NETGEAR

ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N

CLI Reference Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

August 2012
202-10827-01
v3.0

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, get support online, or for more information about the topics covered in this manual, visit the Support website at

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/app/answers/detail/a_id/984.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10827-01	3.0	August 2012	Many commands changed and some commands added
202-10827-01	2.0	May 2012	Minor corrections
202-10827-01	1.0	April 2012	First publication

Contents

Chapter 9 Show Commands

Chapter 10 Utility Commands

CLI Command Index

Introduction

1

This document describes the command-line interface (CLI) for the NETGEAR ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N.

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

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

Note: For more information about the features that you can configure using the CLI, see the *ProSafe Wireless-N 8-port Gigabit VPN Firewall FVS318N Reference Manual*.

Note: You cannot generate and upload a certificate through the CLI. You need to 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 down 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 need to 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 need to type a value. You need to 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 following information is provided:

- **Format**. Shows the command keywords and the required and optional parameters.
- **Mode**. Identifies the command mode you need to 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 font conventions are used:

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

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 need to 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 need to 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 need to 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** {**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 need to select is either **6To4** or **Global-Local-ISATAP**.

- If you select **6To4**, you also need to issue the **sla_id keyword** and enter a value for the <*id number*> parameter.
- If you select **Global-Local-ISATAP**, you also need to issue the **prefix_address** keyword and enter a value for the <*ipv6-address*> parameter, and you need to issue the **prefix_length** keyword and enter a value for the <*prefix length*> parameter.

prefix_life_time is a keyword. <*seconds*> is the required parameter for which you need to enter a value.

Command example:

```
FVS318N> 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 need to 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 the following formats: • FE80:0000:0000:0000:020F:24FF:FEBF:DBCB, or • FE80:0:0:0:20F:24FF:FEBF:DBCB, or • FE80::20F:24FF:FEBF:DBCB, or • 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.

The Four Categories of Commands

There are four CLI command categories:

- Configuration commands with five main configuration modes. For more information, see the following section, *The Five Main Modes for Configuration Commands*). Save commands also fall into this category (see *Save Commands* on page 13).
- Show commands that are available for the five main configuration modes (see *Chapter 8, Overview of the Show Commands* and *Chapter 9, Show Commands*).
- Utility commands (see *Chapter 10, Utility Commands*).
- Global commands (see *Global Commands* on page 14).

The Five Main Modes for Configuration Commands

For the configuration commands, there are five main modes in the CLI: net, security, system, dot11, 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 7*).

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 addresses Advanced IPv4 LAN settings IPv6 LAN settings Secondary IPv6 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
	wan	IPv4 WAN (Internet) settings IPv6 WAN (Internet) settings MTU, port speed, and MAC address	Network Configuration > WAN Settings
	wan_settings	NAT or Classical Routing	Network Configuration > WAN Settings

Table 3. Main configuration modes (continued)

CLI			Web Management Interface (GUI)
Main Mode	**Submode**	**Feature That You Can Configure**	**Basic Path**
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		Security > Services
	upnp		Security > UPnP
Administration and monitoring configuration commands			
system	logging		Monitoring > Firewall Logs & E-mail
	remote_management		Administration > Remote Management
	snmp		Administration > SNMP
	time		Administration > Time Zone
	traffic_meter		Monitoring > Traffic Meter
Wireless configuration commands			
dot11	profile	Wireless profiles	Network Configuration > Wireless Settings
	radio	Wireless radio	Network Configuration > Wireless Settings

Table 3. Main configuration modes (continued)

CLI			Web Management Interface (GUI)
Main Mode	**Submode**	**Feature That You Can Configure**	**Basic Path**
VPN configuration commands			
vpn	ipsec	IKE policies VPN policies VPN IPSec Wizard Mode Config records	VPN > IPSec VPN
	l2tp	L2TP server	VPN > L2TP Server
	radius	RADIUS servers for VPN	VPN > IPSec VPN > RADIUS Client
	sslvpn	SSL policies Resources Portal layouts SSL VPN clients Client routes Port forwarding	VPN > SSL VPN
		Domains Groups User accounts User login and IP policies	Users

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 five 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 have issued 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 need to save your changes:

- **net lan ipv4 configure** <*vlan id*> lets you enter the net-config [lan-ipv4] configuration mode. After you made 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 made your changes, issue **save** or **exit** to save your changes.
- **dot11 profile configure** <*profile name*> lets you enter the dot11-config [profile] configuration mode. After you made 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 have issued 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*>
- **dot11 profile disable** <*profile 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 need to 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.

The 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 wan1 ipv4 configure`**
	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 need to enter a parameter to enter a configuration mode. For example, **`security schedules edit`** <*`row id`*> requires you to enter the row ID parameter to 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 ID or a name. For example, **`security firewall ipv4 delete`** <*`row id`*> requires you to enter the row ID parameter to delete the firewall rule.

  For this type of command, the format and mode are shown in this manual:

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 also, the format and mode are shown in this manual:

Format	**`util restore_factory_defaults`**
Mode	util

Command Autocompletion and Command Abbreviation

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

The following keys both perform autocompletion for the current command. If the command prefix is not unique, a subsequent repeat of the key displays possible completions.

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

CLI Line-Editing Conventions

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 has been 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 need to type all of the required keywords and parameters before you use autocompletion.	
Enter (or Return)	Autocompletes, syntax-checks, and then executes a command. If there is a syntax error, the offending part of the command line is highlighted and explained. If the command prefix is not unique, a subsequent repeat of the key displays possible completions.
Spacebar	Autocompletes, or if the command is already resolved, inserts a space. If the command prefix is not unique, a subsequent repeat of the key displays 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.

Table 6. CLI editing conventions (continued)

Key or Key Sequence	Description
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. FVS318N> is the CLI prompt.

