.
general_local_ipv6_prefix_length	*prefix length*	If the **general_local_network_type** keyword is set to **SUBNET**, and if the **general_ip_version** keyword is set to **IPv6**, specifies the prefix length.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Traffic selector settings—Remote address information		
general_remote_network_type	**ANY**, **SINGLE**, **RANGE**, or **SUBNET**	Specifies the address or addresses that are part of the VPN tunnel on the remote end: • **ANY**. All computers and devices on the network. • **SINGLE**. A single IP address on the network. Depending on the setting of the **general_ip_version** keyword, issue one of the following keywords: - **general_remote_start_address** to specify an IPv4 address. - **general_remote_start_address_ipv6** to specify an IPv6 address. • **RANGE**. A range of IP addresses on the network. Depending on the setting of the **general_ip_version** keyword, issue one of the following sets of keywords: - **general_remote_start_address** and **general_remote_end_address** to specify IPv4 addresses. - **general_remote_start_address_ipv6** and **general_remote_end_address_ipv6** to specify IPv6 addresses. • **SUBNET**. A subnet on the network. Depending on the setting of the **general_ip_version** keyword, issue one of the following sets of keywords: - **general_remote_start_address** to specify an IPv4 address and **general_remote_subnet_mask** to specify a subnet mask. - **general_remote_start_address_ipv6** to specify an IPv6 address and **general_remote_ipv6_prefix_length** to specify a prefix length.
general_remote_start_address	*ipaddress*	If the **general_remote_network_type** keyword is set to **SINGLE**, **RANGE**, or **SUBNET**, and if the **general_ip_version** keyword is set to **IPv4**, specifies the remote IPv4 (start) address.
general_remote_end_address	*ipaddress*	If the **general_remote_network_type** keyword is set to **RANGE**, and if the **general_ip_version** keyword is set to **IPv4**, specifies the remote IPv4 end address.
general_remote_subnet_mask	*subnet mask*	If the **general_remote_network_type** keyword is set to **SUBNET**, and if the **general_ip_version keyword** is set to **IPv4**, specifies the subnet mask.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
general_remote_start_address_ipv6	*ipv6-address*	If the **general_remote_network_type** keyword is set to **SINGLE**, **RANGE**, or **SUBNET**, and if the **general_ip_version** keyword is set to **IPv6**, specifies the remote IPv6 (start) address.
general_remote_end_address_ipv6	*ipv6-address*	If the **general_remote_network_type** keyword is set to **RANGE**, and if the **general_ip_version** keyword is set to **IPv6**, specifies the remote IPv6 end address.
general_remote_ipv6_prefix_length	*prefix length*	If the **general_remote_network_type** keyword is set to **SUBNET,** and if the **general_ip_version** keyword is set to **IPv6**, specifies the prefix length.
Manual policy settings—Inbound policy		
manual_spi_in	*number*	The security parameter index (SPI) for the inbound policy as a hexadecimal value between 3 and 8 characters.
manual_encryption_algorithm	**None**, **DES**, **3DES**, **AES-128**, **AES-192**, **AES-256**	Specifies the encryption algorithm, if any, to negotiate the security association (SA): • **None**. No encryption algorithm is enabled. • **DES**. Data Encryption Standard (DES). • **3DES**. Triple DES. • **AES-128**. Advanced Encryption Standard (AES) with a 128-bit key size. • **AES-192**. AES with a 192-bit key size. • **AES-256**. AES with a 256-bit key size.
manual_encryption_key_in	*key*	The encryption key for the inbound policy. The length of the key depends on setting of the **manual_encryption_algorithm** keyword.
manual_encryption_key_out	*key*	The encryption key for the outbound policy. The length of the key depends on setting of the **manual_encryption_algorithm** keyword.
Manual policy settings—Outbound policy		
manual_spi_out	*number*	The security parameters index (SPI) for the outbound policy as a hexadecimal value between 3 and 8 characters.
manual_integrity_algorithm	**MD5** or **SHA-1**	Specifies the integrity (authentication) algorithm for the security association (SA): • **SHA-1**. Hash algorithm that produces a 160-bit digest. • **MD5**. Hash algorithm that produces a 128-bit digest.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
manual_integrity_key_in	*key*	The integrity (encryption) key for the inbound policy. The length of the key depends on setting of the **manual_integrity_algorithm** keyword.
manual_integrity_key_out	*key*	The integrity (encryption) key for the outbound policy. The length of the key depends on setting of the **manual_integrity_algorithm** keyword.
Auto policy settings		
auto_sa_lifetime_type	**Seconds** or **KBytes**	Specifies the type of lifetime of the security association (SA): • **Seconds**. The SA lifetime is defined in a period of seconds. You must issue the **auto_sa_lifetime** keyword and specify the period in seconds. • **KBytes**. The SA lifetime is defined in transmitted data in KBytes. You must issue the **auto_sa_lifetime** keyword and specify the number of bytes. **Note:** After the SA lifetime is exceeded, the SA becomes invalid and must be renegotiated.
auto_sa_lifetime	*seconds* or *number*	If the **auto_sa_lifetime_type** keyword is set to **Seconds**, specify the SA lifetime in seconds. If the **auto_sa_lifetime_type** keyword is set to **KBytes**, specify the SA lifetime in bytes.
auto_encryption_algorithm	**None**, **DES**, **3DES**, **AES-128**, **AES-192**, **AES-256**	Specifies the encryption algorithm, if any, to negotiate the security association (SA): • **None**. No encryption algorithm is enabled. • **DES**. Data Encryption Standard (DES). • **3DES**. Triple DES. • **AES-128**. Advanced Encryption Standard (AES) with a 128-bit key size. • **AES-192**. AES with a 192-bit key size. • **AES-256**. AES with a 256-bit key size.
auto_integrity_algorithm	**MD5** or **SHA-1**	Specifies the integrity (authentication) algorithm to negotiate the security association (SA): • **SHA-1**. Hash algorithm that produces a 160-bit digest. • **MD5**. Hash algorithm that produces a 128-bit digest.
auto_enable_pfskeygroup	**Y** or **N**	Enables or disables Perfect Forward Secrecy (PFS). If you enable PFS, you must issue the **auto_dh_group** keyword to specify a group.

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
auto_dh_group	**Group1_768_bit**, **Group2_1024_bit**, or **Group5_1536_bit**	Specifies the Diffie-Hellman (DH) group, which sets the strength of the algorithm in bits. The higher the group, the more secure the exchange.
auto_select_ike_policy	*ike policy name*	Selects an existing IKE policy that defines the authentication negotiation.

Command example:

```
FVS336Gv2> vpn ipsec vpnpolicy configure FVS-to-Paris
vpn-config[vpn-policy]> general_policy_type Auto-Policy
vpn-config[vpn-policy]> general_ip_version IPv4
vpn-config[vpn-policy]> general_select_local_gateway WAN1
vpn-config[vpn-policy]> general_enable_rollover Y
vpn-config[vpn-policy]> general_rollover_gateway WAN2
vpn-config[vpn-policy]> general_remote_end_point_type IP-Address
vpn-config[vpn-policy]> general_remote_end_point ip_address 10.112.71.154
vpn-config[vpn-policy]> general_local_network_type SUBNET
vpn-config[vpn-policy]> general_local_start_address 192.168.1.0
vpn-config[vpn-policy]> general_local_subnet_mask 255.255.255.0
vpn-config[vpn-policy]> general_remote_network_type SUBNET
vpn-config[vpn-policy]> general_remote_start_address 192.168.50.0
vpn-config[vpn-policy]> general_remote_subnet_mask 255.255.255.255
vpn-config[vpn-policy]> auto_sa_lifetime type Seconds
vpn-config[vpn-policy]> auto_sa_lifetime 3600
vpn-config[vpn-policy]> auto_encryption_algorithm 3DES
vpn-config[vpn-policy]> auto_integrity_algorithm SHA-1
vpn-config[vpn-policy]> auto_select_ike_policy FVS-to-Paris
vpn-config[vpn-policy]> save
```

Related show commands: *show vpn ipsec vpnpolicy setup* and *show vpn ipsec vpnpolicy status*

vpn ipsec vpnpolicy delete <vpn policy name>

This command deletes a VPN policy by specifying the name of the VPN policy.

Format	**vpn ipsec vpnpolicy delete** <*vpn policy name*>
Mode	vpn

Related show command: *show vpn ipsec vpnpolicy setup*

vpn ipsec vpnpolicy disable <vpn policy name>

This command disables a VPN connection by specifying the name of the VPN policy.

Format	**vpn ipsec vpnpolicy disable** *<vpn policy name>*
Mode	vpn

Related show command: *show vpn ipsec vpnpolicy setup*

---

vpn ipsec vpnpolicy enable <vpn policy name>

This command enables a VPN connection by specifying the name of the VPN policy.

Format	**vpn ipsec vpnpolicy enable** *<vpn policy name>*
Mode	vpn

Related show command: *show vpn ipsec vpnpolicy setup*

---

vpn ipsec vpnpolicy connect <vpn policy name>

This command establishes a VPN connection by specifying the name of the VPN policy.

Format	**vpn ipsec vpnpolicy connect** *<vpn policy name>*
Mode	vpn

Related show commands: *show vpn ipsec vpnpolicy setup* and *show vpn ipsec vpnpolicy status*

---

vpn ipsec vpnpolicy drop <vpn policy name>

This command terminates an active VPN connection by specifying the name of the VPN policy.

Format	**vpn ipsec vpnpolicy drop** *<vpn policy name>*
Mode	vpn

Related show commands: *show vpn ipsec vpnpolicy setup* and *show vpn ipsec vpnpolicy status*

IPSec VPN Mode Config Commands

This section describes the following commands:

- *vpn ipsec mode_config configure <record name>*
- *vpn ipsec mode_config delete <record name>*

vpn ipsec mode_config configure <record name>

This command configures a Mode Config record. After you issue the **vpn ipsec mode_config configure** command to specify a record name, you enter the vpn-config [modeConfig] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1 **Format** **vpn ipsec mode_config configure** *<record name>*

Mode vpn

Step 2 **Format**

```
first_pool_start_ip <ipaddress>
first_pool_end_ip <ipaddress>
second_pool_start_ip <ipaddress>
second_pool_end_ip <ipaddress>
third_pool_start_ip <ipaddress>
third_pool_end_ip <ipaddress>
wins_server_primary_ip <ipaddress>
wins_server_secondary_ip <ipaddress>
dns_server_primary_ip <ipaddress>
dns_server_secondary_ip <ipaddress>

pfs_key_group {N | Y {dh_group {Group1_768_bit |
   Group2_1024_bit | Group5_1536_bit}}}
sa_lifetime_type {Seconds {sa_lifetime <seconds>} | KBytes
   {sa_lifetime <KBytes>})
encryption_algorithm {None | DES | 3DES | AES-128 |
   AES-192 | AES-256}
integrity_algorithm {MD5 | SHA-1}
local_ip <ipaddress>
local_subnet_mask <subnet mask>
```

Mode vpn-config [modeConfig]

Keyword	Associated Keyword to Select or Parameter to Type	Description
Client pool		
first_pool_start_ip	*ipaddress*	The start IP address for the first Mode Config pool.

Keyword	Associated Keyword to Select or Parameter to Type	Description
first_pool_end_ip	*ipaddress*	The end IP address for the first Mode Config pool.
second_pool_start_ip	*ipaddress*	The start IP address for the second Mode Config pool.
second_pool_end_ip	*ipaddress*	The end IP address for the second Mode Config pool.
third_pool_start_ip	*ipaddress*	The start IP address for the third Mode Config pool.
third_pool_end_ip	*ipaddress*	The end IP address for the third Mode Config pool.
wins_server_primary_ip	*ipaddress*	The IP address of the first WINS server.
wins_server_secondary_ip	*ipaddress*	The IP address of the second WINS server.
dns_server_primary_ip	*ipaddress*	The IP address of the first DNS server that is used by remote VPN clients.
dns_server_secondary_ip	*ipaddress*	The IP address of the second DNS server that is used by remote VPN clients.
Traffic tunnel security level		
pfs_key_group	**Y** or **N**	Enables or disables Perfect Forward Secrecy (PFS). If you enable PFS, you must issue the **dh_group** keyword to specify a group.
dh_group	**Group1_768_bit**, **Group2_1024_bit**, or **Group5_1536_bit**	Specifies the Diffie-Hellman (DH) group, which sets the strength of the algorithm in bits. The higher the group, the more secure the exchange.
sa_lifetime_type	**Seconds** or **KBytes**	Specifies whether the **sa_lifetime** keyword is set in seconds or Kbytes.
sa_lifetime	*seconds* or *number*	Depending on the setting of the **sa_lifetime_type** keyword, the SA lifetime in seconds or in KBytes.
encryption_algorithm	**None**, **DES**, **3DES**, **AES-128**, **AES-192**, or **AES-256**	Specifies the encryption algorithm, if any, to negotiate the security association (SA): • **None**. No encryption algorithm is enabled. • **DES**. Data Encryption Standard (DES). • **3DES**. Triple DES. • **AES-128**. Advanced Encryption Standard (AES) with a 128-bit key size. • **AES-192**. AES with a 192-bit key size. • **AES-256**. AES with a 256-bit key size.

Keyword	Associated Keyword to Select or Parameter to Type	Description
integrity_algorithm	**MD5** or **SHA-1**	Specifies the authentication (integrity) algorithm to negotiate the security association (SA): • **SHA-1**. Hash algorithm that produces a 160-bit digest. • **MD5**. Hash algorithm that produces a 128-bit digest.
local_ip	*ipaddress*	The local IPv4 address to which remote VPN clients have access. If you do not specify a local IP address, the wireless VPN firewall's default LAN IP address is used.
local_subnet_mask	*subnet mask*	The local subnet mask.

Command example:

```
FVS336Gv2> vpn ipsec mode_config configure EMEA Sales
vpn-config[modeConfig]> first_pool_start_ip 172.16.100.1
vpn-config[modeConfig]> first_pool_end_ip 172.16.100.99
vpn-config[modeConfig]> second_pool_start_ip 172.16.200.1
vpn-config[modeConfig]> second_pool_end_ip 172.16.200.99
vpn-config[modeConfig]> dns_server_primary_ip 192.168.1.1
vpn-config[modeConfig]> pfs_key_group Y
vpn-config[modeConfig]> dh_group Group2_1024_bit
vpn-config[modeConfig]> sa_lifetime_type Seconds
vpn-config[modeConfig]> sa_lifetime 3600
vpn-config[modeConfig]> encryption_algorithm 3DES
vpn-config[modeConfig]> integrity_algorithm SHA-1
vpn-config[modeConfig]> local_ip 192.168.1.0
vpn-config[modeConfig]> local_subnet_mask 255.255.255.0
vpn-config[modeConfig]> save
```

Related show command: *show vpn ipsec mode_config setup*

vpn ipsec mode_config delete <record name>

This command deletes a Mode Config record by specifying its record name.

Format	**vpn ipsec mode_config delete** *<record name>*
Mode	vpn

Related show command: *show vpn ipsec mode_config setup*

SSL VPN Wizard Command

This section describes the **vpn sslvpn wizard configure** command.

vpn sslvpn wizard configure

This command configures the SSL VPN wizard for a new SSL portal. After you issue the **vpn sslvpn wizard configure** command, you enter the vpn-config [sslvpn-wizard] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn ssl wizard configure**
	Mode	vpn
Step 2	**Format**	**portal_name** *<portal name>* **portal_title** *<portal title>* **banner_title** *<banner title>* **banner_message** *<message text>* **display_banner** {**Y** | **N**} **enable_httpmetatags** {**Y** | **N**} **enable_activex_web_cache_cleaner** {**Y** | **N**} **enable_vpntunnel** {**Y** | **N**} **enable_portforwarding** {**Y** | **N**} **domain_name** *<domain name>* **authentication_type** {**LocalUserDatabase** | **Radius-PAP**| **Radius-CHAP** | **Radius-MSCHAP** | **Radius-MSCHAPv2** | **WIKID-PAP** | **WIKID-CHAP** | **MIAS-PAP** | **MIAS-CHAP** | **NTDomain** | **ActiveDirectory** | **LDAP**} **authentication_server** *<ipaddress>* **authentication_secret** *<secret>* **workgroup** *<group name>* **ldap_base_dn** *<distinguished name>* **active_directory_domain** *<domain name>* **user_name** *<user name>* **password** *<password>* **confirm_password** *<password>* **idle_timeout** *<minutes>*

```
enable_full_tunnel {Y | N}
dns_suffix <suffix>
primary_dns <ipaddress>
secondary_dns <ipaddress>
begin_client_address <ipaddress>
end_client_address <ipaddress>
destination_network <ipaddress>
subnet_mask <subnet mask>

server_ip <ipaddress>
port <number>
host_server_ip <ipaddress>
host_domain_name <domain name>
```

Mode vpn-config [sslvpn-wizard]

Keyword	Associated Keyword to Select or Parameter to Type	Description
Portal Layout and Theme Name		
portal_name	*portal name*	The portal name (alphanumeric string).
portal_title	*portal title*	The portal title (alphanumeric string). Place text that consists of more than one word between quotes.
banner_title	*banner name*	The banner title (alphanumeric string). Place text that consists of more than one word between quotes.
banner_message	*message text*	The banner message (alphanumeric string). Place text that consists of more than one word between quotes.
display_banner	**Y** or **N**	Enables or disables display of the banner message.
enable_httpmetatags	**Y** or **N**	Enables or disables HTTP meta tags.
enable_activex_web_cache_cleaner	**Y** or **N**	Enables or disables the ActiveX web cache cleaner.
SSL VPN Portal Pages to Display		
enable_vpntunnel	**Y** or **N**	Enables or disables the VPN tunnel.
enable_portforwarding	**Y** or **N**	Enables or disables port forwarding.
Domain		
domain_name	*domain name*	The domain name (alphanumeric string).

Keyword	Associated Keyword to Select or Parameter to Type	Description
authentication_type	**LocalUserDatabase**, **Radius-PAP**, **Radius-CHAP**, **Radius-MSCHAP**, **Radius-MSCHAPv2**, **WIKID-PAP**, **WIKID-CHAP**, **MIAS-PAP**, **MIAS-CHAP**, **NTDomain**, **ActiveDirectory**, or **LDAP**	Specifies the authentication method that applies to the domain. Note the following: • For all selections with the exception of **LocalUserDatabase**, you must issue the **authentication_server** keyword and specify an IP address. • For all PAP and CHAP selections, you must issue the **authentication_secret** keyword and specify a secret. • For the **NTDomain** selection, you must issue the **workgroup** keyword and specify the workgroup. • For the **ActiveDirectory** selection, you must issue the **active_directory_domain** keyword and specify the Active Directory. • For the **LDAP** selection, you must issue the **ldap_base_dn** keyword and specify a DN.
authentication_server	*ipaddress*	The IP address of the authentication server.
authentication_secret	*secret*	The authentication secret (alphanumeric string).
workgroup	*group name*	The NT domain workgroup name (alphanumeric string).
ldap_base_dn	*distinguished name*	The LDAP base distinguished name (DN; alphanumeric string). Do not include spaces.
active_directory_domain	*domain name*	The Active Directory domain name (alphanumeric string).
User		
user_name	*user name*	The user name (alphanumeric string).
password	*password*	The password (alphanumeric string) that is assigned to the user. You must issue the **confirm_password** keyword and confirm the password.
confirm_password	*password*	The confirmation of the password.
idle_timeout	*minutes*	The idle time-out in minutes.

Keyword	Associated Keyword to Select or Parameter to Type	Description
Client IP Address Range and Route		
enable_full_tunnel	**Y** or **N**	Enables or disables full-tunnel support: • **Yes**. Enables full-tunnel support. • **No**. Disables full-tunnel support and enables split-tunnel support. If you enable split-tunnel support and you assign an entirely different subnet to the VPN tunnel clients from the subnet that is used by the local network, you must add a client route to ensure that a VPN tunnel client connects to the local network over the VPN tunnel. Issue the **destination_network** and **subnet_mask** keywords to specify the client route.
dns_suffix	*suffix*	The DNS suffix to be appended to incomplete DNS search strings. This setting is optional.
primary_dns	*ipaddress*	The IP address of the primary DNS server. This setting is optional. **Note:** If you do not assign a DNS server, the DNS settings remain unchanged in the VPN client after a VPN tunnel is established.
secondary_dns	*ipaddress*	The IP address of the secondary DNS server. This setting is optional.
begin_client_address	*ipaddress*	The start IP address of the IPv4 client range. The default address is 192.168.251.1.
end_client_address	*ipaddress*	The end IP address of the IPv4 client range. The default address is 192.168.251.254.
destination_network	*ipaddress*	If the **enable_full_tunnel** keyword is set to **N**, the network IP address for the client route.
subnet_mask	*subnet mask*	If the **enable_full_tunnel** keyword is set to **N**, the network subnet mask for the client route.
Port Forwarding		
server_ip	*ipaddress*	The IP address of the local server that hosts the application. **Note:** The IP address must be the same as the IP address that you assigned through the **host_server_ip** keyword for the same application.

Keyword	Associated Keyword to Select or Parameter to Type	Description
port	*number*	The TCP port number of the local server that hosts the application.
host_server_ip	*ipaddress*	The IP address of the local server that hosts the application. **Note:** The IP address must be the same as the IP address that you assigned through the **server_ip** keyword for the same application.
host_domain_name	*domain name*	The domain name for the local server that hosts the application.

Command example:

```
FVS336Gv2> vpn ssl wizard configure
vpn-config[sslvpn-wizard]> portal_name CSup
vpn-config[sslvpn-wizard]> portal_title “Customer Support”
vpn-config[sslvpn-wizard]> banner_title “Welcome to Customer Support”
vpn-config[sslvpn-wizard]> banner_message “In case of login difficulty,
                           call 123-456-7890.”
vpn-config[sslvpn-wizard]> display_banner Y
vpn-config[sslvpn-wizard]> enable_httpmetatags Y
vpn-config[sslvpn-wizard]> enable_activex_web_cache_cleaner Y
vpn-config[sslvpn-wizard]> enable_vpntunnel Y
vpn-config[sslvpn-wizard]> enable_portforwarding Y
vpn-config[sslvpn-wizard]> domain_name Headquarter
vpn-config[sslvpn-wizard]> authentication_type LDAP
vpn-config[sslvpn-wizard]> authentication_server 192.168.24.118
vpn-config[sslvpn-wizard]> ldap_base_dn dc=netgear,dc=com
vpn-config[sslvpn-wizard]> user_name PeterBrown
vpn-config[sslvpn-wizard]> password 3goTY5!Of6hh
vpn-config[sslvpn-wizard]> confirm_password 3goTY5!Of6hh
vpn-config[sslvpn-wizard]> idle_timeout 10
vpn-config[sslvpn-wizard]> enable_full_tunnel Y
vpn-config[sslvpn-wizard]> primary_dns 192.168.10.5
vpn-config[sslvpn-wizard]> secondary_dns 192.168.10.6
vpn-config[sslvpn-wizard]> begin_client_address 192.168.251.1
vpn-config[sslvpn-wizard]> end_client_address 192.168.251.254
vpn-config[sslvpn-wizard]> server_ip 192.168.51.227
vpn-config[sslvpn-wizard]> port 3389
vpn-config[sslvpn-wizard]> host_server_ip 192.168.51.227
vpn-config[sslvpn-wizard]> host_domain_name RemoteDesktop
vpn-config[sslvpn-wizard]> save
```

Related show commands: The following commands display information about the SSL portal that you can create with the **vpn ssl wizard configure** command:

- *show vpn sslvpn portal_layouts*
- *show vpn sslvpn users domains*
- *show vpn sslvpn users users*
- *show vpn sslvpn client*
- *show vpn sslvpn route*

- *show vpn sslvpn portforwarding appconfig*
- *show vpn sslvpn portforwarding hostconfig*

SSL VPN Portal Layout Commands

This section describes the following commands:

- *vpn sslvpn portal_layouts add*
- *vpn sslvpn portal_layouts edit <row id>*
- *vpn sslvpn portal_layouts delete <row id>*
- *vpn sslvpn portal_layouts set_default <row id>*

vpn sslvpn portal_layouts add

This command configures a new SSL VPN portal layout. After you issue the **vpn sslvpn portal_layouts add** command, you enter the vpn-config [portal-settings] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1

Format `vpn sslvpn portal_layouts add`

Mode vpn

Step 2

Format
```
portal_name <portal name>
portal_title <portal title>
banner_title <banner title>
banner_message <message text>
display_banner {Y | N}
enable_httpmetatags {Y | N}
enable_activex_web_cache_cleaner {Y | N}
enable_vpntunnel {Y | N}
enable_portforwarding {Y | N}
```

Mode vpn-config [portal-settings]

Keyword	Associated Keyword to Select or Parameter to Type	Description
portal_name	*portal name*	The portal name (alphanumeric string).
portal_title	*portal title*	The portal title (alphanumeric string). Place text that consists of more than one word between quotes.

Keyword	Associated Keyword to Select or Parameter to Type	Description
banner_title	*banner name*	The banner title (alphanumeric string). Place text that consists of more than one word between quotes.
banner_message	*message text*	The banner message (alphanumeric string). Place text that consists of more than one word between quotes.
display_banner	**Y** or **N**	Enables or disables display of the banner message.
enable_httpmetatags	**Y** or **N**	Enables or disables HTTP meta tags.
enable_activex_web_cache_cleaner	**Y** or **N**	Enables or disables the ActiveX web cache cleaner.
enable_vpntunnel	**Y** or **N**	Enables or disables the VPN tunnel.
enable_portforwarding	**Y** or **N**	Enables or disables port forwarding.

Command example:

```
FVS336Gv2> vpn sslvpn portal_layouts add
vpn-config[portal-settings]> portal_name CSup
vpn-config[portal-settings]> portal_title “Customer Support”
vpn-config[portal-settings]> banner_title “Welcome to Customer Support”
vpn-config[portal-settings]> banner_message “In case of login difficulty,
                             call 123-456-7890.”
vpn-config[portal-settings]> display_banner Y
vpn-config[portal-settings]> enable_httpmetatags Y
vpn-config[portal-settings]> enable_activex_web_cache_cleaner Y
vpn-config[portal-settings]> enable_vpntunnel Y
vpn-config[portal-settings]> save
```

Related show command: *show vpn sslvpn portal_layouts*

vpn sslvpn portal_layouts edit <row id>

This command configures an existing SSL VPN portal layout. After you issue the **vpn sslvpn portal_layouts edit** command to specify the row to be edited, you enter the vpn-config [portal-settings] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. You cannot change the name of the portal layout.

Step 1	**Format**	**vpn sslvpn portal_layouts edit** *<row id>*
	Mode	vpn

Step 2 **Format**

```
portal_title <portal title>
banner_title <banner title>
banner_message <message text>
display_banner {Y | N}
enable_httpmetatags {Y | N}
enable_activex_web_cache_cleaner {Y | N}
enable_vpntunnel {Y | N}
enable_portforwarding {Y | N}
```

Mode vpn-config [portal-settings]

Keyword	Associated Keyword to Select or Parameter to Type	Description
portal_title	*portal title*	The portal title (alphanumeric string). Place text that consists of more than one word between quotes.
banner_title	*banner name*	The banner title (alphanumeric string). Place text that consists of more than one word between quotes.
banner_message	*message text*	The banner message (alphanumeric string). Place text that consists of more than one word between quotes.
display_banner	**Y** or **N**	Enables or disables display of the banner message.
enable_httpmetatags	**Y** or **N**	Enables or disables HTTP meta tags.
enable_activex_web_cache_cleaner	**Y** or **N**	Enables or disables the ActiveX web cache cleaner.
enable_vpntunnel	**Y** or **N**	Enables or disables the VPN tunnel.
enable_portforwarding	**Y** or **N**	Enables or disables port forwarding.

Related show command: *show vpn sslvpn portal_layouts*

vpn sslvpn portal_layouts delete <row id>

This command deletes an SSL VPN portal layout by specifying its row ID.

Format	**vpn sslvpn portal_layouts delete** *<row id>*
Mode	vpn

Related show command: *show vpn sslvpn portal_layouts*

---

vpn sslvpn portal_layouts set_default <row id>

This command configures an SSL VPN portal as the default portal by specifying its row ID.

Format	**vpn sslvpn portal_layouts set_default** *<row id>*
Mode	vpn

Related show command: *show vpn sslvpn portal_layouts*

SSL VPN Authentication Domain Commands

This section describes the following commands:

- *vpn sslvpn users domains add*
- *vpn sslvpn users domains edit <row id>*
- *vpn sslvpn users domains delete <row id>*
- *vpn sslvpn users domains disable_Local_Authentication {Y | N}*

vpn sslvpn users domains add

This command configures a new authentication domain that is not limited to SSL VPN users. After you issue the **vpn sslvpn users domains add** command, you enter the vpn-config [user-domains] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn sslvpn users domains add**
	Mode	vpn

Step 2 **Format** **domain_name** *<domain name>*
portal *<portal name>*
authentication_type {**LocalUserDatabase** | **Radius-PAP** | **Radius-CHAP** | **Radius-MSCHAP** | **Radius-MSCHAPv2** | **WIKID-PAP** | **WIKID-CHAP** | **MIAS-PAP** | **MIAS-CHAP** | **NTDomain** | **ActiveDirectory** | **LDAP**}
authentication_server1 *<ipaddress>*
authentication_secret *<secret>*
workgroup *<group name>*
ldap_base_dn *<distinguished name>*
active_directory_domain *<domain name>*

Mode vpn-config [user-domains]

Keyword	Associated Keyword to Select or Parameter to Type	Description
domain_name	*domain name*	The domain name (alphanumeric string).
portal	*portal name*	The portal name (alphanumeric string). **Note:** For information about how to configure a portal, see *SSL VPN Portal Layout Commands*.
authentication_type	**LocalUserDatabase**, **Radius-PAP**, **Radius-CHAP**, **Radius-MSCHAP**, **Radius-MSCHAPv2**, **WIKID-PAP**, **WIKID-CHAP**, **MIAS-PAP**, **MIAS-CHAP**, **NTDomain**, **ActiveDirectory**, or **LDAP**	Specifies the authentication method that applies to the domain. Note the following: • For all selections with the exception of **LocalUserDatabase**, you must issue the **authentication_server1** keyword and specify an IP address. • For all PAP and CHAP selections, you must issue the **authentication_secret** keyword and specify a secret. • For the **NTDomain** selection, you must issue the **workgroup** keyword and specify the workgroup. • For the **ActiveDirectory** selection, you must issue the **active_directory_domain** keyword and specify the Active Directory. • For the **LDAP** selection, you must issue the **ldap_base_dn** keyword and specify a DN.
authentication_server1	*ipaddress*	The IP address of the authentication server.
authentication_secret	*secret*	The authentication secret (alphanumeric string).
workgroup	*group name*	The NT domain workgroup name (alphanumeric string).

Keyword	Associated Keyword to Select or Parameter to Type	Description
ldap_base_dn	*distinguished name*	The LDAP base distinguished name (DN; alphanumeric string). Do not include spaces.
active_directory_domain	*domain name*	The Active Directory domain name (alphanumeric string).

Command example:

```
FVS336Gv2> vpn sslvpn users domains add
vpn-config[user-domains]> domain_name Headquarter
vpn-config[user-domains]> portal CSup
vpn-config[user-domains]> authentication_type LDAP
vpn-config[user-domains]> authentication_server1 192.168.24.118
vpn-config[user-domains]> ldap_base_dn dc=netgear,dc=com
vpn-config[user-domains]> save
```

Related show command: *show vpn sslvpn users domains*

vpn sslvpn users domains edit <row id>

This command configures an existing authentication domain that is not limited to SSL VPN users. After you issue the **vpn sslvpn users domains edit** command to specify the row to be edited, you enter the vpn-config [user-domains] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. You cannot change the name of the domain and the type of authentication.

Step 1	**Format**	**vpn sslvpn users domains edit** *<row id>*
	Mode	vpn
Step 2	**Format**	**portal** *<portal name>* **authentication_server1** *<ipaddress>* **authentication_secret** *<secret>* **workgroup** *<group name>* **ldap_base_dn** *<distinguished name>* **active_directory_domain** *<domain name>*
	Mode	vpn-config [user-domains]

Keyword	Associated Parameter to Type	Description
portal	*portal name*	The portal name (alphanumeric string). **Note:** For information about how to configure a portal, see *SSL VPN Portal Layout Commands*.
authentication_server1	*ipaddress*	The IP address of the authentication server.

Keyword	Associated Parameter to Type	Description
authentication_secret	*secret*	The authentication secret (alphanumeric string).
workgroup	*group name*	The NT domain workgroup name (alphanumeric string).
ldap_base_dn	*distinguished name*	The LDAP base distinguished name (DN; alphanumeric string). Do not include spaces.
active_directory_domain	*domain name*	The Active Directory domain name (alphanumeric string).

Related show command: *show vpn sslvpn users domains*

vpn sslvpn users domains delete <row id>

This command deletes an SSL VPN authentication domain by specifying its row ID.

Format	**vpn sslvpn users domains delete** *<row id>*
Mode	vpn

Related show command: *show vpn sslvpn users domains*

vpn sslvpn users domains disable_Local_Authentication {Y | N}

This command enables or disables local authentication of users globally by specifying **Y** (local authentication is disabled) or **N** (local authentication is enabled).

Format	**vpn sslvpn users domains disable_Local_Authentication {Y | N}**
Mode	vpn

Related show command: *show vpn sslvpn users domains*

SSL VPN Authentication Group Commands

This section describes the following commands:

- *vpn sslvpn users groups add*
- *vpn sslvpn users groups edit <row id>*
- *vpn sslvpn users groups delete <row id>*

vpn sslvpn users groups add

This command configures a new authentication group that is not limited to SSL VPN users. After you issue the **vpn sslvpn users groups add** command, you enter the vpn-config [user-groups] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn sslvpn users groups add**
	Mode	vpn
Step 2	**Format**	**domain_name** *<domain name>* **group_name** *<group name>* **idle_timeout** *<minutes>*
	Mode	vpn-config [user-groups]

Keyword	Associated Parameter to Type	Description
domain_name	*domain name*	The domain name (alphanumeric string) to which the group belongs. **Note:** For information about configuring domains, see *SSL VPN Authentication Domain Commands*.
group_name	*group name*	The group name (alphanumeric string).
idle_timeout	*minutes*	The idle time-out in minutes.

Command example:

```
FVS336Gv2> vpn sslvpn users groups add
vpn-config[user-groups]> domain_name Headquarter
vpn-config[user-groups]> group_name Sales
vpn-config[user-groups]> idle_timeout 15
vpn-config[user-groups]> save
```

Related show command: *show vpn sslvpn users groups*

vpn sslvpn users groups edit <row id>

This command configures an existing authentication group that is not limited to SSL VPN users. After you issue the **vpn sslvpn users groups edit** command to specify the row to be edited, you enter the vpn-config [user-groups] mode and then you can change the idle time-out only.

Step 1	**Format**	**vpn sslvpn users groups edit** *<row id>*
	Mode	vpn
Step 2	**Format**	**idle_timeout** *<minutes>*
	Mode	vpn-config [user-groups]

Keyword	Associated Parameter to Type	Description
idle_timeout	*minutes*	The idle time-out in minutes.

Related show command: *show vpn sslvpn users groups*

---

vpn sslvpn users groups delete <row id>

This command deletes an authentication group by specifying its row ID.

Format	**vpn sslvpn users groups delete** *<row id>*
Mode	vpn

Related show command: *show vpn sslvpn users groups*

SSL VPN User Commands

This section describes the following commands:

- *vpn sslvpn users users add*
- *vpn sslvpn users users edit <row id>*
- *vpn sslvpn users users delete <row id>*
- *vpn sslvpn users users login_policies <row id>*
- *vpn sslvpn users users ip_policies configure <row id>*
- *vpn sslvpn users users ip_policies delete <row id>*
- *vpn sslvpn users users browser_policies <row id>*

vpn sslvpn users users add

This command configures a new user account. The command is not limited to SSL VPN users. After you issue the **vpn sslvpn users users add** command, you enter the vpn-config [users] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn sslvpn users users add**
	Mode	vpn
Step 2	**Format**	**user_name** *<user name>* **user_type** {**SSLVPNUser** | **Administrator** | **Guest** | **IPSECVPNUser** | **L2TPUser** | **PPTPUser**} **group** *<group name>* **password** *<password>* **confirm_password** *<password>* **idle_timeout** *<minutes>*
	Mode	vpn-config [users]

Keyword	Associated Keyword to Select or Parameter to Type	Description
user_name	*user name*	The user name (alphanumeric string).
user_type	**SSLVPNUser**, **Administrator**, **Guest**, **IPSECVPNUser**, **L2TPUser**, or **PPTPUser**	Specifies the user type.
group	*group name*	The group name (alphanumeric string) to which the user belongs. **Note:** For information about how to configure groups, see *SSL VPN Authentication Group Commands*.
password	*password*	The password (alphanumeric string) that is assigned to the user. You must issue the **confirm_password** keyword and confirm the password.
confirm_password	*password*	The confirmation of the password.
idle_timeout	*minutes*	The idle time-out in minutes.

Command example:

```
FVS336Gv2> vpn sslvpn users users add
vpn-config[users]> user_name PeterBrown
vpn-config[users]> user_type SSLVPNUser
vpn-config[users]> group Sales
vpn-config[users]> password 3goTY5!Of6hh
vpn-config[users]> confirm_password 3goTY5!Of6hh
vpn-config[users]> idle_timeout 10
vpn-config[users]> save
```

Related show command: *show vpn sslvpn users users*

vpn sslvpn users users edit <row id>

This command configures an existing user account. The command is not limited to SSL VPN users. After you issue the **vpn sslvpn users users edit** command to specify the row to be edited, you enter the vpn-config [users] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. You cannot change the name of the user or the group to which the user is assigned. The changes you can make to the user type are restricted.

Step 1	**Format**	**vpn sslvpn users users edit** *<row id>*
	Mode	vpn
Step 2	**Format**	**user_type** {**SSLVPNUser** | **Administrator** | **Guest** | **IPSECVPNUser** | **L2TPUser** | **PPTPUser**} **password** *<password>* **confirm_password** *<password>* **idle_timeout** *<minutes>*
	Mode	vpn-config [users]

Keyword	Associated Keyword to Select or Parameter to Type	Description
user_type	**SSLVPNUser**, **Administrator**, **Guest**, **IPSECVPNUser**, **L2TPUser**, or **PPTPUser**	Specifies the user type. **Note:** You cannot change an existing user from the **L2TPUser** or **PPTPUser** user type to another type or from another type to the **L2TPUser** or **PPTPUser** type.
password	*password*	The password (alphanumeric string) that is assigned to the user. You must issue the **confirm_password** keyword and confirm the password.
confirm_password	*password*	The confirmation of the password.
idle_timeout	*minutes*	The idle time-out in minutes.

Related show command: *show vpn sslvpn users users*

vpn sslvpn users users delete <row id>

This command deletes a user account by specifying its row ID.

Format	**vpn sslvpn users users delete** *<row id>*
Mode	vpn

Related show command: *show vpn sslvpn users users*

vpn sslvpn users users login_policies <row id>

This command configures the login policy for a user. The command is not limited to SSL VPN users. After you issue the **vpn sslvpn users users login_policies** command to specify the row ID that represents the user, you enter the vpn-config [user-login-policy] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn sslvpn users users login_policies** *<row id>*
	Mode	vpn
Step 2	**Format**	**deny_login_from_wan_interface** {**Y** | **N**} **disable_login** {**Y** | **N**}
	Mode	vpn-config [user-login-policy]

Keyword	Associated Keyword to Select	Description
deny_login_from_wan_interface	**Y** or **N**	Allows or blocks login from the WAN interface.
disable_login	**Y** or **N**	Allows or blocks login from any interface.

Command example:

```
FVS336Gv2> vpn sslvpn users users login_policies 4
vpn-config[user-login-policy]> deny_login_from_wan_interface N
vpn-config[user-login-policy]> disable_login N
vpn-config[user-login-policy]> save
```

Related show commands: *show vpn sslvpn users users* and *show vpn sslvpn users login_policies <row id>*

vpn sslvpn users users ip_policies configure <row id>

This command configures source IP addresses from which a user is either allowed or denied access. The command is not limited to SSL VPN users. After you issue the **vpn sslvpn users users ip_policies configure** command to specify the row ID that represents the user, you enter the vpn-config [user-ip-policy] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn sslvpn users users ip_policies configure** *<row id>*
	Mode	vpn

Step 2 **Format**

```
allow_login_from_defined_addresses {Y | N}
ip_version {IPv4 | IPv6}
source_address_type {IPAddress {{source_address <ipaddress>} |
   {source_address6 <ipv6-address>}} | IPNetwork
   {{source_address <ipaddress>} {mask_length <mask length>} |
   {source_address6 <ipv6-address>} {prefix_length
   <prefix length>}}}
```

Mode vpn-config [user-ip-policy]

Keyword	Associated Keyword to Select or Parameter to Type	Description
allow_login_from_defined_addresses	**Y** or **N**	Allows or denies login from a single-source IP address or network IP addresses.
ip_version	**IPv4** or **IPv6**	Specifies the IP version of the source IP address: • **IPv4**. The IP address or network address is defined by an IPv4 address. You must issue the **source_address** keyword and specify an IPv4 address. For a network address, you also must issue the **mask_length** keyword and specify a subnet mask length. • **IPv6**. The IP address or network address is defined by an IPv6 address. You must issue the **source_address6** keyword and specify an IPv6 address. For a network address, you also must issue the **prefix_length** keyword and specify a prefix length.
source_address_type	**IPAddress** or **IPNetwork**	Specifies the source address type: • **IPAddress**. A single IP address. The setting of the **ip_version** keyword determines whether you must issue the **source_address** keyword and specify an IPv4 address or issue the **source_address6** keyword and specify an IPv6 address. • **IPNetwork**. A subnet of IP addresses. The setting of the **ip_version** keyword determines whether you must issue the **mask_length** keyword and specify an IPv4 subnet mask or issue the **prefix_length** keyword and specify an IPv6 prefix length.
source_address	*ipaddress*	The IPv4 IP address or network address if the **ip_version** keyword is set to **IPv4**.