```
FVS318N login: admin
Password:
**********************************************
    Welcome to FVS318N Command Line Interface
**********************************************
FVS318N>
```

2 Overview of the Configuration Commands

This chapter provides an overview of all configuration commands in the five configuration command modes. The keywords and associated parameters that are available for these commands are explained in the following chapters. The chapter includes the following sections:

- *Network Settings (Net Mode) Configuration Commands*
- *Security Settings (Security Mode) Configuration Commands*
- *Administrative and Monitoring Settings (System Mode) Configuration Commands*
- *Wireless Settings (Dot11 Mode) Configuration Commands*
- *VPN Settings (VPN Mode) Configuration Commands*

Network Settings (Net Mode) 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 Dynamic DNS (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 pool ipv6 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 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.
	net lan ipv4 multi_homing edit <row id>	Configure an existing secondary IPv4 address.
	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 configure	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.

		delegation.
lan (continued)	*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.
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 wan1 ipv4 configure*	Configure the IPv4 settings of the WAN interface.
	net wan wan1 ipv6 configure	Configure the IPv6 settings of the WAN interface.
wan_settings	*net wan_settings wanmode configure*	Configure the mode of IPv4 routing (NAT or classical routing) between the WAN interface and LAN interfaces.

Security Settings (Security Mode) 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 {IPv4 | IPv6}	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.
bandwidth	*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.

		groups.
content_filter	*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 igmp configure	Enable or disable multicast pass-through for IPv4 traffic.
	security firewall attack_checks jumboframe configure	Enable or disable jumbo frames for IPv4 traffic.
	security firewall attack_checks vpn_passthrough configure	Configure VPN 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.
	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.

firewall (continued)	*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.

firewall (continued)		limits.
	security firewall session_settings configure	Configure global session time-outs.
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.
upnp	*security upnp configure*	Configure UPnP.

Administrative and Monitoring Settings (System Mode) 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.

snmp	*system snmp trap configure <ip address>*	Configure an SNMP agent and community.
	system snmp trap delete <ipaddress>	Delete an SNMP agent.
time	*system time configure*	Configure the system time, date, and NTP servers.
traffic_meter	*system traffic_meter configure*	Configure the WAN traffic meter.

Wireless Settings (Dot11 Mode) Configuration Commands

Enter the **`dot11 ?`** command at the CLI prompt to display the submodes in the dot11 mode. The following table lists the submodes and their commands in alphabetical order:

Table 10. Dot11 mode configuration commands

Submode	Command Name	Purpose
profile	*dot11 profile acl configure <row id >*	Configure an ACL for a specific profile.
	dot11 profile add	Configure a new wireless profile.
	dot11 profile delete <row id>	Delete a wireless profile.
	dot11 profile disable <row id>	Disable a wireless profile.
	dot11 profile enable <row id>	Enable a wireless profile.
	dot11 profile edit <row id>	Configure an existing wireless profile.
	dot11 profile wps configure	Configure Wi-Fi Protected Setup™ (WPS).
radio	*dot11 radio advanced configure*	Configure advanced radio settings.
	dot11 radio configure	Configure basic radio settings.

Table 11. 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.
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.
	vpn sslvpn portal_layouts edit <row id>	Configure an existing SSL VPN portal layout.

sslvpn (continued)	*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.
	vpn sslvpn users users ip_policies configure <row id>	Configure source IP addresses from which a user is either allowed or denied access.

(continued)	*vpn sslvpn users users login_policies <row id>*	Configure the login policy for a user.

3 Net Mode Configuration Commands

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

IMPORTANT:

After you have issued a command that includes the word `configure`, add, or `edit`, you need to save (or cancel) your changes. For more information, see *Save Commands* on page 13.

This command configures the MTU, port speed, and MAC address of the wireless VPN firewall. After you have issued the **net wan port_setup configure** command, you enter the net-config [port_setup] mode, and then you can configure the MTU, port speed, and MAC address.

Step 1

Format **net wan port_setup configure**

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_Half_Duplex** | **1000_BaseT_Full_Duplex**}
mac_type {**Use-Default-Mac** | **Use-This-Computers-Mac** | **Use-This-Mac** {**mac_address** <*mac address*>}}

Mode net-config [port_setup]

Keyword	Associated Keyword to Select or Parameter to Type	Description
def_mtu	**Default** or **Custom**	Specifies whether the default MTU or a custom MTU is used. If you select **Custom**, you need to 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 have configured IPv4 mode, type a number between 68 and 1500 bytes. • If you have configured IPv4/IPv6 mode, type a number between 1280 and 1500 bytes.
port_speed	**Auto_Sense**, **10_BaseT_Half_Duplex**, **10_BaseT_Full_Duplex**, **100_BaseT_Half_Duplex**, **100_BaseT_Full_Duplex**, **1000_BaseT_Half_Duplex**, or **1000_BaseT_Full_Duplex**	Specifies the port speed and duplex mode of the WAN port. The keywords are self-explanatory.

	or **Use-This-Mac**	If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, select either **Use-This-Computers-Mac** or select **Use-This-Mac**. If you select the latter keyword, you need to 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**.

Command example:

```
FVS318N> net wan port_setup configure
net-config[port_setup]> def_mtu Custom
net-config[port_setup]> mtu_size 1498
net-config[port_setup]> port_speed 1000_BaseT_Full_Duplex
net-config[port_setup]> mac_type Use-This-Computers-Mac
net-config[port_setup]> save
```

Related show command: *show net wan port_setup*

This command configures the mode of IPv4 routing between the WAN interface and LAN interfaces. After you have issued 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:

```
FVS318N> 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 wan1 ipv4 configure

This command configures the IPv4 settings of the WAN interface. After you have issued the **net wan wan1 ipv4 configure** command, you enter the net-config [wan1-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

Mode net

Step 2 **Format** **isp_connection_type** {**STATIC** | **DHCPC** | **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** {**idletime** <*minutes*>}}
pppoe connection_reset {**N** | **Y** {**reset_hour** <*hour*>} {**reset_min** <*minutes*>} {**delay_in_reset** <*seconds*>}}
pppoe get_ip_dynamically {**Y** | **N** {**static_ip** <*ipaddress*>} {**subnet_mask** <*subnet mask*>}}
pppoe get_dns_from_isp {**Y** | **N** {**primary_dns** <*ipaddress*>} [**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_dns_from_isp {**Y** | **N** {**pptp primary_dns** <*ipaddress*>} [**pptp secondary_dns** <*ipaddress*>]}

Mode net-config [wan1-ipv4]

		• **STATIC**. Configure the keywords and parameters in the STATIC section of this table. • **DHCPC**. Configure the keywords and parameters in the DHCPC section of this table. • **PPPoE**. Configure the keywords and parameters in the PPPoE section of this table. • **PPTP**. Configure the keywords and parameters in the PPTP section of this table. You need to confirm your selection by typing **Yes** (that is, **Yes**, and not just **Y**).
	Yes	
isp_login_required	**Y** or **N**	Enables or disables the ISP login requirement if the type of ISP connection is PPPoE or PPTP.
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 (These keywords consist of two separate words)		
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.

		the ISP. If you select **N**, you need to 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 (These keywords consist of two separate words)		
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 need to 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 connection_reset	**Y** or **N**	Specifies whether or not the PPPoE connection is automatically reset. If it is reset, you need to issue the **reset_hour** and **reset_min** keywords and enter the hour and minutes after which the connection is reset. You also need to issue the **delay_in_reset** keyword and enter the number of seconds of delay.
pppoe reset_hour	*hour*	The hour at which the PPPoE connection is reset.
pppoe reset_min	*minutes*	The minutes at which the PPPoE connection is reset.