Keyword	Associated Keyword to Select or Parameter to Type	Description
mask_length	*mask length*	If the **source_address_type** keyword is set to **IPNetwork** and the **ip_version** keyword is set to **IPv4**, the mask length of the IPv4 network.
source_address6	*ipv6-address*	The IPv6 IP address or network address if the **ip_version** keyword is set to **IPv6**.
prefix_length	*prefix length*	If the **source_address_type** keyword is set to **IPNetwork** and the **ip_version** keyword is set to **IPv6**, the prefix length of the IPv6 network.

Command example:

```
FVS336Gv2> vpn sslvpn users users ip_policies configure 4
vpn-config[user-ip-policy]> allow_login_from_defined_addresses Y
vpn-config[user-ip-policy]> ip_version IPv4
vpn-config[user-ip-policy]> source_address_type IPAddress
vpn-config[user-ip-policy]> source_address 10.156.127.39
vpn-config[user-ip-policy]> save
```

Related show commands: *show vpn sslvpn users users* and *show vpn sslvpn users ip_policies <row id>*

vpn sslvpn users users ip_policies delete <row id>

This command deletes a source IP address for a user by specifying the row ID of the table.

Format	**vpn sslvpn users ip_policies delete** *<row id>*
Mode	vpn

Related show commands: *show vpn sslvpn users users* and *show vpn sslvpn users ip_policies <row id>*

vpn sslvpn users users browser_policies <row id>

This command configures a client browser from which a user is either allowed or denied access. The command is not limited to SSL VPN users. After you issue the **vpn sslvpn users users browser_policies** command to specify the row ID that represents the user, you enter the vpn-config [user-browser-policy] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn sslvpn users users browser_policies** *<row id>*
	Mode	vpn

Step 2	**Format**	**add browser** {**InternetExplorer** | **NetscapeNavigator** | **Opera** | **Firefox** | **Mozilla**} **delete_browser** {**InternetExplorer** | **NetscapeNavigator** | **Opera** | **Firefox** **Mozilla**} **enable_or_disable_login_from_defined_browsers** {**Y** | **N**}
	Mode	vpn-config [user-browser-policy]

Keyword	Associated Keyword to Select	Description
add_browser	**InternetExplorer**, **NetscapeNavigator**, **Opera**, **Firefox**, or **Mozilla**	Adds a browser to the browser list. **Note:** By default, the browser list is empty.
delete_browser	**InternetExplorer**, **NetscapeNavigator**, **Opera**, **Firefox**, or **Mozilla**	Removes a browser from the browser list.
enable_or_disable_login_from_defined_browsers	**Y** or **N**	Specifies whether access through the browsers on the browser list is allowed or denied: • **Yes**. Allows access through the browsers on the browser list. • **No**. Denies access through the browsers on the browser list.

Command example:

```
FVS336Gv2> vpn sslvpn users users browser_policies 4
vpn-config[user-browser-policy]> add_browser NetscapeNavigator
vpn-config[user-browser-policy]> enable_or_disable_login_from_defined_browsers N
vpn-config[user-browser-policy]> save
vpn-config[user-browser-policy]> add_browser InternetExplorer
vpn-config[user-browser-policy]> enable_or_disable_login_from_defined_browsers N
vpn-config[user-browser-policy]> save
```

Related show commands: *show vpn sslvpn users users* and *show vpn sslvpn users browser_policies <row id>*

SSL VPN Port Forwarding Commands

This section describes the following commands:

- *vpn sslvpn portforwarding appconfig add*
- *vpn sslvpn portforwarding appconfig delete <row id>*
- *vpn sslvpn portforwarding hostconfig add*
- *vpn sslvpn portforwarding hostconfig delete <row id>*

vpn sslvpn portforwarding appconfig add

This command configures a new SSL port forwarding application. After you issue the **vpn sslvpn portforwarding appconfig add** command, you enter the vpn-config [portforwarding-settings] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn sslvpn portforwarding appconfig add**
	Mode	vpn
Step 2	**Format**	**server_ip** *<ipaddress>* **port** *<number>*
	Mode	vpn-config [portforwarding-settings]

Keyword	Associated Parameter to Type	Description
server_ip	*ipaddress*	The IP address of the local server that hosts the application.
port	*number*	The TCP port number of the local server that hosts the application.

Command example:

```
FVS336Gv2> vpn sslvpn portforwarding appconfig add
vpn-config[portforwarding-settings]> server_ip 192.168.51.227
vpn-config[portforwarding-settings]> port 3389
vpn-config[portforwarding-settings]> save
```

Related show command: *show vpn sslvpn portforwarding appconfig*

vpn sslvpn portforwarding appconfig delete <row id>

This command deletes an SSL port forwarding application by specifying its row ID.

Format	**vpn sslvpn portforwarding appconfig delete** *<row id>*
Mode	vpn

Related show command: *show vpn sslvpn portforwarding appconfig*

vpn sslvpn portforwarding hostconfig add

This command configures a new host name for an SSL port forwarding application. After you issue the **vpn sslvpn portforwarding hostconfig add** command, you enter the vpn-config [portforwarding-host-settings] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn sslvpn portforwarding hostconfig add**
	Mode	vpn
Step 2	**Format**	**server_ip** *<ipaddress>* **domain_name** *<domain name>*
	Mode	vpn-config [portforwarding-host-settings]

Keyword	Associated Parameter to Type	Description
server_ip	*ipaddress*	The IP address of the local server that hosts the application. **Note:** The IP address must be the same as the IP address that you assigned through the *vpn sslvpn portforwarding appconfig add* command for the same application.
domain_name	*domain name*	The domain name for the local server that hosts the application.

Command example:

```
FVS336Gv2> vpn sslvpn portforwarding hostconfig add
vpn-config[portforwarding-host-settings]> server_ip 192.168.51.227
vpn-config[portforwarding-host-settings]> domain_name RemoteDesktop
vpn-config[portforwarding-host-settings]> save
```

Related show command: *show vpn sslvpn portforwarding hostconfig*

vpn sslvpn portforwarding hostconfig delete <row id>

This command deletes a host name for an SSL port forwarding application by specifying the row ID of the host name.

Format	**vpn sslvpn portforwarding hostconfig delete** *<row id>*
Mode	vpn

Related show command: *show vpn sslvpn portforwarding hostconfig*

SSL VPN Client and Client Route Commands

This section describes the following commands:

- *vpn sslvpn client ipv4*
- *vpn sslvpn client ipv6*
- *vpn sslvpn route add*
- *vpn sslvpn route delete <row id>*

vpn sslvpn client ipv4

This command configures the SSL client IP address range. After you issue the **vpn sslvpn client ipv4** command, you enter the vpn-config [sslvpn-client-ipv4-settings] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn sslvpn client ipv4**
	Mode	vpn
Step 2	**Format**	**enable_full_tunnel** {**Y** | **N**} **dns_suffix** <*suffix*> **primary_dns** <*ipaddress*> **secondary_dns** <*ipaddress*> **begin_client_address** <*ipaddress*> **end_client_address** <*ipaddress*>
	Mode	vpn-config [sslvpn-client-ipv4-settings]

Keyword	Associated Keyword to Select or Parameter to Type	Description
enable_full_tunnel	**Y** or **N**	Enables or disables full-tunnel support: • **Yes**. Enables full-tunnel support. • **No**. Disables full-tunnel support and enables split-tunnel support. If you enable split-tunnel support and you assign an entirely different subnet to the VPN tunnel clients from the subnet that is used by the local network, you must add a client route to ensure that a VPN tunnel client connects to the local network over the VPN tunnel (see the *vpn sslvpn route add* command).
dns_suffix	*suffix*	The DNS suffix to be appended to incomplete DNS search strings. This setting is optional.
primary_dns	*ipaddress*	The IP address of the primary DNS server. This setting is optional. **Note:** If you do not assign a DNS server, the DNS settings remain unchanged in the VPN client after a VPN tunnel is established.

Keyword	Associated Keyword to Select or Parameter to Type	Description
secondary_dns	*ipaddress*	The IP address of the secondary DNS server. This setting is optional.
begin_client_address	*ipaddress*	The start IP address of the IPv4 client range. The default address is 192.168.251.1.
end_client_address	*ipaddress*	The end IP address of the IPv4 client range. The default address is 192.168.251.254.

Command example:

```
FVS336Gv2> vpn sslvpn client ipv4
vpn-config[sslvpn-client-ipv4-settings]> enable_full_tunnel Y
vpn-config[sslvpn-client-ipv4-settings]> primary_dns 192.168.10.5
vpn-config[sslvpn-client-ipv4-settings]> secondary_dns 192.168.10.6
vpn-config[sslvpn-client-ipv4-settings]> begin_client_address 192.168.251.1
vpn-config[sslvpn-client-ipv4-settings]> end_client_address 192.168.251.254
vpn-config[sslvpn-client-ipv4-settings]> save
```

Related show command: *show vpn sslvpn client*

vpn sslvpn client ipv6

This command configures the SSL client IP address range. After you issue the **vpn sslvpn client ipv6** command, you enter the vpn-config [sslvpn-client-ipv6-settings] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn sslvpn client ipv6**
	Mode	vpn
Step 2	**Format**	**enable_full_tunnel** {**Y** | **N**} **begin_client_address** <*ipv6-address*> **end_client_address** <*ipv6-address*>
	Mode	vpn-config [sslvpn-client-ipv6-settings]

Keyword	Associated Keyword to Select or Parameter to Type	Description
enable_full_tunnel	**Y** or **N**	Enables or disables full-tunnel support: • **Yes**. Enables full-tunnel support. • **No**. Disables full-tunnel support and enables split-tunnel support. If you enable split-tunnel support and you assign an entirely different subnet to the VPN tunnel clients from the subnet that is used by the local network, you must add a client route to ensure that a VPN tunnel client connects to the local network over the VPN tunnel (see the *vpn sslvpn route add* command).
begin_client_address	*ipv6-address*	The start IP address of the IPv6 client range. The default address is 4000::1.
end_client_address	*ipv6-address*	The end IP address of the IPv6 client range. The default address is 4000::200.

Command example:

```
FVS336Gv2> vpn sslvpn client ipv6
vpn-config[sslvpn-client-ipv6-settings]> enable_full_tunnel N
vpn-config[sslvpn-client-ipv6-settings]> begin_client_address 4000::1000:2
vpn-config[sslvpn-client-ipv6-settings]> end_client_address 4000::1000:50
vpn-config[sslvpn-client-ipv6-settings]> save
```

Related show command: *show vpn sslvpn client*

vpn sslvpn route add

This command configures a static client route to a destination network. After you issue the **vpn sslvpn route add** command, you enter the vpn-config [sslvpn-route-settings] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Note: When full-tunnel support is enabled, client routes are not operable. For client routes to be operable, enable split-tunnel support.

Step 1	**Format**	**vpn sslvpn route add**
	Mode	vpn
Step 2	**Format**	**ip_version** {**IPv4** {**destination_network** <*ipaddress*>} {**subnet_mask** <*subnet mask*>} | **IPv6** {**destination_network6** <*ipv6-address*>} {**prefix_length** <*prefix length*>}}
	Mode	vpn-config [sslvpn-route-settings]

Keyword	Associated Parameter to Type	Description
ip_version	**IPv4** or **IPv6**	Specifies the IP version of the destination network for the route: • **IPv4**. The network address is an IPv4 address. You must issue the **destination_network** and **subnet_mask** keywords and specify an IPv4 address and subnet mask. • **IPv6**. The network address is an IPv6 address. You must issue the **destination_network6** and **prefix_length** keywords and specify an IPv6 address and prefix length.
destination_network	*ipaddress*	If the **ip_version** keyword is set to **IPv4**, the IPv4 address of the destination network for the route.
subnet_mask	*subnet mask*	If the **ip_version** keyword is set to **IPv4**, the subnet mask of the destination network for the route.
destination_network6	*ipv6-address*	If the **ip_version** keyword is set to **IPv6**, the IPv6 address of the destination network for the route.
prefix_length	*prefix length*	If the **ip_version** keyword is set to **IPv6**, the prefix length of the destination network for the route.

Command example:

```
FVS336Gv2> vpn sslvpn route add
vpn-config[sslvpn-route-settings]> ip_version IPv4
vpn-config[sslvpn-route-settings]> destination_network 192.168.4.20
vpn-config[sslvpn-route-settings]> subnet_mask 255.255.255.254
vpn-config[sslvpn-route-settings]> save
```

Related show command: *show vpn sslvpn route*

vpn sslvpn route delete <row id>

This command deletes a client route by specifying its row ID.

Format	**vpn sslvpn route delete** *<row id>*
Mode	vpn

Related show command: *show vpn sslvpn route*

SSL VPN Resource Commands

This section describes the following commands:

- *vpn sslvpn resource add*
- *vpn sslvpn resource delete <row id>*
- *vpn sslvpn resource configure add <resource name>*
- *vpn sslvpn resource configure delete <row id>*

vpn sslvpn resource add

This command adds a new resource. After you issue the **vpn sslvpn resource add** command, you enter the vpn-config [sslvpn-resource-settings] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn sslvpn resource add**
	Mode	vpn
Step 2	**Format**	**resource_name** *<resource name>* **service_type** {**VPNTunnel** | **PortForwarding** | **All**}
	Mode	vpn-config [sslvpn-resource-settings]

Keyword	Associated Keyword to Select or Parameter to Type	Description
resource_name	*resource name*	The resource name (alphanumeric string).
service_type	**VPNTunnel**, **PortForwarding**, or **All**	Specifies the type of service to which the resource applies: • **VPNTunnel**. The resource applies only to a VPN tunnel. • **PortForwarding**. The resource applies only to port forwarding. • **All**. The resource applies both to a VPN tunnel and to port forwarding.

Command example:

```
FVS336Gv2> vpn sslvpn resource add
vpn-config[sslvpn-resource-settings]> resource_name TopSecure
vpn-config[sslvpn-resource-settings]> service_type PortForwarding
vpn-config[sslvpn-resource-settings]> save
```

Related show command: *show vpn sslvpn resource*

vpn sslvpn resource delete <row id>

This command deletes a resource by specifying its row ID.

Format	**vpn sslvpn resource delete** *<row id>*
Mode	vpn

Related show command: *show vpn sslvpn resource*

---

vpn sslvpn resource configure add <resource name>

This command configures a resource object. (You first must add a resource with the *vpn sslvpn resource add* command.) After you issue the **vpn sslvpn resource configure add** command to specify the resource name, you enter the vpn-config [sslvpn-resource-settings] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1

Format **vpn sslvpn resource configure add** *<resource name>*

Mode vpn

Step 2

Format **object_type** {**IPAddress** | **IPNetwork**}

For a single IP address:

ip_version {**IPv4** {**object_address** *<ipaddress>*} | **IPv6** {**object_address6** *<ipv6-address>*}}
start_port *<port number>*
end_port *<port number>*

For an IP network:

ip_version {**IPv4** {**object_address** *<ipaddress>*} {**mask_length** *<subnet mask length>*} | **IPv6** {**object_address6** *<ipv6-address>*} {**mask_length** <prefix length>}}
start_port *<port number>*
end_port *<port number>*

Mode vpn-config [sslvpn-resource-settings]

Keyword	Associated Keyword to Select or Parameter to Type	Description
object_type	**IPAddress** or **IPNetwork**	Specifies the source address type for the object: • **IPAddress**. A single IP address. The setting of the **ip_version** keyword determines whether you must issue the **object_address** keyword and specify an IPv4 address or the **object_address6** keyword and specify an IPv6 address. • **IPNetwork**. A subnet of IP addresses. The setting of the **ip_version** keyword determines whether you must issue the **object_address** and **mask_length** keywords and specify an IPv4 network address and mask length or issue the **object_address6** and **mask_length** keywords and specify an IPv6 network address and prefix length.
ip_version	**IPv4** or **IPv6**	Specifies the IP version of the IP address or IP network: • **IPv4**. The IP address or IP network is defined by an IPv4 address. You must issue the **object_address** keyword and specify an IPv4 address. For a network address, you also must issue the **mask_length** keyword and specify a subnet mask length. • **IPv6**. The IP address or network address is defined by an IPv6 address. You must issue the **object_address6** keyword and specify an IPv6 address. For a network address, you also must issue the **mask_length** keyword and specify a prefix length.
object_address	*ipaddress*	The IPv4 address, if the policy is for an IPv4 address or IPv4 network.
object_address6	*ipv6-address*	The IPv6 address, if the policy is for an IPv6 address or IPv6 network.
mask_length	*subnet mask length* or *prefix length*	The nature of this keyword and parameter depends on the setting of the **ip_version** and **object_type** keywords: • If the **ip_version** keyword is set to **IPv4** and the **object_type** keyword is set to **IPNetwork**, the subnet mask length of the IPv4 network. • If the **ip_version** keyword is set to **IPv6** and the **object_type** keyword is set to **IPNetwork**, the prefix length of the IPv6 network.
start_port	*number*	The start port number for the port range that applies to the object.
end_port	*number*	The end port number for the port range that applies to the object.

Command example:

```
FVS336Gv2> add TopSecure
vpn-config[sslvpn-resource-settings]> object_type IPNetwork
vpn-config[sslvpn-resource-settings]> ip_version IPv4
vpn-config[sslvpn-resource-settings]> object_address 192.168.30.56
vpn-config[sslvpn-resource-settings]> mask_length 24
vpn-config[sslvpn-resource-settings]> start_port 3391
vpn-config[sslvpn-resource-settings]> end_port 3393
vpn-config[sslvpn-resource-settings]> save
```

Related show command: *show vpn sslvpn resource_object <resource name>*

---

vpn sslvpn resource configure delete <row id>

This command deletes a resource object by specifying its row ID. To delete the resource itself, use the *vpn sslvpn resource delete <row id>* command.

Format	**vpn sslvpn resource configure delete** *<row id>*
Mode	vpn

Related show command: *show vpn sslvpn resource_object <resource name>*

SSL VPN Policy Commands

This section describes the following commands:

- *vpn sslvpn policy add*
- *vpn sslvpn policy edit <row id>*
- *vpn sslvpn policy delete <row id>*

vpn sslvpn policy add

This command configures a new SSL VPN policy. After you issue the **vpn sslvpn policy add** command, you enter the vpn-config [sslvpn-policy-settings] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn sslvpn policy add**
	Mode	vpn

Step 2 **Format** **policy_name** <*policy name*>
policy_type {**Global** | **Group** {**policy_owner** <*group name*>} | **User** {**policy_owner** <*user name*>}}
destination_object_type {**NetworkResource** | **IPAddress** | **IPNetwork** | **All**}

In addition to a policy name, policy type, and destination object type, configure the following for a network resource:

ip_version {**IPv4** | **IPv6**}
resource_name <*resource name*>
policy_permission {**Permit** | **Deny**}

In addition to a policy name, policy type, and destination object type, configure the following for an IP address:

ip_version {**IPv4** {**policy_address** <*ipaddress*>} | **IPv6** {**policy_address6** <*ipv6-address*>}}
start_port <*port number*>
end_port <*port number*>
service_type {**VPNTunnel** | **PortForwarding** | **All**}
policy_permission {**Permit** | **Deny**}

In addition to a policy name, policy type, and destination object type, configure the following for an IP network:

ip_version {**IPv4** {**policy_address** <*ipaddress*>} {**policy_mask_length** <*subnet mask*>} | **IPv6** {**policy_address6** <*ipv6-address*>} {**policy_ipv6_prefix_length** <*prefix length*>}}
start_port <*port number*>
end_port <*port number*>
service_type {**VPNTunnel** | **PortForwarding** | **All**}
policy_permission {**Permit** | **Deny**}

In addition to a policy name, policy type, and destination object type, configure the following for all addresses (that is, the **destination_object_type** keyword is set to **All**):

ip_version {**IPv4** | **IPv6**}
start_port <*port number*>
end_port <*port number*>
service_type {**VPNTunnel** | **PortForwarding** | **All**}
policy_permission {**Permit** | **Deny**}

Mode vpn-config [sslvpn-policy-settings]

Keyword	Associated Keyword to Select or Parameter to Type	Description
policy_name	*policy name*	The policy name (alphanumeric string).
policy_type	**Global**, **Group**, or **User**	Specifies the SSL VPN policy type: • **Global**. The policy is global and includes all groups and users. • **Group**. The policy is limited to a single group. For information about how to create groups, see *SSL VPN Authentication Group Commands*. You must issue the **policy_owner** keyword and specify the group name. • **User**. The policy is limited to a single user. For information about how to create user accounts, see *SSL VPN User Commands*. You must issue the **policy_owner** keyword and specify the user name.
policy_owner	*group name* or *user name*	Specifies the owner of the policy. The owner depends on the setting of the **policy_type** keyword: • **Group**. Specify the group name to which the policy applies. • **User**. Specify the user name to which the policy applies.
destination_object_type	**NetworkResource**, **IPAddress**, **IPNetwork**, or **All**	Specifies the policy destination type, which determines how the policy is applied, and, in turn, which keywords you must issue to specify the policy: • **NetworkResource**. The policy applies to an existing IPv4 or IPv6 resource. For information about how to create and configure network resources, see *SSL VPN Resource Commands*. You must issue the following keywords and their associated parameters and keywords: - **policy_name** - **ip_version** - **resource_name** - **policy_permission** - **policy_owner** if the **policy_type** keyword is set to **Group** or **User**.

Keyword	Associated Keyword to Select or Parameter to Type	Description
destination_object_type (continued)	**NetworkResource**, **IPAddress**, **IPNetwork**, or **All** (continued)	• **IPAddress**. The policy applies to a single IPv4 or IPv6 address. You must issue the following keywords and their associated parameters and keywords: - **policy_name** - **ip_version** - **policy_address** or **policy_address6** (depending on the setting of the **ip_version** keyword) - **start_port** and **end_port** - **service_type** - **policy_permission** - **policy_owner** if the **policy_type** keyword is set to **Group** or **User**. • **IPNetwork**. The policy applies to an IPv4 or IPv6 network address. You must issue the following keywords and their associated parameters and keywords: - **policy_name** - **ip_version** - **policy_address** and **policy_mask_length** or **policy_address6** and **policy_ipv6_prefix_length** (depending on the setting of the **ip_version** keyword) - **start_port** and **end_port** - **service_type** - **policy_permission** - **policy_owner** if the **policy_type** keyword is set to **Group** or **User**. • **All**. The policy applies to all addresses. You must issue the following keywords and their associated parameters and keywords: - **policy_name** - **ip_version** - **start_port** and **end_port** - **service_type** - **policy_permission** - **policy_owner** if the **policy_type** keyword is set to **Group** or **User**.
resource_name	*resource name*	The name of a resource that you configured with the *vpn sslvpn resource add* command. This keyword and parameter apply only if the policy is for a network resource.

Keyword	Associated Keyword to Select or Parameter to Type	Description
policy_permission	**Permit** or **Deny**	Specifies whether the policy permits or denies access.
ip_version	**IPv4** or **IPv6**	Specifies the IP version that applies to the policy: • **IPv4**. The policy is for an IPv4 network resource, IPv4 address, IPv4 network, or all IPv4 addresses. For an IP address or IP network, you must issue the **policy_address** keyword and specify an IPv4 address. For a network address, you also must issue the **policy_mask_length** keyword and specify a subnet mask. • **IPv6**. The policy is for an IPv6 network resource, IPv6 address, IPv6 network, or all IPv6 addresses. For an IP address or IP network, you must issue the **policy_address6** keyword and specify an IPv6 address. For a network address, you also must issue the **policy_ipv6_prefix_length** keyword and specify a prefix length.
policy_address	*ipaddress*	The IPv4 address, if the policy is for an IPv4 address or IPv4 network.
policy_mask_length	*subnet mask*	The subnet mask, if the policy is for an IPv4 network.
policy_address6	*ipv6-address*	The IPv6 address, if the policy is for an IPv6 address or IPv6 network.
policy_ipv6_prefix_length	*prefix length*	The prefix length, if the policy is for an IPv6 network.
start_port	*port number*	The start port number for a policy port range. (This does not apply if the policy is for a network resource.)
end_port	*port number*	The end port number for a policy port range. (This does not apply if the policy is for a network resource.)
service_type	**VPNTunnel**, **PortForwarding**, or **All**	Specifies the service type for the policy: • **VPNTunnel**. The policy applies only to a VPN tunnel. • **PortForwarding**. The policy applies only to port forwarding. • **All**. The policy applies both to a VPN tunnel and to port forwarding.

Command example:

```
FVS336Gv2> vpn sslvpn policy add
vpn-config[sslvpn-policy-settings]> policy_name RoadWarriorPolicy
vpn-config[sslvpn-policy-settings]> ip_version IPv4
vpn-config[sslvpn-policy-settings]> policy_type Global
vpn-config[sslvpn-policy-settings]> destination_object_type NetworkResource
vpn-config[sslvpn-policy-settings]> resource_name RoadWarrior
vpn-config[sslvpn-policy-settings]> policy_permission Permit
vpn-config[sslvpn-policy-settings]> save
vpn-config[sslvpn-policy-settings]> policy_name GuestFTPPolicy
vpn-config[sslvpn-policy-settings]> ip_version IPv4
vpn-config[sslvpn-policy-settings]> policy_type User
vpn-config[sslvpn-policy-settings]> policy_owner guest
vpn-config[sslvpn-policy-settings]> destination_object_type All
vpn-config[sslvpn-policy-settings]> start_port 25077
vpn-config[sslvpn-policy-settings]> end_port 25078
vpn-config[sslvpn-policy-settings]> service_type PortForwarding
vpn-config[sslvpn-policy-settings]> policy_permission Deny
vpn-config[sslvpn-policy-settings]> save
```

Related show command: *show vpn sslvpn policy*

---

vpn sslvpn policy edit <row id>

This command configures an existing SSL VPN policy. After you issue the **vpn sslvpn policy edit** command to specify the row to be edited (for row information, see the output of the *show vpn sslvpn policy* command), you enter the vpn-config [sslvpn-policy-settings] mode. You can then configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. You cannot change the policy type, policy owner, destination object, IP version, or service type.

Step 1	**Format**	**vpn sslvpn policy edit** *<row id>*
	Mode	vpn
Step 2	**Format**	**policy_name** *<policy name>*

In addition to the policy name, you can change the following for a network resource:

resource_name *<resource name>*
policy_permission {**Permit** | **Deny**}

In addition to the policy name, you can change the following for an IP address:

{{**policy_address** *<ipaddress>*} | {**policy_address6** *<ipv6-address>*}}
start_port *<port number>*
end_port *<port number>*
policy_permission {**Permit** | **Deny**}

In addition to the policy name, you can change the following for an IP network:

```
{{policy_address <ipaddress>} {policy_mask_length
   <subnet mask>} | {policy_address6 <ipv6-address>}
   {policy_ipv6_prefix_length <prefix length>}}
start_port <port number>
end_port <port number>
policy_permission {Permit | Deny}
```

In addition to the policy name, you can change the following for all addresses (that is, the **destination_object_type** keyword is set to **All**):

```
start_port <port number>
end_port <port number>
policy_permission {Permit | Deny}
```

Mode vpn-config [sslvpn-policy-settings]

Keyword	Associated Keyword to Select or Parameter to Type	Description
policy_name	*policy name*	The policy name (alphanumeric string).
policy_address	*ipaddress*	The IPv4 address, if the policy is for an IPv4 address or IPv4 network.
policy_mask_length	*subnet mask*	The subnet mask, if the policy is for an IPv4 network.
policy_address6	*ipv6-address*	The IPv6 address, if the policy is for an IPv6 address or IPv6 network.
policy_ipv6_prefix_length	*prefix length*	The prefix length, if the policy is for an IPv6 network.
start_port	*port number*	The start port number for a policy port range. (This does not apply if the policy is for a network resource.)
end_port	*port number*	The end port number for a policy port range. (This does not apply if the policy is for a network resource.)
resource_name	*resource name*	The name of a resource that you configured with the *vpn sslvpn resource add* command. This keyword and parameter apply only if the policy is for a network resource.
policy_permission	**Permit** or **Deny**	Specifies whether the policy permits or denies access.

Command example:

```
FVS336Gv2> vpn sslvpn policy edit 2
vpn-config[sslvpn-policy-settings]> policy_name RoadWarriorPolicyIII
vpn-config[sslvpn-policy-settings]> start_port 35406
```

```
vpn-config[sslvpn-policy-settings]> end_port 35408
vpn-config[sslvpn-policy-settings]> policy_permission Permit
vpn-config[sslvpn-policy-settings]> save
```

Related show command: *show vpn sslvpn policy*

---

vpn sslvpn policy delete <row id>

This command deletes an SSL VPN policy by specifying its row ID.

Format	**vpn sslvpn policy delete** *<row id>*
Mode	vpn

Related show command: *show vpn sslvpn policy*

RADIUS Server Command

This section describes the **vpn ipsec radius configure** command.

vpn ipsec radius configure

This command configures a RADIUS server. After you issue the **vpn ipsec radius configure** command, you enter the vpn-config [radius-config] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn ipsec radius configure**
	Mode	vpn
Step 2	**Format**	**enable** {**Y** | **N**} **radius-server** *<ipaddress>* **secret** *<secret>* **nas_identifier** *<identifier>* **backup_server_enable** {**Y** | **N**} **backup-radius_server** *<ipaddress>* **backup_server_secret** *<secret>* **backup_server_nas_identifier** *<identifier>* **timeout** *<seconds>* **retries** *<number>*
	Mode	vpn-config [radius-config]

Keyword	Associated Keyword to Select or Parameter to Type	Description
Primary RADIUS server		
enable	**Y** or **N**	Enables or disables the primary RADIUS server.
radius-server	*ipaddress*	The IPv4 address of the primary RADIUS server.
secret	*secret*	The secret phrase (alphanumeric string) for the primary RADIUS server.
nas_identifier	*identifier*	The NAS ID for the primary RADIUS server.
Backup RADIUS server		
backup_server_enable	**Y** or **N**	Enables or disables the backup RADIUS server.
backup_radius_server	*ipaddress*	The IPv4 address of the backup RADIUS server.
backup_server_secret	*secret*	The secret phrase (alphanumeric string) for the backup RADIUS server.
backup_server_nas_identifier	*identifier*	The NAS ID for the backup RADIUS server.
Connection configuration		
timeout	*seconds*	The connection time-out in seconds for the RADIUS server.
retries	*number*	The number of connection retry attempts for the RADIUS server.

Command example:

```
FVS336Gv2> vpn ipsec radius configure
vpn-config[radius-config]> enable Y
vpn-config[radius-config]> radius-server 192.168.4.2
vpn-config[radius-config]> secret Hlo0ole1H12aaq43
vpn-config[radius-config]> nas_identifier FVS336Gv2-Bld3
vpn-config[radius-config]> backup_server_enable Y
vpn-config[radius-config]> backup_radius-server 192.168.4.3
vpn-config[radius-config]> backup_server_secret Hduo0oplH54bqX91
vpn-config[radius-config]> backup_server_nas_identifier FVS336Gv2-Bld3
vpn-config[radius-config]> timeout 30
vpn-config[radius-config]> retries 4
vpn-config[radius-config]> save
```

Related show command: *show vpn ipsec radius [ipaddress]*

PPTP Server Command

This section describes the **vpn pptp server configure** command.

vpn pptp server configure

This command configures the PPTP server. After you issue the **vpn pptp server configure** command, you enter the vpn-config [pptp-config] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1

Format `vpn pptp server configure`

Mode vpn

Step 2

Format

```
enable {Y | N}
start_address <ipaddress>
end_address <ipaddress>
idle_timeout <minutes>

{Authentication CHAP {Y | N} | Authentication MSCHAP {Y | N} |
   Authentication MSCHAPv2 {Y | N} | Authentication PAP {Y | N}}

{Encryption MPPE_128 {Y | N} | Encryption MPPE_40 {Y | N} |
   Encryption MPPE_stateful {Y | N})
```

Mode vpn-config [pptp-config]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
PPTP server configuration		
enable	**Y** or **N**	Enables or disables the PPTP server.
start_address	*ipaddress*	The start IPv4 address of the PPTP server range.
end_address	*ipaddress*	The end IPv4 address of the PPTP server range.
idle_timeout	*minutes*	The idle time-out after which the connection is terminated.
Authentication		
Authentication CHAP	**Y** or **N**	The PPTP server uses RADIUS-Challenge Handshake Authentication Protocol (CHAP).
Authentication MSCHAP	**Y** or **N**	The PPTP server uses RADIUS-Microsoft CHAP (MSCHAP).

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
Authentication MSCHAPv2	**Y** or **N**	The PPTP server uses RADIUS-Microsoft CHAP version 2 (MSCHAPv2).
Authentication PAP	**Y** or **N**	The PPTP server uses RADIUS-Password Authentication Protocol (PAP).
Encryption		
Encryption MPPE_128	**Y** or **N**	The PPTP server uses MPPE 128-bit encryption. **Note:** This encryption mode is supported only if the authentication is MSCHAP or MSCHAPv2.
Encryption MPPE_40	**Y** or **N**	The PPTP server uses MPPE 40-bit encryption. **Note:** This encryption mode is supported only if the authentication is MSCHAP or MSCHAPv2.
Encryption MPPE_stateful	**Y** or **N**	The PPTP server uses Stateful MPPE encryption. **Note:** This encryption mode is supported only if the authentication is MSCHAP or MSCHAPv2.

Command example:

```
FVS336Gv2> vpn pptp server configure
vpn-config[pptp-config]> enable Y
vpn-config[pptp-config]> start_address 192.168.112.1
vpn-config[pptp-config]> end_address 192.168.112.25
vpn-config[pptp-config]> idle_timeout 10
vpn-config[pptp-config]> Authentication MSCHAPv2
vpn-config[pptp-config]> Encryption MPPE_128
vpn-config[pptp-config]> save
```

Related show commands: *show vpn pptp server setup* and *show vpn pptp server connections*

L2TP Server Command

This section describes the **vpn l2tp server configure** command.

vpn l2tp server configure

This command configures the L2TP server. After you issue the **vpn l2tp server configure** command, you enter the vpn-config [l2tp-config] mode and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer.

Step 1	**Format**	**vpn l2tp server configure**
	Mode	vpn
Step 2	**Format**	**enable** {**Y** | **N**} **start_address** *<ipaddress>* **end_address** *<ipaddress>* **idle_timeout** *<minutes>*
	Mode	vpn-config [l2tp-config]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
L2TP server configuration		
enable	**Y** or **N**	Enables or disables the L2TP server.
start_address	*ipaddress*	The start IPv4 address of the L2TP server range.
end_address	*ipaddress*	The end IPv4 address of the L2TP server range.
idle_timeout	*minutes*	The idle time-out after which the connection is terminated.
Authentication		
Authentication CHAP	**Y** or **N**	The L2TP server uses RADIUS-Challenge Handshake Authentication Protocol (CHAP).
Authentication MSCHAP	**Y** or **N**	The L2TP server uses RADIUS-Microsoft CHAP (MSCHAP).
Authentication MSCHAPv2	**Y** or **N**	The L2TP server uses RADIUS-Microsoft CHAP version 2 (MSCHAPv2).
Authentication PAP	**Y** or **N**	The L2TP server uses RADIUS-Password Authentication Protocol (PAP).

Command example:

```
FVS336Gv2> vpn l2tp server configure
vpn-config[l2tp-config]> enable Y
vpn-config[l2tp-config]> start_address 192.168.112.1
vpn-config[l2tp-config]> end_address 192.168.112.25
vpn-config[l2tp-config]> idle_timeout 10
vpn-config[l2tp-config]> Authentication PAP Y
vpn-config[l2tp-config]> save
```

Related show commands: *show vpn l2tp server setup* and *show vpn l2tp server connections*

7. Overview of the Show Commands

This chapter provides an overview of all show commands for the four configuration command modes. The chapter includes the following sections:

- *Network Settings Show Commands*
- *Security Settings Show Commands*
- *Administrative and Monitoring Settings Show Commands*
- *VPN Settings Show Commands*

Network Settings Show Commands

Enter the **show net ?** command at the CLI prompt to display the submodes in the show net mode. The following table lists the submodes and their commands in alphabetical order:

Table 12. Show commands: show net mode

Submode	Command Name	Purpose
ddns	*show net ddns setup*	Display the Dynamic DNS configuration.
dmz	*show net dmz ipv4 setup*	Display the IPv4 DMZ configuration.
	show net dmz ipv6 setup	Display the IPv6 DMZ configuration.
ethernet	*show net ethernet*	Display the MAC address and VLAN status for a single or all Ethernet interfaces.
ipv6	*show net ipv6 ipmode setup*	Display the IPv6 routing mode configuration.
ipv6_tunnel	*show net ipv6_tunnel setup*	Display the IPv6 tunnel configuration.
	show net ipv6_tunnel status	Display the status of the IPv6 tunnels.
lan	*show net lan available_lan_hosts list*	Display the IPv4 hosts.
	show net lan dhcp leased_clients list	Display the LAN clients that received a leased DHCP IP address.
	show net lan dhcp logs	Display the LAN DHCP log.
	show net lan dhcp reserved_ip setup	Display information about the DHCP clients, including the assigned (reserved) IP addresses.
	show net lan ipv4 advanced setup	Display the advanced IPv4 LAN configuration.
	show net lan ipv4 detailed setup <vlan id>	Display the detailed configuration for a VLAN.
	show net lan ipv4 multiHoming	Display the LAN secondary IPv4 addresses.
	show net lan ipv4 setup	Display the IPv4 LAN configuration.
	show net lan ipv4 traffic_meter detailed_setup <row id>	Display the detailed traffic meter information for a specified IP address.
	show net lan ipv4 traffic_meter setup	Display the LAN traffic meter configuration.
	show net lan ipv6 multiHoming	Display the LAN secondary IPv6 addresses.
	show net lan ipv6 setup	Display the IPv6 LAN configuration.
	show net lan lan_groups	Display the LAN groups.
protocol binding	*show net protocol_binding setup*	Display the protocol bindings.
qos	*show net qos setup*	Display the WAN QoS configuration.
radvd	*show net radvd dmz setup*	Display the DMZ RADVD configuration.
	show net radvd lan setup	Display the LAN RADVD configuration.

Table 12. Show commands: show net mode (continued)

Submode	Command Name	Purpose
routing	*show net routing dynamic setup*	Display the dynamic routing configuration.
	show net routing static ipv4 setup	Display the IPv4 static routes configuration.
	show net routing static ipv6 setup	Display the IPv6 static routes configuration.
siit	*show net siit setup*	Displays the status of the Stateless IP/ICMP Translation.
statistics	*show net statistics*	Display the network statistics for a single or all Ethernet interfaces.
wan	*show net wan port_setup ipv4 <wan interface>*	Display the configuration for an IPv4 WAN interface.
	show net wan port_setup ipv6 <wan interface>	Display the configuration for an IPv6 WAN interface.
	show net wan wan ipv4 secondary_addresses <wan interface>	Display the secondary IPv4 addresses for a WAN interface.
	show net wan wan ipv4 setup <wan interface>	Display the IPv4 configuration for a WAN interface.
	show net wan wan ipv4 status <wan interface>	Display the IPv4 connection status for a WAN interface.
	show net wan wan ipv6 setup <wan interface>	Display the IPv6 configuration for a WAN interface.
	show net wan wan ipv6 status <wan interface>	Display the IPv6 connection status for a WAN interface.
wan_settings	*show net wan_settings wanmode*	Display the IPv4 WAN routing mode.

Security Settings Show Commands

Enter the **show security ?** command at the CLI prompt to display the submodes in the show security mode. The following table lists the submodes and their commands in alphabetical order:

Table 13. Show commands: show security mode

Submode	Command Name	Purpose
address_filter	*show security address_filter enable_email_log*	Display the configuration of the IP/MAC binding log.
	show security address_filter ip_or_mac_binding setup	Display the IPv4 and IPv6 MAC bindings.
	show security address_filter mac_filter setup	Display the MAC addresses for source MAC filtering.
bandwidth	*show security bandwidth profile setup*	Display the configured bandwidth profiles.
content_filter	*show security content_filter block_group*	Display the groups for which content filtering is enabled.
	show security content_filter blocked_keywords	Display the keywords that are blocked.
	show security content_filter content_filtering	Display the status of content filtering and the web components.
	show security content_filter trusted_domains	Display the trusted domains.
firewall	*show security firewall advanced algs*	Display whether or not SIP ALG is enabled.
	show security firewall attack_checks igmp	Display whether or not the IGMP proxy is enabled.
	show security firewall attack_checks setup ipv4	Display which WAN and LAN security checks are enabled for IPv4.
	show security firewall attack_checks setup ipv6	Display which WAN and LAN security checks are enabled for IPv6.
	show security firewall attack_checks vpn_passthrough setup	Display which VPN pass-through features are enabled.
	show security firewall igmp allowed_networks	Display the alternate networks from which the VPN firewall can accept multicast traffic.
	show security firewall ipv4 setup dmz_wan	Display the IPv4 DMZ WAN firewall rules.
	show security firewall ipv4 setup lan_dmz	Display the IPv4 LAN DMZ firewall rules.
	show security firewall ipv4 setup lan_wan	Display the IPv4 LAN WAN firewall rules.
	show security firewall ipv6 setup	Display all IPv6 firewall rules.

Table 13. Show commands: show security mode (continued)

Submode	Command Name	Purpose
firewall (continued)	*show security firewall session_limit*	Display the session limit settings.
	show security firewall session_settings	Display the session time-out settings.
porttriggering_rules	*show security porttriggering_rules setup*	Display the port triggering rules.
	show security porttriggering_rules status	Display the port triggering status.
schedules	*show security schedules setup*	Display the configured schedules.
services	*show security services ip_group ip_setup*	Display the configured IP groups.
	show security services qos_profile setup	Display the configured QoS profiles.
	show security services service_group setup	Display the configured service groups.
	show security services setup	Display the configured custom services.
upnp	*show security upnp portmap*	Display the UPnP portmap table.
	show security upnp setup	Display the UPnP configuration.