		PPPoE connection attempt is made.
pppoe get_ip_dynamically	**Y** or **N**	Specifies whether or not the IP address is dynamically received from the ISP. If it is not, you need to issue the **static_ip** keyword and enter the static IP address, and issue the **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.
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 need to 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 (These keywords consist of two separate words)		
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 need to issue the **pptp idle_time** keyword and enter the idle time-out period.

		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_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 need to 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.

Command example:

```
FVS318N> net wan wan1 ipv4 configure
net-config[wan1-ipv4]> isp_connection_type DHCPC
net-config[wan1-ipv4]> dhcpc client_identifier Y
net-config[wan1-ipv4]> dhcpc get_dns_from_isp N
net-config[wan1-ipv4]> dhcpc primary_dns 10.124.56.118
net-config[wan1-ipv4]> dhcpc secondary_dns 10.124.56.132
net-config[wan1-ipv4]> save
```

Related show commands: *show net wan wan1 ipv4 setup* **and** *show net wan wan1 ipv4 status*

This command configures the IPv6 settings of the WAN interface. After you have issued the **net wan wan1 ipv6 configure** command, you enter the net-config [wan1-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 wan1 ipv6 configure**

Mode net

Step 2 **Format** **isp type** {**static** | **dhcpc**}

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**}

Mode net-config [wan1-ipv6]

Keyword (consists of two separate words)	Associated Keyword to Select or Parameter to Type	Description
isp type	**static** or **dhcpc**	Specifies the type of ISP connection: • **static**. Configure the keywords and parameters in the Static section of this table. • **dhcpc**. Configure the keywords and parameters in the DHCPC 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.

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.
dhcpc 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.

Command example:

```
FVS318N> net wan wan1 ipv6 configure
net-config[wan1-ipv6]> isp type dhcpc
net-config[wan1-ipv6]> dhcpc stateless_mode_enable StatelessAddrAutoConfig
net-config[wan1-ipv6]> dhcpc prefix_delegation_enable Y
net-config[wan1-ipv6]> save
```

Related show commands: *show net wan wan1 ipv6 setup* **and** *show net wan wan1 ipv6 status*

---

net ipv6 ipmode configure

This command configures the IPv6 routing mode. After you have issued 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 IPv6 mode causes the wireless 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]

Command example:

```
FVS318N> net ipv6 ipmode configure
net-config[mode]> ip_type IPv4/IPv6
net-config[mode]> save
```

Related show command: *show net ipv6 ipmode setup*

---

net siit configure

This command enables and configures Stateless IP/ICMP Translation (SIIT). After you have issued 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:

```
SRX5308> net siit configure
net-config[siit]> enable Y
net-config[siit]> ipv4_address 192.168.4.118
net-config[siit]> save
```

Related show command: *show net siit setup*

This command configures a new ISATAP tunnel. After you have issued 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 configure an ISATAP tunnel, you first need to set the IP mode to IPv4/IPv6 (see *net ipv6 ipmode configure*).

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 wireless VPN firewall. The endpoint can be the LAN interface or a specific LAN IPv4 address. If you select **Other_IP**, you also need to 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:

```
FVS318N> 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*

Step 1	**Format**	**net ipv6_tunnel isatap edit** *<row id>*
	Mode	net
Step 2	**Format**	**subnet_prefix** *<subnet prefix>*
	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.

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:** To delete an ISATAP tunnel, you first need to set the IP mode to IPv4/IPv6 (see *net ipv6 ipmode configure*).

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-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:

```
FVS318N> 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*

This command enables, configures, or disables Dynamic DNS (DDNS) service. After you have issued 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.