Administrative and Monitoring Settings Show Commands

Enter the **`show system ?`** command at the CLI prompt to display the submodes in the show system mode. The following table lists the submodes and their commands in alphabetical order:

Table 14. Show commands: show system mode

Submode	Command Name	Purpose
Not applicable	*show sysinfo*	Display system information, including MAC addresses, serial number, and firmware version.
dns_logs	*show system dns_logs*	Display the DNS logs.
firmware_version	*show system firmware_version*	Display the firmware version.
logging	*show system logging remote setup*	Display the configuration and the schedule of the email logs.
	show system logging setup	Display the configuration of the IPv4 and IPv6 logs.
logs	*show system logs*	Display the system logs.
remote_management	*show system remote_management setup*	Display the configuration of remote management for Telnet and HTTPS access.
schedule_reboot	*show system schedule_reboot*	Display whether a system reboot is scheduled and at what time it is scheduled.

Table 14. Show commands: show system mode (continued)

Submode	Command Name	Purpose
snmp	*show system snmp remote_snmp status*	Displays whether SNMP access over a WAN interface is enabled.
	show system snmp snmpv3_users	Display the SNMPv3 user configuration.
	show system snmp sys	Display the SNMP system configuration of the SNMP agent and the SNMP system information of the wireless VPN firewall.
	show system snmp trap [agent ipaddress]	Display the SNMP trap configuration of the SNMP agent.
	show system snmp trap_events	Displays which SNMP trap events are enabled.
status	*show system status*	Display the system status information.
time	*show system time setup*	Display the time configuration and the configuration of the NTP server.
traffic_meter	*show system traffic_meter setup <wan interface>*	Display the configuration of the traffic meter and the Internet traffic statistics.

VPN Settings Show Commands

Enter the **show vpn ?** command at the CLI prompt to display the submodes in the show vpn mode. The following table lists the submodes and their commands in alphabetical order:

Table 15. Show commands: show vpn mode

Submode	Command Name	Purpose
ipsec	*show vpn ipsec ikepolicy setup*	Display the IKE policies.
	show vpn ipsec logs	Display the IPSec VPN logs.
	show vpn ipsec mode_config setup	Display the Mode Config records.
	show vpn ipsec radius [ipaddress]	Display the configuration of all or a specific RADIUS server.
	show vpn ipsec vpnpolicy setup	Display the IPSec VPN policies.
	show vpn ipsec vpnpolicy status	Display status information about the active and nonactive IPSec VPN policies.
l2tp	*show vpn l2tp server connections*	Display the users that are connected through the L2TP server.
	show vpn l2tp server setup	Display the configuration of the PPTP server.

Table 15. Show commands: show vpn mode (continued)

Submode	Command Name	Purpose
pptp	*show vpn pptp server connections*	Display the users that are connected through the PPTP server.
	show vpn pptp server setup	Display the configuration of the L2TP server.
sslvpn	*show vpn sslvpn client*	Display the SSL VPN client range and configuration.
	show vpn sslvpn logs	Display the SSL VPN logs.
	show vpn sslvpn policy	Display the SSL VPN policies.
	show vpn sslvpn portal_layouts	Display the SSL VPN portal layout.
	show vpn sslvpn portforwarding appconfig	Display the SSL VPN port forwarding application configuration.
	show vpn sslvpn portforwarding hostconfig	Display the SSL VPN port forwarding host configuration.
	show vpn sslvpn resource	Display the SSL VPN resource configuration.
	show vpn sslvpn resource_object <resource name>	Display the detailed configuration for a specific resource object.
	show vpn sslvpn route	Display the SSL VPN client routes.
	show vpn sslvpn users active_users	Display the active SSL VPN users.
	show vpn sslvpn users browser_policies <row id>	Display the login restrictions based on web browsers for a specific user.
	show vpn sslvpn users domains	Display the domain configurations.
	show vpn sslvpn users groups	Display the group configurations.
	show vpn sslvpn users ip_policies <row id>	Display the login restrictions based on IP addresses for a specific user.
	show vpn sslvpn users login_policies <row id>	Display the login restrictions based on login policies for a specific user.
	show vpn sslvpn users users	Display the user account configurations.

Show Commands

8

This chapter explains the show commands and associated parameters for the four configuration command modes. The chapter includes the following sections:

- *Network Settings Show Commands*
- *Security Settings Show Commands*
- *Administrative and Monitoring Settings Show Commands*
- *VPN Settings Show Commands*

Network Settings Show Commands

This section contains the following subsections:

- *WAN IPv4 and WAN IPv6 Show Commands*
- *IPv6 Mode, IPv6 Tunnel, and SIIT Show Commands*
- *LAN DHCP Show Commands*
- *Dynamic DNS Show Command*
- *IPv4 LAN Show Commands*
- *IPv6 LAN Show Commands*
- *DMZ Show Commands*
- *Routing Show Commands*
- *Network Statistics Show Command*

WAN IPv4 and WAN IPv6 Show Commands

This section describes the following commands:

- *show net wan_settings wanmode*
- *show net wan port_setup ipv4 <wan interface>*
- *show net wan port_setup ipv6 <wan interface>*
- *show net wan wan ipv4 setup <wan interface>*
- *show net wan wan ipv4 status <wan interface>*
- *show net wan wan ipv4 secondary_addresses <wan interface>*
- *show net wan wan ipv6 setup <wan interface>*
- *show net wan wan ipv6 status <wan interface>*
- *show net protocol_binding setup*
- *show net qos setup*

show net wan_settings wanmode

This command displays the IPv4 WAN routing mode:

```
Routing Mode between WAN and LAN

_____________________________________

NAT is Enabled
```

show net wan port_setup ipv4 <wan interface>

This command displays the configuration of an IPv4 WAN port. For the WAN interface, type **WAN1** or **WAN2**.

```
WAN1 Port Setup

_______________
```

```
MTU Type:       Default
Port Speed:     Auto Sense

WAN MODE Setup

_____________
WAN Mode: Primary Wan Mode Using WAN1
Auto Rollover: Auto Rollover is Disabled
WAN Failure Detection Method: WAN DNS Servers
Retry Interval: 30
Failover After: 4

Router's MAC Address for WAN1

_____________________________
MAC Address Type: This MAC Address
MAC Address: 00:00:00:00:11:22

Upload/Download Settings for WAN1

_____________________________________
WAN Connection Type: DSL
WAN Connection Speed Upload Type: Custom
WAN Connection Speed Upload: 1500
WAN Connection Speed Download Type: 1 Gbps
WAN Connection Speed Download: 1000000
```

show net wan port_setup ipv6 <wan interface>

This command displays the failure detection ping settings of an IPv6 WAN port. For the WAN interface, type **WAN1** or **WAN2**.

```
WAN1 Port Setup

_______________

PING IP: fec1::1
Retry Interval: 30
Failover After: 4
```

show net wan wan ipv4 setup <wan interface>

This command displays the IPv4 configuration for a WAN interface. For the WAN interface, type **WAN1** or **WAN2**.

```
Broadband Setup

_______________

STATIC Configuration:
Internet (IP) Address Source: Use Static IP Address
IP Address: 10.139.54.228
```

```
IP Subnet Mask: 255.255.255.248
Gateway IP Address: 10.139.54.225
Domain Name Servers (DNS) Source: Use these DNS Servers
Primary DNS Server: 10.80.130.23
Secondary DNS Server: 10.80.130.24
```

show net wan wan ipv4 status <wan interface>

This command displays the IPv4 WAN connection status. For the WAN interface, type **WAN1** or **WAN2**.

```
WAN1 Status
_____________

WAN1 Status (Ipv4):
MAC Address: AA:AB:BB:00:00:02
IPv4 Address: 10.139.54.228 / 255.255.255.248
Wan State: UP
NAT (IPv4 only): Enabled
IPv4 Connection Type: STATIC
IPv4 Connection State: Connected
Link State: LINK UP
WAN Mode: Use only single WAN portWAN1
Gateway: 10.139.54.225
Primary DNS: 10.80.130.23
Secondary DNS: 8.8.8.8
```

show net wan wan ipv4 secondary_addresses <wan interface>

This command displays the secondary IPv4 addresses for a WAN interface. For the WAN interface, type **WAN1** or **WAN2**.

```
WAN2 Secondary Addresses
_________________________

List of Secondary WAN addresses
_____________________________________
Row Id: 1
IP Address: 10.168.50.1
Subnet Mask: 255.255.255.0
```

show net wan wan ipv6 setup <wan interface>

This command displays the IPv6 WAN configuration. For the WAN interface, type **WAN1** or **WAN2**.

```
IPv6 WAN1 Setup
_______________

Dynamic IPv6 (DHCP) Configuration:
Stateless Address Auto Configuration: Enabled
Prefix Delegation: Disabled
```

show net wan wan ipv6 status <wan interface>

This command displays the IPv6 WAN1 connection status. For the WAN interface, type **WAN1** or **WAN2**.

```
IPv6 WAN1 Status
________________

IPv6 Connection Type: Dynamic IPv6 (DHCP)
IPv6 Connection State: Connected
IPv6 Address: fe80::a8ab:bbff:fe00:2
IPv6 Prefix Length: 64
Default IPv6 Gateway:
Primary DNS Server:
Secondary DNS Server:
```

show net protocol_binding setup

This command displays the protocol bindings:

```
List of Protocol Bindings
_________________________

ROW ID State   Service Local Gateway Source Network Destination Network
______ _______ _______ _____________ ______________ ___________________
1      Enabled FTP     WAN1          Any            10.122.178.214
2      Enabled PPTP    WAN2          Any            Any
```

show net qos setup

This command displays the WAN QoS configuration:

```
Quality of Service
_____________________

Enabled: Yes
QoS Type: Rate Control

List of Network QoS Profiles
_____________________________________
ROW ID QoS Type     Interface Name ServiceName Direction       Rate         Hosts
______ ____________ ______________ ___________ _____________ ____________ ___________________________________
1      Rate Control WAN2           HTTP        Inbound         7500 - 15000 192.168.110.2 - 192.168.110.199
2      Priority     WAN1           RTSP:TCP    Inbound Traffic High         -
```

IPv6 Mode, IPv6 Tunnel, and SIIT Show Commands

This section describes the following commands:

- *show net ipv6 ipmode setup*
- *show net ipv6_tunnel setup*
- *show net ipv6_tunnel status*
- *show net siit setup*

show net ipv6 ipmode setup

This command displays the IPv6 routing mode configuration:

```
IP MODE
________
IPv4 only mode : Disabled
IPv4/IPv6 mode : Enabled
```

show net ipv6_tunnel setup

This command displays the IPv6 tunnel configuration:

```
IPv6 Tunnels
_____________
6 to 4 Tunneling

Automatic Tunneling is Enabled

List of Available ISATAP Tunnels
```

```
ROW ID LocalEndpoint ISATAP Subnet Prefix
______ _____________ ____________________
1      192.168.1.1   FE80:2006::
2      10.29.33.4    2004::
```

show net ipv6_tunnel status

This command displays the status of the IPv6 tunnels:

```
Tunnel Name     IPv6 Address(es)
___________     ________________________________________________
sit0-WAN1       2002:408b:36e2::408b:36e2/64, ::127.0.0.1/96, ::176.16.2.1/96, ::192.168.1.1/96,
                ::192.168.20.1/96, ::192.168.70.1/96, ::64.139.54.226/96
isatap1-LAN     fe80::5efe:c0a8:101/64
isatap2-LAN     ::10.29.33.4/128, fe80::5efe:a1d:2104/64
```

show net siit setup

This command displays the status of the Stateless IP/ICMP Translation (SIIT):

```
SIIT Configuration
__________________
Status          enabled
IPv4 Address    192.168.5.117
```

LAN DHCP Show Commands

This section describes the following commands:

- *show net lan dhcp leased_clients list*
- *show net lan dhcp logs*
- *show net lan dhcp reserved_ip setup*

show net lan dhcp leased_clients list

This command displays the LAN clients that received a leased DHCP IP address:

```
List of Available DHCP Leased Clients
_____________________________________
```

show net lan dhcp logs

This command displays the LAN DHCP log:

```
Jul 10 10:23:50 FVS336Gv2 local7.info dhcpd: Wrote 0 deleted host decls to leases file.
Jul 10 10:23:50 FVS336Gv2 local7.info dhcpd: Wrote 0 new dynamic host decls to leases
file.
Jul 10 10:23:50 FVS336Gv2 local7.info dhcpd: Wrote 0 leases to leases file.
```

```
Jul 10 10:23:51 FVS336Gv2 local7.info dhcpd: Listening on
LPF/eth0.4094/00:00:00:00:00:06/176.16.2.0/24
Jul 10 10:23:51 FVS336Gv2 local7.info dhcpd: Sending on
LPF/eth0.4094/00:00:00:00:00:06/176.16.2.0/24
Jul 10 10:23:51 FVS336Gv2 local7.err dhcpd:
Jul 10 10:23:51 FVS336Gv2 local7.err dhcpd: No subnet declaration for eth0.20
(192.168.70.1).
```

show net lan dhcp reserved_ip setup

This command displays information about the DHCP clients, including the assigned (reserved) IP addresses:

```
List of DHCP Reserved Addresses
_____________________________________

Name          IP Address    MAC Address       Group      Profile Name
_____________ _____________ _________________ __________ _____________
IPphoneRoom12 192.168.1.100 d1:d2:44:45:9e:9f GROUP1     Default
SalesServer   192.168.70.15 a1:c1:33:44:2a:2b GROUP5     Sales
Mobile3008    192.168.90.22 a1:b1:11:12:1a:12 Management Marketing
FN_Server     192.168.70.2  a1:a2:a3:11:bc:de Management Sales
```

Dynamic DNS Show Command

This section describes the **`show net ddns setup`** command.

show net ddns setup

This command displays the Dynamic DNS configuration:

```
WAN Mode
________

Single Port WAN1

WAN1 Dynamic DNS service currently disabled
_____________________________________________

WAN2 Dynamic DNS service currently disabled
_____________________________________________
```

IPv4 LAN Show Commands

This section describes the following commands:

- *show net lan ipv4 setup*
- *show net lan ipv4 detailed setup <vlan id>*
- *show net ethernet*
- *show net lan ipv4 advanced setup*
- *show net lan available_lan_hosts list*
- *show net lan lan_groups*
- *show net lan ipv4 multiHoming*
- *show net lan ipv4 traffic_meter setup*
- *show net lan ipv4 traffic_meter detailed_setup <row id>*

show net lan ipv4 setup

This command displays the IPv4 LAN configuration:

```
VLAN Profiles
_____________

Status   Profile Name VLAN Id IPv4 Address Subnet Mask     DHCP Status Server Address
________ ____________ _______ ___________ _______________ ___________ ___________________________
Enabled  Default      1       192.168.1.1  255.255.255.0   DHCP Server 192.168.1.100 - 192.168.1.254
Enabled  Sales        20      192.168.70.1 255.255.255.0   Disabled    Not Applicable
Disabled Marketing    40      192.168.90.5 255.255.255.128 Disabled    Not Applicable

Default VLAN
____________
Port1: Sales
Port2: Default
Port3: Default
Port4: DMZ
```

show net lan ipv4 detailed setup <vlan id>

This command displays the detailed configuration for a VLAN. For the VLAN ID, type a VLAN number.

```
Detailed Setup (IPv4) of VLAN :- Default
_______________________________________


Status: : Enabled
Profile Name: : Default
VLAN Id: : 1
IPv4 Address: : 192.168.1.1
Subnet Mask: : 255.255.255.0
DHCP Status: : DHCP Server
Server Address: : 192.168.1.100 - 192.168.1.254
Primary DNS Server: :
Secondary DNS Server: :
```

```
WINS Server: :
Lease Time: : 24
LDAP Status: : Disabled
DNS Proxy: : Enabled
Inter VLAN Routing: : Disabled
```

show net ethernet

> **Note:** The **show net ethernet** command might be removed and the output included in the output of the *show net statistics* command.

This command displays the MAC address and VLAN status for all Ethernet interfaces.

```
Ethernet Interfaces
_____________________

VLAN ID Interface Name VLAN Enabled Native VLAN
_______ _______________ _____________ ___________
1       eth0           N             N
1       eth1           N             N
```

show net lan ipv4 advanced setup

This command displays the advanced IPv4 LAN configuration:

```
LAN Advanced Setup
__________________

VLAN MAC Settings:
MAC Address for VLANs: Unique
Advanced Settings:
ARP Broadcast: Enabled
```

show net lan available_lan_hosts list

This command displays the IPv4 hosts (that is, the known computers and devices in the LAN):

```
List of Available Lan Hosts
___________________________
```

show net lan lan_groups

This command displays the LAN groups:

```
Row ID : Group Name
_____________________
1       GROUP1
2       GROUP2
3       Finance
4       GROUP4
5       GROUP5
6       SalesEMEA
7       SalesAmericas
8       Management
```

show net lan ipv4 multiHoming

This command displays the LAN secondary IP addresses:

```
IPv4 LAN Multi-homing
_____________________

Available Secondary LAN IPs :-
_____________________________

Row Id IP Address     Subnet Mask
______ _____________ _______________
1      192.168.20.1   255.255.255.0
2      192.168.70.240 255.255.255.128
```

show net lan ipv4 traffic_meter setup

This command displays the LAN traffic meter configuration:

```
LAN Traffic Meter Table
_______________________

Row Id LAN IP Address Direction       Limit (MB) Traffic (MB) State
______ _____________ _______________ __________ ____________ _______
1      192.168.11.68  Download Only   30000      0            Allowed
2      192.168.11.204 Both Directions 45000      0            Allowed
```

show net lan ipv4 traffic_meter detailed_setup <row id>

Note: The row ID refers to the LAN Traffic Meter Table in the output of the **show net lan ipv4 traffic_meter setup** command.

This command displays the detailed traffic meter information for the specified IP address:

```
LAN Traffic Meter Account
_____________________________
LAN IP Address: 192.168.11.204

Direction: Both Directions

Limit in (MB): 45000

Traffic Counter
_______________
Traffic Counter: Restart Counter

Restart Time (HH/MM-Day of Month): 12/0-1
Send e-mail before restarting Counter: Disabled

When Limit is reached
_____________________
Send e-mail alert: Disabled

LAN IP Traffic Statistics
_____________________________
Start Date / Time: Sun Jul  1 00:00:16 2012

Outgoing Traffic Volume: 0
Incoming Traffic Volume: 0
Average per day:
% of Standard Limit:
State: Allowed
```

IPv6 LAN Show Commands

This section describes the following commands:

- *show net lan ipv6 setup*
- *show net radvd lan setup*
- *show net lan ipv6 multiHoming*

show net lan ipv6 setup

This command displays the IPv6 LAN configuration:

```
IPv6 LAN Configuration
_____________________

LAN TCP/IP Setup:
IPv6 Address: fec0::1
IPv6 Prefix Length: 64
DHCPv6:
DHCP Status: Disable DHCPv6 Server
DHCP Mode: Stateless
Prefix Delegation: Disable
Domain Name: netgear.com
Server Preference: 255
DNS Servers: Use Below
Primary DNS Server:
Secondary DNS Server:
Lease/Rebind Time: 86400

List of IPv6 Address Pools
__________________________

Row Id Start Address    End Address        Prefix Length
______ _________________ _________________ _____________
1      fec0::db8:2      fec0::db8:199      10
2      fec0::db8:10a1:1 fec0::db8:10a1:300 10

List of Prefixes for Prefix Delegation
______________________________________

Row Id IPv6 Prefix    IPv6 Prefix Length
______ _____________ ___________________
1      2001:db8::     64
2      2001:db8:ac2:: 64
```

show net radvd lan setup

This command displays the LAN RADVD configuration:

```
Router Advertisement Daemon ( RADVD )
_____________________________________

RADVD Status: Enabled
Advertise Mode: Unsolicited Multicast
Advertise Interval: 30
RA Flags
```

```
Managed: Disabled
Other: Enabled
Router Preference: High
MTU: 1500
Router Lifetime: 3600 Seconds

List of Available Prefixes to Advertise
_______________________________________

ROW ID IPv6 Prefix        IPv6 Prefix Length Life Time
______ _________________ ___________________ _________
1      2002:408b:36e4:a:: 64                  43200
2      FE80:0:0:CC40::    64                  21600
```

show net lan ipv6 multiHoming

This command displays the LAN secondary IPv6 addresses:

```
IPv6 LAN Multi-homing
_____________________

Available Secondary LAN IPs :-
______________________________

Row Id: 1
IPv6 Address: 2001:db8:3000::2192
Prefix Length: 10
```

DMZ Show Commands

This section describes the following commands:

- *show net dmz ipv4 setup*
- *show net dmz ipv6 setup*
- *show net radvd dmz setup*

show net dmz ipv4 setup

This command displays the IPv4 DMZ configuration:

```
DMZ Setup
_________

IPv4 Address: 176.16.2.1
Subnet Mask: 255.255.255.0
```

```
DHCP Setup Configuration:
DHCP Mode: DHCP Server
Domain Name: netgear.com
Starting IP Address: 176.16.2.100
Ending IP Address: 176.16.2.254
Primary DNS Server:
Secondary DNS Server:
WINS Server:
Lease Time in hrs : 24
LDAP Status: Disabled
DNS Proxy:  Enabled
```

show net dmz ipv6 setup

This command displays the IPv6 DMZ configuration:

```
DHCP Setup Configuration
_____________________________

IPv6 Address: 176::1
Prefix Length: 64
DHCP Status: DHCP Server Enabled
Mode: Stateless
Domain Name: netgear.com
DNS Server: Use DNS Proxy
Lease Time in Sec : 86400
Starting IP Address :  176::1100 176::2031:1500
Ending IP Address   :  176::1220 176::2031:1650
Pool Prefix Length  :  56 56
```

show net radvd dmz setup

This command displays the DMZ RADVD configuration:

```
Router Advertisement Daemon ( RADVD )
_____________________________________
RADVD Status: Enabled
Advertise Mode: Unsolicited Multicast
Advertise Interval: 30
RA Flags

Managed: Disabled
Other: Enabled
Router Preference: High
MTU: 1500
Router Lifetime: 3600 Seconds
```

```
List of Available Prefixes to Advertise
_______________________________________

ROW ID IPv6 Prefix           IPv6 Prefix Length Life Time
______ ____________________ __________________ _________
1      2001:db8:abdd::       64                 3600
2      2002:408b:36e2:2727:: 64                 7200
```

Routing Show Commands

This section describes the following commands:

- *show net routing dynamic setup*
- *show net routing static ipv4 setup*
- *show net routing static ipv6 setup*

show net routing dynamic setup

This command displays the dynamic routing configuration:

```
Dynamic Routing
_______________

RIP
___
RIP Direction Both
RIP Version RIP-2M
Authentication for RIP-2B/2M: Enabled
First Key Parameters
MD5 Key Id: 1
MD5 Auth Key:  *****
Not Valid Before: 2011/12/01@07:00:00
Not Valid After: 2012/12/31@23:59:59
Second Key Parameters
MD5 Key Id: 2
MD5 Auth Key: *****
Not Valid Before: 2012/12/31@24:00:00
Not Valid After: 2013/03/31@23:59:59
```

show net routing static ipv4 setup

This command displays the IPv4 static routes configuration:

```
Name    Destination     Gateway         Interface       Metric  Active  Private
----    -----------     -------         ---------       ------  -------  -------
Orly    10.118.215.178  10.192.44.13    WAN1            7       1       1
```

show net routing static ipv6 setup

This command displays the IPv6 static routes configuration:

```
Name    Destination           Gateway               Interface  Metric  Active
----    -----------           -------               ---------  ------  -------
SFO2    2002:201b:24e2::1001  FE80::2001:5efe:ab23  WAN1       2       1
```

Network Statistics Show Command

This section describes the **`show net statistics`** command.

Note: The **`show net statistics`** command might be modified to include the output of the *show net ethernet* command.

show net statistics

This command displays the network statistics for all Ethernet interfaces.

```
Interface Statistics
_____________________

IFACE PktRx  PktTx  ByteRx   ByteTx   ErrRx ErrTx DropRx DropTx Mcast Coll
_____ ______ ______ ________ ________ _____ _____ ______ ______ _____ ____
eth0  20802  31569  2148358  38409384 0     0     0      0      0     0
eth1  359059 186965 61156441 28586367 0     0     0      0      0     0
```

Security Settings Show Commands

This section contains the following subsections:

- *Services Show Commands*
- *Schedules Show Command*
- *Firewall Rules Show Commands*
- *Attack Checks and IGMP Show Commands*
- *Session Limits Show Commands*
- *Advanced Firewall Show Command*
- *Address Filter Show Commands*
- *Port Triggering Show Commands*
- *UPnP Show Commands*
- *Bandwidth Profiles Show Command*
- *Content Filtering Show Commands*

Services Show Commands

This section describes the following commands:

- *show security services setup*
- *show security services qos_profile setup*
- *show security services ip_group ip_setup*
- *show security services service_group setup*

show security services setup

This command displays the configured custom services:

```
List of Available Custom Services
_____________________________________

ROW ID Name              Type ICMP Type / Port Range
______ ________________ ____ ________________________
76     Ixia              TCP  10115-10117
77     RemoteManagement  TCP  8888-8888
78     Traceroute        ICMP 20
```

show security services qos_profile setup

This command displays the configured Qos profiles:

```
List of QoS Profiles
_____________________

ROW ID Profile Name QoS Type      QoS Value Priority
______ ____________ _____________ _________ ________
1      Voice        DSCP          24        High
2      Video        IP-Precedence 5         High
3      Standard     IP-Precedence 0         Default
```

show security services ip_group ip_setup

This command displays the configured IP groups:

```
List of IP Group's IP Table
_____________________________

ROW ID IP Group     IP Address
______ ____________ _____________
1      TechSuppport 10.55.3.201
2      TechSuppport 10.167.88.241
3      VIPcustomers 10.222.24.190
4      VIPcustomers 10.147.219.43
```

show security services service_group setup

This command displays the configured service groups:

```
Custom Service Groups Table
_____________________________

ROW ID Service Group Name List of Services
_______ ___________________ ____________________________________________________
1       CombinedTCP         RPC-TCP,RTSP:TCP,SIP-TCP,SNMP-TRAPS:TCP,SNMP:TCP,SSH:TCP
2       WebAccess           FTP,HTTP,HTTPS
```

Schedules Show Command

This section describes the **show security schedules setup** command.

show security schedules setup

This command displays the configured schedules:

```
Schedules
_________
List of Available Schedules

ROW ID Name      Days                       Start Time End Time
_______ _________ _________________________ __________ ________
1       schedule1 Monday, Wednesday, Friday 07:15 AM   06:30 PM
2       schedule2 All Days                  12:00 AM   11:59 PM
3       schedule3 All Days                  12:00 AM   12:00 AM
```

Firewall Rules Show Commands

This section describes the following commands:

- *show security firewall ipv4 setup lan_wan*
- *show security firewall ipv4 setup dmz_wan*
- *show security firewall ipv4 setup lan_dmz*
- *show security firewall ipv6 setup*

show security firewall ipv4 setup lan_wan

This command displays the configured IPv4 LAN WAN firewall rules:

```
Default Outbound Policy for IPv4 : Allow Always

LAN WAN Outbound Rules
_____________________

ROWID Status  Service Name Filter                          LAN User      WAN User QoS Profile Bandwidth Profile Log
_____ _______ ____________ ____________________________ ____________ ________ ___________ _________________ _____
29    Enabled HTTP         ALLOW Always                   SalesAmericas Any      None        PriorityQueue     Never
30    Enabled AIM          BLOCK by schedule,otherwise allow Any       Any      Voice       NONE              Always

LAN WAN Inbound Rules
____________________

ROWID Status  Service Name Filter                          LAN Server IP Address LAN User WAN User     Destination QoS Profile Bandwidth Profile Log
_____ _______ ____________ ____________________________ ____________________ ________ ____________ ___________ ___________ _________________ _____
31    Enabled FTP          ALLOW Always                   192.168.5.71                  Any          WAN1        None        NONE              Never
32    Enabled RTSP:TCP     BLOCK by schedule,otherwise allow 192.168.20.171             VIPcustomers WAN1        Voice       NONE              Always
```

show security firewall ipv4 setup dmz_wan

This command displays the configured IPv4 DMZ WAN firewall rules:

```
Default Outbound Policy for IPv4 : Allow Always

DMZ WAN Outbound Rules
_____________________

ROWID Status  Service Name Filter                          DMZ User WAN User QoS Profile Log
_____ _______ ____________ ____________________________ _________ _________ ___________ _____
15    Enabled CU-SEEME:TCP BLOCK by schedule,otherwise allow Any      Any      Video       Never
23    Enabled ANY          BLOCK Always                    Any      Any      None        Never

DMZ WAN Inbound Rules
____________________

ROWID Status  Service Name Filter       DMZ Server IP Address DMZ User WAN User     Destination QoS Profile Log
_____ _______ ____________ ____________ ____________________ ________ ____________ ___________ ___________ _____
16    Enabled BOOTP_CLIENT ALLOW Always 192.168.24.112                10.132.215.4 10.168.50.1 None        Always
24    Enabled ANY          BLOCK Always                               Any          WAN1        None        Never
```

show security firewall ipv4 setup lan_dmz

This command displays the configured IPv4 LAN DMZ firewall rules:

```
Default Outbound Policy for IPv4 : Allow Always

LAN DMZ Outbound Rules
______________________

ROWID Status  Service Name Filter       LAN User DMZ User                      Log
_____ _______ ____________ ____________ ________ ____________________________ _____
17    Enabled FTP          ALLOW Always GROUP4   176.14.2.30 - 176.14.2.79 Never
25    Enabled ANY          BLOCK Always Any      Any                        Never
```

```
LAN DMZ Inbound Rules
_____________________

ROWID Status  Service Name Filter                                DMZ User      LAN User       Log
_____ ________ ____________ ____________________________________ _____________ ______________ _______
18    Enabled SSH:UDP      BLOCK by schedule,otherwise allow 176.16.2.101 192.168.5.108 Always
26    Enabled ANY          BLOCK Always                       Any           Any            Never
```

show security firewall ipv6 setup

This command displays all configured IPv6 firewall rules:

```
Default Outbound Policy
_______________________
For IPv6 : Allow Always

List of Available IPv6 Firewall Rules
_____________________________________

ROW ID Status  Rule Type  Service         Action                          Source Users                                 Destination Users        Log    Qos Priority   Schedule
______ _______ _________ _____________ ____________________________ ____________________________________ ____________________ ______ ____________ ________
130    Enabled WAN To LAN RTELNET       ALLOW Always                2002::B32:AAB1:fD41                  FEC0::db8:145            Always Normal-Service
131    Enabled WAN To LAN HTTP          ALLOW Always                Any                                  Any                      Never  Normal-Service
132    Enabled LAN To WAN HTTP          ALLOW Always                Any                                  Any                      Never  Normal-Service
133    Enabled LAN To WAN HTTPS         ALLOW Always                Any                                  Any                      Never  Normal-Service
134    Enabled DMZ To WAN FTP           ALLOW by schedule,otherwise block FEC0::db8:10a1:201 - FEC0::db8:10a1:299 2001:db6::30f4:fbbf:ccbc Never  Normal-Service schedule1
135    Enabled WAN To DMZ VDOLIVE       BLOCK Always                Any                                  176::1150 - 176::1200    Always Normal-Service
136    Enabled DMZ To LAN RTSP:TCP      BLOCK Always                Any                                  Any                      Always Normal-Service
137    Enabled DMZ To LAN RTSP:UDP      BLOCK Always                Any                                  Any                      Always Normal-Service
138    Enabled LAN To DMZ ICMPv6-TYPE-134 BLOCK Always              Any                                  176::1121 - 176::1142    Always Normal-Service
```

Attack Checks and IGMP Show Commands

This section describes the following commands:

- *show security firewall attack_checks setup ipv4*
- *show security firewall attack_checks setup ipv6*
- *show security firewall attack_checks vpn_passthrough setup*
- *show security firewall attack_checks igmp*
- *show security firewall igmp allowed_networks*

show security firewall attack_checks setup ipv4

This command displays which WAN and LAN security checks are enabled for IPv4:

```
Attack Checks
_____________

WAN Security Checks:
____________________
Respond to ping on Wan            : No
Enable Stealth mode               : Yes
Block TCP Flood                   : Yes [100]

LAN Security Checks:
____________________
Block UDP Flood                   : Yes
Disable Ping Reply on LAN Ports   : No
Maximum UDP Connection Limit      :    40
```

show security firewall attack_checks setup ipv6

This command displays which security checks are enabled for IPv6:

```
Attack Checks IPv6

_____________________
WAN Security Checks:
Respond to ping on Wan           : No
VPN IPSec Passthrough            : Yes
```

show security firewall attack_checks vpn_passthrough setup

This command displays which VPN pass-through features are enabled:

```
Passthrough

____________
IPSec VPN Passthrough:

IPSec Passthrough : Enabled
PPTP Passthrough  : Disabled
L2TP Passthrough  : Enabled
```

show security firewall attack_checks igmp

This command displays whether the IGMP proxy is enabled:

```
IGMP Configuration

_____________________
Igmp Proxy: Disabled
```

show security firewall igmp allowed_networks

This command displays the alternate networks from which the VPN firewall can accept multicast traffic.

```
Allowed Networks

_________________

Row Id Network Address Subnet Mask

_______ _________________ _____________
1       203.0.113.54     255.255.255.0
2       203.0.113.62     255.255.255.0
```

Session Limits Show Commands

This section describes the following commands:

- *show security firewall session_limit*
- *show security firewall session_settings*

show security firewall session_limit

This command displays the session limit settings:

```
Session Settings

_________________

Session Limit Enable:   Enabled
Connection Limit Type:  Percentage of Maximum Sessions
User Connection Limit:  2
Session Limit Control:  When Single IP Exceeds
Block IP to Add New Session for time:   5
TCP Session Timeout Duration:   1200(Secs)
UDP Session Timeout Duration:   180(Secs)
ICMP Session Timeout Duration:  8(Secs)
```

show security firewall session_settings

This command displays the session time-out settings:

```
Session Settings

_________________

TCP Session Timeout Duration:1200(Secs)
UDP Session Timeout Duration:180(Secs)
ICMP Session Timeout Duration:8(Secs)
```

Advanced Firewall Show Command

This section describes the **`show security firewall advanced algs`** command.

show security firewall advanced algs

This command displays whether or not SIP ALG is enabled:

```
ALGs

____

Sip: Disabled
```

Address Filter Show Commands

This section describes the following commands:

- *show security address_filter enable_email_log*
- *show security address_filter ip_or_mac_binding setup*
- *show security address_filter mac_filter setup*

show security address_filter enable_email_log

This command displays the configuration of the IP/MAC binding log:

```
Email logs for IP/MAC binding violation IPv4

_____________________________________________

Email logs for IP/MAC binding violation:        Enabled

Email logs for IP/MAC binding violation IPv6

_____________________________________________

Email logs for IP/MAC binding violation:        Disabled
```

show security address_filter ip_or_mac_binding setup

This command displays the IP/MAC bindings:

```
ROW ID Name            MAC Address       IP Address         Log Dropped Packets IP Version
______ _______________ _________________ ___________________ ___________________ __________
1      PhoneConfRoom52 d1:e1:55:54:8e:7f 192.151.1.107      Disabled            IPv4
2      FinanceServer3  c3:e3:ee:f2:a2:db fec0::db8:10b1:166 Enabled             IPv6
```

show security address_filter mac_filter setup

This command displays the configuration of the MAC filter and the MAC addresses for source MAC filtering:

```
Source MAC Filter


__________________


MAC Filtering: Enabled
Policy for MAC Addresses: Block and Permit the rest

List of Available MAC Addresses


_____________________________________
```

```
ROW ID MAC Address
_____ _________________
1      aa:11:bb:22:cc:33
2      a1:b2:c3:de:11:22
3      a1:b2:c3:de:11:25
```

Port Triggering Show Commands

This section describes the following commands:

- *show security porttriggering_rules setup*
- *show security porttriggering_rules status*

show security porttriggering_rules setup

This command displays the port triggering rules:

```
Port Triggering
_______________

List of Available Port Triggering Rules
_______________________________________

ROW ID: 1
Name: Skype
Enable: Yes
Type: TCP
Interface: LAN
Outgoing Start Port: 61196
Outgoing End Port: 61196
Incoming Start Port: 61197
Incoming End Port: 61197
```

show security porttriggering_rules status

This command displays the port triggering status:

```
PortTriggering Rules Status
___________________________
```

UPnP Show Commands

This section describes the following commands:

- *show security upnp portmap*
- *show security upnp setup*

show security upnp portmap

This command displays the UPnP portmap table:

```
UPnP Portmap Table
_____________________
```

show security upnp setup

This command displays the UPnP configuration:

```
UPnP configuration
_____________________

Advertisement Period: 60
Advertisement Time To Live: 6
```

Bandwidth Profiles Show Command

This section describes the **`show security bandwidth profile setup`** command.

show security bandwidth profile setup

This command displays the configured bandwidth profiles:

```
List of Available Bandwidth Profiles
_____________________________________

ROW ID Name           Direction       Inbound Bandwidth Range Outbound Bandwidth Range Is Group
______ _____________  _______________ _______________________ ________________________ ________
1      PriorityQueue  Inbound         10000-100000            NA                       0
2      BusinessLevelI Both Directions 7500-25000              5000-10000               1
```

Content Filtering Show Commands

This section describes the following commands:

- *show security content_filter content_filtering*
- *show security content_filter block_group*
- *show security content_filter blocked_keywords*
- *show security content_filter trusted_domains*

show security content_filter content_filtering

This command displays the status of content filtering and the web components:

```
Content Filtering

_________________
WAN Security Checks

Content Filtering : Enabled

LAN Security Checks
-------------------

Proxy : Disabled
Java : Enabled
ActiveX : Enabled
Cookies : Disabled
```

show security content_filter block_group

This command displays the groups for which content filtering is enabled:

```
Blocked Groups

_____________
List of Blocked Groups

Blocked Groups: GROUP1, GROUP2, Finance, Management
Unblocked Groups : GROUP4, GROUP5, SalesEMEA, SalesAmericas
```

show security content_filter blocked_keywords

This command displays the keywords that are blocked:

```
Blocked Keywords

_______________
List of available Blocked Keywords
```

```
ROW ID Blocked Keyword  Status
______ _______________ _______
2      casino          Enabled
3      nude            Enabled
4      gambl*          Enabled
5      guns            Enabled
```

show security content_filter trusted_domains

This command displays the trusted domains:

```
List of available  Approved URLS

ROW ID Domain
______ __________
1      netgear
2      google.com
3      www.irs.gov
```

Administrative and Monitoring Settings Show Commands

This section contains the following subsections:

- *Remote Management Show Command*
- *SNMP Show Commands*
- *Time Show Command*
- *Firmware Version Show Command*
- *Status Show Command*
- *WAN Traffic Meter Show Command*
- *Logging Configuration Show Commands*
- *Logs Show Commands*
- *Reboot Show Command*

Note: The VPN logs and RADIUS logs are part of the VPN Mode show commands (see *VPN Settings Show Commands* on page 334).

Remote Management Show Command

This section describes the **show system remote_management setup** command.

show system remote_management setup

This command displays the configuration of remote management for Telnet and HTTPS access:

```
Remote Mgmt Configuration for telnet
_____________________________________

IPv4 access granted to everyone
IPv6 access granted to a range of IPs from : FEC0::3001 to FEC0::3100
port being used : 23

Remote Mgmt Configuration for https
____________________________________

IPv4 access granted to everyone
IPv6 access granted to everyone
port being used : 445
```

SNMP Show Commands

This section describes the following commands:

- *show system snmp sys*
- *show system snmp trap [agent ipaddress]*
- *show system snmp trap_events*
- *show system snmp remote_snmp status*
- *show system snmp snmpv3_users*

show system snmp sys

This command displays the SNMP system configuration of the VPN firewall:

```
SNMP System Configuration
_________________________

SysContact: AdminFVS@netgear.com
SysLocation: San Jose
SysName: FVS336Gv2-Bld3
```

show system snmp trap [agent ipaddress]

This command displays the SNMP trap configuration of an SNMP agent:

```
Trap Agent IP Address
_____________________

IP Address: 10.118.33.245
Subnet Mask: 255.255.255.0
Port: 162
Community: public
```

show system snmp trap_events

This command displays which SNMP trap events are enabled:

```
SNMP Trap Events
________________
Trap WAN Connection Failure Event : Yes
Trap SNMP Firewall events         : No
Trap SNMP IPSec-VPN events        : No
Trap SNMP SSL-VPN events          : No
Trap SNMP User Login events       : Yes
Trap SNMP User-Login Failure event: Yes
Trap SNMP WAN Fail-Over events    : No
Trap Configuration change events  : No
```

show system snmp remote_snmp status

This command displays whether SNMP access over a WAN interface is enabled:

```
Remote SNMP Configuration
_________________________
Remote SNMP :   Enabled
```

show system snmp snmpv3_users

This command displays the SNMPv3 user settings:

```
SNMPv3 Users
____________

 User Name Access Type Security Level
 _________ ___________ _______________
 admin     RWUSER      NoAuthNoPriv
 guest     ROUSER      NoAuthNoPriv
```

Time Show Command

This section describes the **show system time setup** command.

show system time setup

This command displays the time configuration and the configuration of the NTP servers:

```
Time Zone & NTP Servers Configuration
_____________________________________

Current Time: Friday, January 24, 2014, 21:46:11 (GMT +0000)
Timezone: (GMT) Greenwich Mean Time : Edinburgh, London
Automatically Adjust for Daylight Savings Time: No
Default NTP servers used : Yes
Resolving ipV6 address: Disabled
NTP Mode: Authoritative Mode
Stratum: 10
ReSynch NTP value: 120
```

Firmware Version Show Command

This section describes the **show system firmware_version** command.

show system firmware_version

This command displays the firmware version:

```
Firmware Version : 4.3.1-17
Secondary Firmware Version :
```

Note: The VPN firewall does not support a secondary firmware image.

Status Show Command

This section describes the **show system status** command.

show system status

This command displays the system status (also referred to as router status) information:

```
System Info
___________

System Name: FVS336Gv2
Firmware Version: 4.3.1-17
```

```
Lan Port 1 Information
_____________________
VLAN Profile:   Sales
VLAN ID:        20
MAC Address:    00:00:00:00:00:08
IP Address:     192.168.70.1
Subnet Mask:    255.255.255.0
DHCP Status:    Disabled

Lan Port 2 Information
_____________________
VLAN Profile:   Default
VLAN ID:        1
MAC Address:    00:00:00:00:00:01
IP Address:     192.168.1.1
Subnet Mask:    255.255.255.0
DHCP Status:    Enabled

Lan Port 3 Information
_____________________
VLAN Profile:   Marketing
VLAN ID:        40
MAC Address:    00:00:00:00:00:04
IP Address:     192.168.90.5
Subnet Mask:    255.255.255.128
DHCP Status:    Enabled

Lan Port 4/DMZ  Information
_____________________________
VLAN Profile:   DMZ
VLAN ID:        4094
MAC Address:    00:00:00:00:00:06
IP Address:     176.16.2.1
Subnet Mask:    255.255.255.0
DHCP Status:    Enabled

DMZ IPv6 Information
___________________
IPv6 Address:
DHCPv6 Server:: Disabled

LAN IPv6 Information
___________________
MAC Address: C0:3F:0E:3B:15:92
IPv6 Address:: fe80::c23f:eff:fe3b:1592 / 64, fec0::1 / 64
```

```
DHCP Server:: Enabled
DHCP Relay:: Disabled
DHCPv6 Server:: Disabled

Broadband Information for WAN1
_____________________________

MAC Address: 00:00:00:00:11:22
IPv4 Address: 10.139.54.228 / 255.255.255.248
IPv6 Address: ::ffff:0:a86:5d9 / 96, fe80::200:ff:fe00:1122 / 64
Wan State: UP
NAT (IPv4 only): Enabled
IPv4 Connection Type: STATIC
IPv6 Connection Type: Dynamic IP (DHCPv6)
IPv4 Connection State: Connected
IPv6 Connection State: Connected
Link State: LINK UP
Upload Connection Speed: 1500
Download Connection Speed: 1000000
Gateway: 10.139.54.225
Primary DNS: 10.80.130.23
Secondary DNS: 8.8.8.8
Gateway (IPv6):
Primary DNS(IPv6):
Secondary DNS(IPv6):

Broadband Information for WAN2
_____________________________

MAC Address: 00:00:00:00:00:01
IPv4 Address: 0.0.0.0 / 0.0.0.0
IPv6 Address:
Wan State: DOWN
NAT (IPv4 only): Enabled
IPv4 Connection Type: Dynamic IP (DHCP)
IPv6 Connection Type: Dynamic IP (DHCPv6)
IPv4 Connection State: Not Yet Connected
IPv6 Connection State: Not Yet Connected
Link State: LINK DOWN
Upload Connection Speed: 1000000
Download Connection Speed: 1000000
Gateway: 0.0.0.0
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0
Gateway (IPv6):
Primary DNS(IPv6):
Secondary DNS(IPv6):
```

WAN Traffic Meter Show Command

This section describes the **show system traffic_meter setup** <**wan interface**> command.

show system traffic_meter setup <wan interface>

This command displays the configuration of the traffic meter and the Internet traffic statistics. For the WAN interface, type **WAN1** or **WAN2**.

```
Enable Traffic Meter
_____________________
Traffic Meter is Enabled

Limit Type Both Directions

Monthly Limit in (MB): 255000

Increase this month limit: Enabled

Increase limit by in (MB): 125000

This month limit:

Traffic Counter
_______________
Traffic Counter: Specific Time

Restart Time (HH:MM-Day of Month): 12:0 AM - 1
Send e-mail before restarting: Enabled
When Limit is reached
_____________________
Traffic Block Status: Block All Traffic Except Email

Send e-mail alert: Enabled

Internet Traffic Statistics
___________________________
Start Date / Time: Fri Jan 24 10:48:54 2014

Outgoing Traffic Volume: 0
Incoming Traffic Volume: 0
Average per day: 0
% of Standard Limit: 0
% of this Month's Limit: 0
```

Logging Configuration Show Commands

This section describes the following commands:

- *show system logging setup*
- *show system logging remote setup*
- *show system dns_logs*

show system logging setup

This command displays the configuration of the IPv4 and IPv6 logs:

```
Logging Config
_____________

Routing Logs
____________

LAN to WAN
__________
Accepted Packets:        Disabled
Dropped Packets:         Disabled

WAN to LAN
__________
Accepted Packets:        Disabled
Dropped Packets:         Disabled

DMZ to WAN
__________
Accepted Packets:        Disabled
Dropped Packets:         Disabled

WAN to DMZ
__________
Accepted Packets:        Disabled
Dropped Packets:         Disabled

LAN to DMZ
__________
Accepted Packets:        Disabled
Dropped Packets:         Disabled

DMZ to LAN
__________
Accepted Packets:        Disabled
Dropped Packets:         Disabled
```

```
System Logs
___________
Change of time by NTP:                  Disabled
Login attempts:                         Disabled
Secure Login attempts:                  Disabled
Reboots:                                Disabled
All Unicast Traffic:                    Disabled
All Broadcast/Multicast Traffic:        Disabled
WAN Status:                             Disabled
Resolved DNS Names:                     Disabled
VPN Logs:                               Disabled
DHCP Server:                            Disabled

Other Event Logs
________________
Source MAC Filter:       Disabled
Session Limit:           Disabled
Bandwidth Limit:         Disabled
```

show system logging remote setup

This command displays the configuration and the schedule of the email logs:

```
Log Identifier: FVS336Gv2-BLD3

Enable E-Mail Logs
__________________

E-Mail Server Address: SMTP.Netgear.com
Return E-Mail Address: FVS336Gv2@netgear.com
Send to E-Mail Address: admin2@netgear.com
Authentication: No Authentication
Respond to Identd from SMTP Server: N

Send E-mail logs by Schedule
____________________________

Unit: Weekly
Day: Sunday
Time: 03 AM

Syslog Configuration
____________________

Syslog Server: Disabled
```

show system dns_logs

This command displays the DNS logs.

Logs Show Commands

This section describes the following commands:

- *show system logs*
- *show sysinfo*

show system logs

This command displays the system logs (the following example shows only part of the command output):

```
Sat Jan 25 21:10:28 2014((GMT)) [FVS336Gv2][Kernel][KERNEL] p->perfect 0000000000000000
p->h a800000417bab200
Sat Jan 25 21:10:28 2014((GMT)) [FVS336Gv2][Kernel][KERNEL] HTB: quantum of class 10001
is big. Consider r2q change.
Sat Jan 25 21:10:28 2014((GMT)) [FVS336Gv2][Kernel][KERNEL] HTB: quantum of class 10002
is big. Consider r2q change.
Sat Jan 25 21:10:28 2014((GMT)) [FVS336Gv2][Kernel][KERNEL] HTB: quantum of class 11024
is big. Consider r2q change.
Sat Jan 25 21:10:28 2014((GMT)) [FVS336Gv2][Kernel][KERNEL] eth0.1: del
01:00:5e:7f:ff:fa mcast address from master interface
Sat Jan 25 21:10:28 2014((GMT)) [FVS336Gv2][Kernel][KERNEL] eth0.1: add
01:00:5e:7f:ff:fa mcast address to master interface
Sat Jan 25 21:10:28 2014((GMT)) [FVS336Gv2][Kernel][KERNEL] tcindex_destroy(tp
a800000416f94600),p a80000041696d680
Sat Jan 25 21:10:28 2014((GMT)) [FVS336Gv2][Kernel][KERNEL] tcindex_walk(tp
a800000416f94600,walker a800000415f4f900),p a80000041696d680
Sat Jan 25 21:10:28 2014((GMT)) [FVS336Gv2][Kernel][KERNEL] tcindex_delete(tp
a800000416f94600,arg 0xa800000416981e08),p a80000041696d680,f 0000000000000000
```

show sysinfo

This command displays system information, including MAC addresses, serial number, and firmware version:

```
System - Manufacturer Information
*************************
Usage:getmd [version|mac|status|serial| productID]
Usage:getmd [version|mac|status|serial| productID]
mac address:C03F0E3B1592
Usage:getmd [version|mac|status|serial| productID]
serial number : 2CH1043E0003B
image status: OK
image version :4.3.1-17
```

```
productID : FVS336Gv2
*************************
```

Reboot Show Command

This section describes the **show system schedule_reboot** command.

show system schedule_reboot

This command displays whether a system reboot is scheduled and at what time it is scheduled:

```
Status : Enable
Minute : 45
Hour   : 23
```

VPN Settings Show Commands

This section contains the following subsections:

- *IPSec VPN Show Commands*
- *SSL VPN Show Commands*
- *SSL VPN User Show Commands*
- *RADIUS Server Show Command*
- *PPTP Server Show Commands*
- *L2TP Server Show Commands*

IPSec VPN Show Commands

This section describes the following commands:

- *show vpn ipsec ikepolicy setup*
- *show vpn ipsec vpnpolicy setup*
- *show vpn ipsec vpnpolicy status*
- *show vpn ipsec mode_config setup*
- *show vpn ipsec logs*

show vpn ipsec ikepolicy setup

This command displays the IKE policies:

```
List of IKE Policies
_____________________

Name               Mode       Local ID                 Remote ID     Encryption Authentication DH Group
___________________ __________ ________________________ _____________ __________ ______________ ____________
iphone             aggressive 10.139.54.228            0.0.0.0       AES-128    SHA-1     Group 2 (1024 bit)
FVS-to-Peer44      main       fe80::a8ab:bbff:fe00:2   peer44.com    3DES       SHA-1     Group 2 (1024 bit)
FVS-to-Paris       main       10.139.54.228            10.112.71.154 3DES       SHA-1     Group 2 (1024 bit)
```

show vpn ipsec vpnpolicy setup

This command displays the IPSec VPN policies:

```
Status  Name             Type        IPSec Mode  Local                                 Remote                          Auth  Encr
_______ _________________ ___________ __________ _____________________________________ _______________________________ ____ ____
Enabled FVS-to-Peer44    Auto Policy Tunnel Mode 2002:408b:36e4:a:a8ab:bbff:fe00:1 / 64 fe80::a4bb:ffdd:fe01:2 / 64    SHA-1 3DES
Enabled FVS-to-Paris     Auto Policy Tunnel Mode 192.168.1.0 / 255.255.255.0           192.168.50.0 / 255.255.255.255 SHA-1 3DES
```

show vpn ipsec vpnpolicy status

This command displays status information about the active and nonactive IPSec VPN policies.

Note: The example output for this command does not relate to the example output for other commands in *VPN Settings Show Commands* section.

```
Row Id Policy Name     Endpoint                       tx ( KB ) tx ( Packets ) State                    Action
______ _________________ ______________________________ _________ _____________ ________________________ _______
1      GW1-to-GW2      10.144.28.226                  0.00      0             IPsec SA Not Established Connect
2      FVS-to-IPv6Peer 2001::da21:1316:df17:dfee:e33c 0.00      0             IPsec SA Not Established Connect
3      10.100.10.1     10.153.46.120                  7.01      31            IPsec SA Established     Drop
4      10.100.10.2     10.153.46.120                  6.68      29            IPsec SA Established     Drop
```

show vpn ipsec mode_config setup

This command displays the Mode Config records:

```
List of Mode Config Records
____________________________

Record Name    Pool Start IP                                  Pool End IP
_______________ ____________________________________________ ____________________________________________
EMEA Sales     172.16.100.1   172.16.200.1                    172.16.100.99   172.16.200.99
Americas Sales 172.25.100.50  172.25.210.1   172.25.220.80    172.25.100.90   172.25.210.99   172.25.220.99
iphone         192.168.22.1                                   192.168.22.2
```

show vpn ipsec logs

This command displays the IPSec VPN logs (the following example shows only part of the command output):

```
Sat Jan 25 21:01:52 2014((GMT)): [FVS336Gv2] [IKE] INFO:  Using IPsec SA configuration:
anonymous
Sat Jan 25 21:01:52 2014((GMT)): [FVS336Gv2] [IKE] INFO:  Re-using previously generated
policy: 100.10.10.2/32[0] 0.0.0.0/0[0] proto=any dir=in
Sat Jan 25 21:01:52 2014((GMT)): [FVS336Gv2] [IKE] WARNING:  less key length proposed,
mine:128 peer:256.  Use initiator's one.
Sat Jan 25 21:01:52 2014((GMT)): [FVS336Gv2] [IKE] INFO:  IPsec-SA established:
ESP/Tunnel 173.11.109.158->64.139.54.228 with spi=73255174(0x45dc906)
Sat Jan 25 21:01:52 2014((GMT)): [FVS336Gv2] [IKE] INFO:  IPsec-SA established:
ESP/Tunnel 10.139.54.228->172.11.109.158 with spi=7343706(0x700e5a)
Sat Jan 25 21:01:52 2014((GMT)): [FVS336Gv2] [IKE] INFO:  Sending Informational Exchange:
notify payload[10637]
```

SSL VPN Show Commands

This section describes the following commands:

- *show vpn sslvpn client*
- *show vpn sslvpn logs*
- *show vpn sslvpn policy*
- *show vpn sslvpn portal_layouts*
- *show vpn sslvpn portforwarding appconfig*
- *show vpn sslvpn portforwarding hostconfig*
- *show vpn sslvpn resource*
- *show vpn sslvpn resource_object <resource name>*
- *show vpn sslvpn route*

show vpn sslvpn client

This command displays the SSL VPN client ranges and configurations:

```
SSL VPN Client(IPv4)
_____________________

Enable Full Tunnel Support: Yes
DNS Suffix:
Primary DNS Server: 192.168.10.5
Secondary DNS Server: 192.168.10.6
Client Address Range Begin: 192.168.251.1
Client Address Range End: 192.168.251.254
```

```
SSL VPN Client(IPv6)

_____________________

Enable Full Tunnel Support: No
DNS Suffix:
Primary DNS Server:
Secondary DNS Server:
Client Address Range Begin: 4000::1
Client Address Range End: 4000::200
```

show vpn sslvpn logs

This command displays the SSL VPN logs (the following example shows only part of the command output):

```
Sat Jan 25 21:01:52 2014(GMT) [FVS336Gv2][SSLVPN][SSLVPN]  SSL_INFO : Login Successful
for geardomain user admin(Admin) from host 10.110.205.58
Sat Jan 25 21:01:52 2014(GMT) [FVS336Gv2][SSLVPN][SSLVPN] SSL_INFO :user admin is
Logged-Out successfully from host 10.110.205.58
Sat Jan 25 21:01:52 2014(GMT) [FVS336Gv2][SSLVPN][SSLVPN]  SSL_INFO : Login Successful
for geardomain user techwriter(Admin) from host 10.110.205.58
Sat Jan 25 21:01:52 2014(GMT) [FVS336Gv2][SSLVPN][SSLVPN]  SSL_INFO : Login Successful
for geardomain user techwriter(Admin) from host 10.110.205.58
Sat Jan 25 21:01:52 2014(GMT) [FVS336Gv2][SSLVPN][SSLVPN]  SSL_INFO : Login Successful
for geardomain user admin(Admin) from host 10.110.205.58
```

show vpn sslvpn policy

This command displays the SSL VPN policies:

```
SSL VPN Policies

__________________

Row Id Policy Name         Policy Type Service Type    Destination Object        Permission
______ ___________________ ___________ _______________ _________________________ __________
1      RoadWarriorPolicy   global      VPN Tunnel      RoadWarrior               Permit
2      RoadWarriorPolicyII global      VPN Tunnel      10.201.33.200:35401-35405 Deny
3      GuestFTPPolicy      user        Port Forwarding 0.0.0.0:25077-25078       Deny
```

show vpn sslvpn portal_layouts

This command displays the SSL VPN portal layouts:

```
List of Layouts

_________________

Row Id Layout Name Description                  Use Count Portal URL (IPv4)                  Portal URL (IPV6)
______ _________ ____________________________ _________ ___________________________________ ____________________________________________
1      SSL-VPN*   Welcome to Netgear Configur... 4         https://10.139.54.228/portal/SSL-VPN https://[fe80::e246:9aff:fe1d:1a9d]/portal/SSL-VPN
2      CSup       In case of login difficulty... 1         https://10.139.54.228/portal/CSup    https://[fe80::e246:9aff:fe1d:1a9d]/portal/CSup
```

show vpn sslvpn portforwarding appconfig

This command displays the SSL VPN port forwarding application configuration:

```
Port Forwarding Application Configuration
_________________________________________

Row Id Server IP      Port
______ _____________ ____
1      192.168.51.227 3389
2      192.168.51.230 4009
```

show vpn sslvpn portforwarding hostconfig

This command displays the SSL VPN port forwarding host configuration:

```
Port Forwarding Host Configuration
__________________________________

Row Id Server IP      FQDN Name
______ _____________ _______________
1      192.168.51.227 RemoteDesktop
2      192.168.51.230 Support.app.com
```

show vpn sslvpn resource

This command displays the SSL VPN resource configuration:

```
RESOURCES
_________

Row Id Resource Name Service
______ _____________ _______________
1      TopSecure     Port Forwarding
2      FTPServer     Port Forwarding
3      RoadWarrior   VPN Tunnel
```

show vpn sslvpn resource_object <resource name>

This command displays the detailed configuration for the specified resource object. Type the name of a resource object that is displayed in the output of the *show vpn sslvpn resource* command.

```
RESOURCE OBJECTS
________________

Row Id: 1
Object Type: IP Address
```

```
Object Address: 192.168.144.23
Mask Length: 32
Start Port: 40133
End Port: 40140
```

show vpn sslvpn route

This command displays the SSL VPN client routes:

```
Configured Client Routes
_________________________

Row Id Destination Network     Subnet Mask
______ ______________________ _______________
1      192.168.4.20            255.255.255.254
2      2001:abcf:1241:dffe::22 10
```

SSL VPN User Show Commands

This section describes the following commands:

- *show vpn sslvpn users domains*
- *show vpn sslvpn users groups*
- *show vpn sslvpn users users*
- *show vpn sslvpn users login_policies <row id>*
- *show vpn sslvpn users ip_policies <row id>*
- *show vpn sslvpn users browser_policies <row id>*
- *show vpn sslvpn users active_users*

show vpn sslvpn users domains

This command displays the domain configurations:

```
List of Domains
_______________

Row_Id Domain Name    Authentication Type Portal Layout Name
______ _____________ ___________________ ____________________
1      geardomain*    Local User Database SSL-VPN
2      Headquarter    LDAP                CSup
3      LevelI_Support Local User Database SSL-VPN
4      TEST           wikid_pap           SSL-VPN
```

show vpn sslvpn users groups

This command displays the group configurations:

```
List of Groups

_____________

Row_Id Name             Domain
_______ _______________ _______________
1      geardomain*      geardomain
2      Headquarter      Headquarter
3      Sales            Headquarter
4      LevelI_Support   LevelI_Support
5      TEST             TEST
```

show vpn sslvpn users users

This command displays the user account configurations:

```
List of Users

_____________

Row_Id User Name      Group          Type           Authentication Domain Login Status
_______ _____________ _____________ _____________ _____________________ ____________________
1      admin*         geardomain     Administrator  geardomain            Enabled (LAN and WAN)
2      guest*         geardomain     Guest          geardomain            Enabled (LAN only)
3      admin2         geardomain     Administrator  geardomain            Enabled (LAN and WAN)
4      PeterBrown     Sales          SSL VPN User   Headquarter           Enabled (LAN and WAN)
5      JohnD_Company  LevelI_Support SSL VPN User   LevelI_Support        Enabled (LAN and WAN)
6      chin           geardomain     Administrator  geardomain            Enabled (LAN and WAN)
7      iphone                        IPSEC VPN User                       Enabled (LAN and WAN)
```

show vpn sslvpn users login_policies <row id>

Note: The row ID refers to the List of Users table in the output of the **show vpn sslvpn users users** command.

This command displays the login restrictions based on login policies for the specified user:

```
User Login Policies

___________________

User Name: PeterBrown
Disable Login: No
Deny Login from Wan Interface: No
```

show vpn sslvpn users ip_policies <row id>

Note: The row ID refers to the List of Users table in the output of the **show vpn sslvpn users users** command.

This command displays the login restrictions based on IP addresses for the specified user:

```
User Ip Policies

_________________
User Name: PeterBrown
Allow Login from Defined Address: Yes

Ip Addresses

_____________

Row_Id: 1
Source Address Type: IP Address
Network/IP Address: 10.156.127.39
Mask Length: 32
```

show vpn sslvpn users browser_policies <row id>

Note: The row ID refers to the List of Users table in the output of the **show vpn sslvpn users users** command.

This command displays the login restrictions based on web browsers for the specified user:

```
User Browser Policies

_____________________
User Name: PeterBrown
Allow Login from Defined Browser: No

Defined Browsers

_________________
Internet Explorer
Netscape Navigator
```

show vpn sslvpn users active_users

This command displays the active SSL VPN users:

```
UserName: : admin
GroupName: : geardomain
LoginAddress: : 10.116.205.166
LoginTime: : Sat Jan 25 20:56:36 2014 (GMT +0000)
```

RADIUS Server Show Command

This section describes the **show vpn ipsec radius** [**ipaddress**] command.

show vpn ipsec radius [ipaddress]

This command displays the configuration of all RADIUS servers or of a specified RADIUS server:

- All RADIUS servers:

```
FVS336Gv2> show vpn ipsec radius

Configured RADIUS Client
_________________________

Server IP   Server Port Timeout Retries NAS Identifier
___________ ___________ _______ _______ _______________
192.168.4.2 1812        30      4       FVS336Gv2
192.168.4.3 1812        30      4       FVS336Gv2
```

- A specified RADIUS server:

```
FVS336Gv2> show vpn ipsec radius 192.168.4.2

RADIUS Configuration
____________________

Auth Server IP Address: 192.168.4.2
Auth Port: 1812
Timeout (in seconds): 30
Retries: 4
Secret: sharedsecret
NAS Identifier: FVS336Gv2
```

PPTP Server Show Commands

This section describes the following commands:

- *show vpn pptp server setup*
- *show vpn pptp server connections*

show vpn pptp server setup

This command displays the configuration of the PPTP server:

```
PPTP Server Configuration
_____________________________

PPTP Server Status: Enabled
PPTP Starting IP Address: 10.119.215.1
PPTP server Ending IP Address: 10.119.215.26
PPTP server Idle Timeout: 999
```

show vpn pptp server connections

This command displays the users that are connected through the PPTP server:

```
List of PPTP Active Users
_____________________________
```

L2TP Server Show Commands

This section describes the following commands:

- *show vpn l2tp server setup*
- *show vpn l2tp server connections*

show vpn l2tp server setup

This command displays the configuration of the L2TP server:

```
L2TP Server Configuration
_____________________________

L2TP Server Status: Enabled
L2TP Starting IP Address: 192.168.112.1
L2TP server Ending IP Address: 192.168.112.25
L2TP server Idle Timeout: 10
```

show vpn l2tp server connections

This command displays the users that are connected through the L2TP server:

```
List of L2TP Active Users
_____________________________
```

Utility Commands

9

This chapter explains the configuration commands, keywords, and associated parameters in the util mode. The chapter includes the following sections:

- *Overview Util Commands*
- *Firmware Backup, Restore, and Upgrade Commands*
- *Diagnostic Commands*

Overview Util Commands

Enter the **`util ?`** command at the CLI prompt to display the utility commands in the util mode. The following table lists the commands in alphabetical order:

Table 16. Utility commands in the util mode

Command Name	Purpose
util backup_configuration	Back up the configuration file of the VPN firewall to a TFTP server.
util dns_lookup	Look up the IP address of a domain name.
util firmware_upgrade	Upgrade the firmware of the VPN firewall from a TFTP server.
util ping	Ping an IP address.
util ping_through_vpn_tunnel	Ping a VPN endpoint IP address.
util reboot	Reboot the VPN firewall.
util restore_factory_defaults	Restore the VPN firewall to factory default settings.
util routing_table_ipv4	Display the IPv4 routing table.
util routing_table_ipv6	Display the IPv6 routing table.
util traceroute	Trace a route to an IP address.
util upload_configuration	Upload a previously backed-up configuration file of the VPN firewall from a TFTP server.

Firmware Backup, Restore, and Upgrade Commands

This section describes the following commands:

- *util backup_configuration*
- *util upload_configuration*
- *util firmware_upgrade*
- *util reboot*
- *util restore_factory_defaults*

util backup_configuration

This command backs up the configuration file of the VPN firewall to a TFTP server.

Format	**`util backup_configuration`** *<destination file name> <tftp server address>*
Mode	util

util upload_configuration

This command uploads a previously backed-up configuration file of the VPN firewall from a TFTP server.

Format	**util upload_configuration** *<source file name> <tftp server address>*
Mode	util

util firmware_upgrade

This command upgrades the firmware of the VPN firewall from a TFTP server.

Format	**util firmware_upgrade** *<source file name> <tftp server address>*
Mode	util

util reboot

This command reboots the VPN firewall. It takes about three minutes for the VPN firewall to come back up.

Format	**util reboot**
Mode	util

util restore_factory_defaults

This command restores the VPN firewall to factory default settings. It takes about three minutes for the VPN firewall to come back up.

Format	**util restore_factory_defaults**
Mode	util

Diagnostic Commands

This section describes the following commands:

- *util dns_lookup*
- *util ping*
- *util ping_through_vpn_tunnel*
- *util traceroute*
- *util routing_table_ipv4*
- *util routing_table_ipv6*

util dns_lookup

This command looks up the IP address of a domain name.

Format	**util dns_lookup** *<domain name>*
Mode	util

```
FVS336Gv2> util dns_lookup netgear.com
Server:    10.80.130.23
Address 1: 10.80.130.23 ns1.megapath.net
Name:      netgear.com
Address 1: 10.16.44.90
```

util ping

This command pings an IP address with 56 data bytes and displays the ping information.

Format	**util ping** *<ipaddress>*
Mode	util

```
FVS336Gv2> util ping 10.136.216.82
PING 10.136.216.82 (10.136.216.82): 56 data bytes
64 bytes from 10.136.216.82: seq=0 ttl=48 time=69.168 ms
64 bytes from 10.136.216.82: seq=1 ttl=48 time=112.606 ms
64 bytes from 10.136.216.82: seq=2 ttl=48 time=46.531 ms
64 bytes from 10.136.216.82: seq=3 ttl=48 time=49.804 ms
64 bytes from 10.136.216.82: seq=4 ttl=48 time=51.247 ms
--- 10.136.216.82 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 46.531/65.871/112.606 ms
```

util ping_through_vpn_tunnel

This command pings a VPN endpoint IP address with 56 data bytes through a VPN tunnel and displays the ping information.

Format	**util ping_through_vpn_tunnel** *<ipaddress>*
Mode	util

```
FVS336Gv2> util ping_through_vpn_tunnel 10.136.24.128
Pinging 192.168.1.1 from 5
Ping passed
64 bytes from 10.136.24.128: icmp_seq=0 ttl=64
64 bytes from 10.136.24.128: icmp_seq=1 ttl=64
64 bytes from 10.136.24.128: icmp_seq=2 ttl=64
64 bytes from 10.136.24.128: icmp_seq=3 ttl=64
64 bytes from 10.136.24.128: icmp_seq=4 ttl=64
```

---

util traceroute

This command traces a route to an IP address.

Format	**util traceroute** *<ipaddress>*
Mode	util

```
FVS336Gv2> util traceroute 10.136.24.128
traceroute to 10.136.24.128 (10.136.24.128), 30 hops max, 40 byte packets|
1   (10.136.24.128)  0.516 ms  0.227 ms  0.218 ms
```

---

util routing_table_ipv4

This command displays the IPv4 routing table.

Format	**util routing_table_ipv4**
Mode	util

---

util routing_table_ipv6

This command displays the IPv6 routing table.

Format	**util routing_table_ipv6**
Mode	util

Command List

net ddns configure . . . 57
net dmz ipv4 configure . . . 81
net dmz ipv6 configure . . . 83
net dmz ipv6 pool configure <ipv6 address> . . . 85
net dmz ipv6 pool delete < ipv6 address> . . . 85
net ethernet configure <interface name or number> . . . 62
net ipv6 ipmode configure . . . 50
net ipv6_tunnel isatap add . . . 55
net ipv6_tunnel isatap delete <row id> . . . 56
net ipv6_tunnel isatap edit <row id> . . . 56
net ipv6_tunnel six_to_four configure . . . 57
net lan dhcp reserved_ip configure <mac address> . . . 65
net lan dhcp reserved_ip delete <mac address> . . . 66
net lan ipv4 advanced configure . . . 64
net lan ipv4 configure <vlan id> . . . 59
net lan ipv4 default_vlan . . . 63
net lan ipv4 delete <vlan id> . . . 62
net lan ipv4 disable <vlan id> . . . 62
net lan ipv4 enable <vlan id> . . . 62
net lan ipv4 multi_homing add . . . 66
net lan ipv4 multi_homing delete <row id> . . . 68
net lan ipv4 multi_homing edit <row id> . . . 67
net lan ipv4 traffic_meter configure <ip address> . . . 68
net lan ipv4 traffic_meter delete <row id> . . . 70
net lan ipv6 configure . . . 71
net lan ipv6 multi_homing add . . . 74
net lan ipv6 multi_homing delete <row id> . . . 75
net lan ipv6 multi_homing edit <row id> . . . 74
net lan ipv6 pool add . . . 72
net lan ipv6 pool delete <row id> . . . 74
net lan ipv6 pool edit <row id> . . . 73
net lan ipv6 prefix_delegation add . . . 79
net lan ipv6 prefix_delegation delete <row id> . . . 80
net lan ipv6 prefix_delegation edit <row id> . . . 80
net lan lan_groups edit <row id> <new group name> . . . 66
net protocol_binding add . . . 43
net protocol_binding delete . . . 49
net protocol_binding disable . . . 49

net protocol_binding edit <row id> 46
net protocol_binding enable 49
net qos configure 90
net qos profile add 90
net qos profile delete <row id> 102
net qos profile disable <row id> 102
net qos profile edit <row id> 96
net qos profile enable <row id> 102
net radvd configure dmz 85
net radvd configure lan 75
net radvd pool dmz add 87
net radvd pool dmz delete <row id> 89
net radvd pool dmz edit <row id> 88
net radvd pool lan add 77
net radvd pool lan delete <row id> 79
net radvd pool lan edit <row id> 78
net routing dynamic configure 104
net routing static ipv4 configure <route name> 103
net routing static ipv4 delete <route name> 104
net routing static ipv4 delete_all 104
net routing static ipv6 configure <route name> 108
net routing static ipv6 delete <route name> 109
net routing static ipv6 delete_all 109
net siit configure 54
net wan port_setup ipv4 configure <wan interface> 30
net wan port_setup ipv6 configure <wan interface> 33
net wan wan ipv4 configure <wan interface> 35
net wan wan ipv4 secondary_address add <wan interface> 41
net wan wan ipv4 secondary_address delete <row id> 41
net wan wan ipv6 configure <wan interface> 50
net wan_settings load_balancing configure 41
net wan_settings wanmode configure 34
security address_filter ip_or_mac_binding add 182
security address_filter ip_or_mac_binding delete <row id> 184
security address_filter ip_or_mac_binding edit <row id> 184
security address_filter ip_or_mac_binding enable_email_log <ip version> 185
security address_filter mac_filter configure 181
security address_filter mac_filter source add 182
security address_filter mac_filter source delete <row id> 182
security bandwidth enable_bandwidth_profiles {Y | N} 189
security bandwidth profile add 189
security bandwidth profile delete <row id> 191
security bandwidth profile edit <row id> 190
security content_filter blocked_keywords add 195

security content_filter blocked_keywords delete <row id> 196
security content_filter blocked_keywords edit <row id> 196
security content_filter block_group disable 194
security content_filter block_group enable 193
security content_filter content_filtering configure 192
security content_filter trusted_domain add 196
security content_filter trusted_domain delete <row id> 197
security content_filter trusted_domain edit <row id> 197
security firewall advanced algs 180
security firewall attack_checks configure ipv4 172
security firewall attack_checks configure ipv6 175
security firewall attack_checks vpn_passthrough configure 174
security firewall igmp alternate_networks add 176
security firewall igmp alternate_networks delete 177
security firewall igmp configure 176
security firewall ipv4 add_rule dmz_wan inbound 146
security firewall ipv4 add_rule dmz_wan outbound 139
security firewall ipv4 add_rule lan_dmz inbound 158
security firewall ipv4 add_rule lan_dmz outbound 152
security firewall ipv4 add_rule lan_wan inbound 129
security firewall ipv4 add_rule lan_wan outbound 122
security firewall ipv4 default_outbound_policy {Allow | Block} 164
security firewall ipv4 delete <row id> 164
security firewall ipv4 disable <row id> 164
security firewall ipv4 edit_rule dmz_wan inbound <row id> 149
security firewall ipv4 edit_rule dmz_wan outbound <row id> 143
security firewall ipv4 edit_rule lan_dmz inbound <row id> 161
security firewall ipv4 edit_rule lan_dmz outbound <row id> 155
security firewall ipv4 edit_rule lan_wan inbound <row id> 135
security firewall ipv4 edit_rule lan_wan outbound <row id> 126
security firewall ipv4 enable <row id> 165
security firewall ipv6 configure 165
security firewall ipv6 default_outbound_policy {Allow | Block} 165
security firewall ipv6 delete <row id> 171
security firewall ipv6 disable <row id> 172
security firewall ipv6 edit <row id> 169
security firewall ipv6 enable <row id> 172
security firewall session_limit configure 177
security firewall session_settings configure 179
security porttriggering_rules add 185
security porttriggering_rules delete <row id> 188
security porttriggering_rules edit <row id> 187
security schedules edit {1 | 2 | 3} 120
security services add 111
security services delete <row id> 113

security services edit <row id> 112
security services ip_group add 117
security services ip_group add_ip_to <group name> 119
security services ip_group delete <row id> 119
security services ip_group delete_ip <row id> 119
security services ip_group edit <row id> 118
security services qos_profile add 114
security services qos_profile delete <row id> 117
security services qos_profile edit <row id> 116
security services service_group add 113
security services service_group delete <row id> 114
security services service_group edit <row id> 113
security upnp configure 188
show net ddns setup 304
show net dmz ipv4 setup 310
show net dmz ipv6 setup 311
show net ethernet 306
show net ipv6 ipmode setup 302
show net ipv6_tunnel setup 302
show net ipv6_tunnel status 303
show net lan available_lan_hosts list 306
show net lan dhcp leased_clients list 303
show net lan dhcp logs 303
show net lan dhcp reserved_ip setup 304
show net lan ipv4 advanced setup 306
show net lan ipv4 detailed setup <vlan id> 305
show net lan ipv4 multiHoming 307
show net lan ipv4 setup 305
show net lan ipv4 traffic_meter detailed_setup <row id> 308
show net lan ipv4 traffic_meter setup 307
show net lan ipv6 multiHoming 310
show net lan ipv6 setup 309
show net lan lan_groups 307
show net protocol_binding setup 301
show net qos setup 302
show net radvd dmz setup 311
show net radvd lan setup 309
show net routing dynamic setup 312
show net routing static ipv4 setup 312
show net routing static ipv6 setup 313
show net siit setup 303
show net statistics 313
show net wan port_setup ipv4 <wan interface> 298
show net wan port_setup ipv6 <wan interface> 299

show net wan wan ipv4 secondary_addresses <wan interface> 300
show net wan wan ipv4 setup <wan interface> 299
show net wan wan ipv4 status <wan interface> 300
show net wan wan ipv6 setup <wan interface> 301
show net wan wan ipv6 status <wan interface> 301
show net wan_settings wanmode 298
show security address_filter enable_email_log 320
show security address_filter ip_or_mac_binding setup 320
show security address_filter mac_filter setup 320
show security bandwidth profile setup 322
show security content_filter blocked_keywords 323
show security content_filter block_group 323
show security content_filter content_filtering 323
show security content_filter trusted_domains 324
show security firewall advanced algs 319
show security firewall attack_checks igmp 318
show security firewall attack_checks setup ipv4 317
show security firewall attack_checks setup ipv6 318
show security firewall attack_checks vpn_passthrough setup 318
show security firewall igmp allowed_networks 318
show security firewall ipv4 setup dmz_wan 316
show security firewall ipv4 setup lan_dmz 316
show security firewall ipv4 setup lan_wan 316
show security firewall ipv6 setup 317
show security firewall session_limit 319
show security firewall session_settings 319
show security porttriggering_rules setup 321
show security porttriggering_rules status 321
show security schedules setup 315
show security services ip_group ip_setup 314
show security services qos_profile setup 314
show security services service_group setup 315
show security services setup 314
show security upnp portmap 322
show security upnp setup 322
show sysinfo 333
show system dns_logs 333
show system firmware_version 327
show system logging remote setup 332
show system logging setup 331
show system logs 333
show system remote_management setup 325
show system schedule_reboot 334
show system snmp remote_snmp status 326
show system snmp snmpv3_users 326

show system snmp sys 325
show system snmp trap [agent ipaddress] 326
show system snmp trap_events 326
show system status 327
show system time setup 327
show system traffic_meter setup <wan interface> 330
show vpn ipsec ikepolicy setup 335
show vpn ipsec logs 336
show vpn ipsec mode_config setup 335
show vpn ipsec radius [ipaddress] 342
show vpn ipsec vpnpolicy setup 335
show vpn ipsec vpnpolicy status 335
show vpn l2tp server connections 343
show vpn l2tp server setup 343
show vpn pptp server connections 343
show vpn pptp server setup 343
show vpn sslvpn client 336
show vpn sslvpn logs 337
show vpn sslvpn policy 337
show vpn sslvpn portal_layouts 337
show vpn sslvpn portforwarding appconfig 338
show vpn sslvpn portforwarding hostconfig 338
show vpn sslvpn resource 338
show vpn sslvpn resource_object <resource name> 338
show vpn sslvpn route 339
show vpn sslvpn users active_users 341
show vpn sslvpn users browser_policies <row id> 341
show vpn sslvpn users domains 339
show vpn sslvpn users groups 340
show vpn sslvpn users ip_policies <row id> 341
show vpn sslvpn users login_policies <row id> 340
show vpn sslvpn users users 340
system logging configure 216
system logging remote configure 219
system remote_management https configure 199
system remote_management telnet configure 201
system schedule_reboot configure 223
system snmp remote_snmp enable 204
system snmp sys configure 206
system snmp trap configure <ip address> 203
system snmp trap delete <ipaddress> 204
system snmp trapevent edit 205
system snmp v3_users edit 206
system time configure 208

system traffic_meter configure <wan interface> 213
util backup_configuration 345
util dns_lookup 347
util firmware_upgrade 346
util ping 347
util ping_through_vpn_tunnel 348
util reboot 346
util restore_factory_defaults 346
util routing_table_ipv4 348
util routing_table_ipv6 348
util traceroute 348
util upload_configuration 346
vpn ipsec ikepolicy configure <ike policy name> 228
vpn ipsec ikepolicy delete <ike policy name> 234
vpn ipsec mode_config configure <record name> 246
vpn ipsec mode_config delete <record name> 248
vpn ipsec radius configure 285
vpn ipsec vpnpolicy configure <vpn policy name> 234
vpn ipsec vpnpolicy connect <vpn policy name> 245
vpn ipsec vpnpolicy delete <vpn policy name> 244
vpn ipsec vpnpolicy disable <vpn policy name> 245
vpn ipsec vpnpolicy drop <vpn policy name> 245
vpn ipsec vpnpolicy enable <vpn policy name> 245
vpn ipsec wizard configure <Gateway | VPN_Client> 225
vpn l2tp server configure 288
vpn pptp server configure 287
vpn sslvpn client ipv4 271
vpn sslvpn client ipv6 272
vpn sslvpn policy add 278
vpn sslvpn policy delete <row id> 285
vpn sslvpn policy edit <row id> 283
vpn sslvpn portal_layouts add 254
vpn sslvpn portal_layouts delete <row id> 257
vpn sslvpn portal_layouts edit <row id> 255
vpn sslvpn portal_layouts set_default <row id> 257
vpn sslvpn portforwarding appconfig add 269
vpn sslvpn portforwarding appconfig delete <row id> 269
vpn sslvpn portforwarding hostconfig add 269
vpn sslvpn portforwarding hostconfig delete <row id> 270
vpn sslvpn resource add 275
vpn sslvpn resource configure add <resource name> 276
vpn sslvpn resource configure delete <row id> 278
vpn sslvpn resource delete <row id> 276
vpn sslvpn route add 273
vpn sslvpn route delete <row id> 274

vpn sslvpn users domains add 257
vpn sslvpn users domains delete <row id> 260
vpn sslvpn users domains disable_Local_Authentication {Y | N} 260
vpn sslvpn users domains edit <row id> 259
vpn sslvpn users groups add 261
vpn sslvpn users groups delete <row id> 262
vpn sslvpn users groups edit <row id> 262
vpn sslvpn users users add 263
vpn sslvpn users users browser_policies <row id> 267
vpn sslvpn users users delete <row id> 264
vpn sslvpn users users edit <row id> 264
vpn sslvpn users users ip_policies configure <row id> 265
vpn sslvpn users users ip_policies delete <row id> 267
vpn sslvpn users users login_policies <row id> 265
vpn sslvpn wizard configure 249