Step 1	**Format**	**net ddns configure**
	Mode	net
Step 2	**Format**	**enable** {**Disable** | **DynDNS** | **TZO** | **DNS_Oray** | **3322_DDNS**} **hostname** <*host name*> **username** <*user name*> **password** <*password*> **wild_flag_enable** {**Y** | **N**} **time_update_enable** {**Y** | **N**}
	Mode	net-config [ddns]

Keyword	Associated Keyword to Select or Parameter to Type	Description
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 had first enabled the service. The other keywords represent DDNS service providers and are self-explanatory.
hostname	*host name*	Configures a host name (string) for a DDNS server.
username	*user name*	Configures a user name (string) for a DDNS server.
password	*password*	Configures a password (string) for a DDNS server.
wild_flag_enable	**Y** or **N**	Enables or disables the use of wildcards for DDNS.
time_update_enable	**Y** or **N**	Enables or disables the automatic update of the DDNS service after 30 days.

Command example:

```
FVS318N> net ddns configure
net-config[ddns]> enable DynDNS
net-config[ddns]> hostname adminnetgear.dyndns.org
net-config[ddns]> username jaybrown
net-config[ddns]> password 4hg!RA278s
net-config[ddns]> wild_flag_enable N
net-config[ddns]> time_update_enable Y
net-config[ddns]> save
```

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 have issued 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}] | [port 5 {Y | N}] |
   [port 6 {Y | N}] | [port 7 {Y | N}] | [port 8 {Y | N}]}
static address <ipaddress>
static subnet_mask <subnet mask>
dhcp mode {None | DHCP-Server | DHCP-Relay}
proxy dns_enable {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>

inter_vlan_routing {Y | N}
```

Mode net-config [lan-ipv4]

port_membership port1	**Y** or **N**	Specifies whether or not the port is a member of the VLAN. You need to specify each port individually.
port_membership port2		
port_membership port3		
port_membership port4		
port_membership port5		
port_membership port6		
port_membership port7		
port_membership port8		
static address	*ipaddress*	The static IPv4 address for the VLAN.
static subnet_mask	*subnet mask*	The IPv4 subnet mask for the VLAN profile.
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 in the DHCP server section of this table. • **DHCP-Relay**. Configure the keywords and parameters 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.
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.

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:

```
FVS318N> 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 4 Y
net-config[lan-ipv4]> port_membership port 5 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 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*

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 have issued 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.

native-vlan	**Y** or **N**	Enables or disables the default (native) VLAN for this interface.

Command example:

```
FVS318N> 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 {interface name | all}*

---

net lan ipv4 default_vlan

This command configures the default VLAN for each port. After you have issued 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>* **port5** *<vlan name>* **port6** *<vlan name>* **port7** *<vlan name>* **port8** *<vlan name>*
	Mode	net-config [lan-ipv4-defvlan]

port2	*vlan name*	Specifies the default VLAN name. You need to specify the name for each port individually.
port3		
port4		
port5		
port6		
port7		
port8		

Command example:

```
FVS318N> 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]> port5 Marketing
net-config[lan-ipv4-defvlan]> port6 Sales
net-config[lan-ipv4-defvlan]> port7 Remote
net-config[lan-ipv4-defvlan]> port8 Default
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 have issued 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]

		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 ARP broadcast.

Command example:

```
FVS318N> 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 have issued 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]

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 that needs to be bound to the specified MAC address. The IP address needs to 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 needs to be assigned. **Note:** You can also enter a custom group name that you have specified with the **net lan lan_groups edit** command.
vlan_profile	*vlan name*	The name of the VLAN to which the computer or device needs to be assigned.

Command example:

```
FVS318N> 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*

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 have issued 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:

```
FVS318N> 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*

---

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*

This command configures the IPv6 LAN address settings and DHCPv6. After you have issued 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**	Specifies whether or not DHCPv6 is enabled. If you enable DHCPv6, you also need to issue the **dhcp** mode keyword and its associated keyword.
dhcp mode	**Stateless** or **Stateful**	Specifies the DHCPv6 mode (stateless or stateful).
dhcp prefix_delegation_enable	**Y** or **N**	Specifies whether or not prefix delegation is enabled.
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.

	useEnteredDns	**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.
dhcp secondary_dns	*ipv6-address*	The IPv6 address for the secondary DNS server in the DHCP configuration.
dhcp rebind_time	*seconds*	The lease time in seconds (integer), from 0 to 604800 seconds.

Command example:

```
FVS318N> 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 prefix_delegation_enable N
net-config[lan-ipv6]> dhcp mode Stateless
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 configure

This command configures a new IPv6 DHCP address pool for the LAN. After you have issued the **net lan ipv6 pool configure** 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 configure**
	Mode	net
Step 2	**Format**	**start_address** <*ipv6-address*> **end_address** <*ipv6-address*> **prefix_value** <*prefix length*>
	Mode	net-config [lan-ipv6-pool]

end_address	*ipv6-address*	The end address of the IPv6 address pool.
prefix_value	*prefix length*	The prefix length for the IPv6 address pool.

Command example:

```
FVS318N> net lan ipv6 pool configure
net-config[lan-ipv6-pool]> start_address 2001::1025
net-config[lan-ipv6-pool]> end_address 2001::1030
net-config[lan-ipv6-pool]> prefix_value 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 have issued 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_value	*prefix length*	The prefix length for the IPv6 address pool.

Related show command: *show net lan ipv6 setup*

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 have issued 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:

```
FVS318N> 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*

---

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 have issued 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

preference {**Low** | **Medium** | **High**}
mtu <*number*>
life_time <*seconds*>

Mode net-config [radvd-lan]

Keyword (might consist of two separate words)	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 wireless 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:

```
FVS318N> net radvd configure lan
net-config[radvd-lan]> enable Y
net-config[radvd-lan]> mode Unsolicited-Multicast
net-config[radvd-lan]> interval 60
```

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 have issued 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`** {**`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 need to issue the **`sla_id`** keyword and specify the interface ID. • **Global-Local-ISATAP**. The prefix is for a global, local, or ISATAP address. This needs to be a global prefix, not the site-local or link-local prefix. You need to issue the **`prefix_address`** and **`prefix_length`** keywords and associated parameters.
`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.

		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:

```
FVS318N> net radvd pool lan add
net-config[radvd-pool-lan]> prefix_type 6To4
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 have issued 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** {**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]

		• **6To4**. The prefix is for a 6to4 address. You need to issue the **sla_id** keyword and specify the interface ID. • **Global-Local-ISATAP**. The prefix is for a global, local, or ISATAP address. This needs to be a global prefix, not the site-local or link-local prefix. You need to issue the **prefix_address** and **prefix_length** keywords and associated parameters.
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 a RADVD 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*

[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 IPv6 prefix.

Command example:

```
SRX5308> 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 have issued 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]

prefix_length	*prefix_length*	The prefix length for 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*

This command enables, configures, or disables the IPv4 DMZ. After you have issued 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.

	DHCP-Relay	• **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 DHCP relay gateway server.

Command example:

```
FVS318N> 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
```

IPv6 DMZ Setup Commands

net dmz ipv6 configure

This command enables, configures, or disables the IPv6 DMZ. After you have issued 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**}
ip_address <*ipv6-address*>
prefix_length <*prefix length*>

dhcp_enable {**N** | **Y** {**dhcp_mode** {**Stateless** | **Stateful**}}}
domain name <*domain-name*>
server_preference <*number*>
dns_server_option {**useDnsProxy** | **useDnsFromISP** | **useEnteredDns** {**primary_dns_server** <*ipv6-address*>} [**secondary_dns_server** <*ipv6-address*>]}
lease_time <*seconds*>

Mode net-config [dmz-ipv6]

Keyword	Associated Keyword to Select or Parameter to Type	Description
enable_dmz	**Y** or **N**	Enables or disables the DMZ.
ip_address	*ipv6-address*	The IPv6 address of the DMZ port.
prefix_length	*prefix length*	The prefix length (integer) for the DMZ port.
DHCPv6 server		
dhcp_enable	**Y** or **N**	Enables or disables the DHCP server for the DMZ.
dhcp_mode	**Stateless** or **Stateful**	Specifies the DHCPv6 mode (Stateless or Stateful).
domain_name	*domain name*	The server domain name (string) for the DHCP server.

dns_server_option	**useDnsProxy, useDnsFromISP**, or **useEnteredDns**	Specifies the DNS server type. If you select **useEnteredDns**, you also need to issue the **primary_dns_server** keyword and associated parameter. The **secondary_dns_server** keyword and associated parameter are optional.
primary_dns_server	*ipv6-address*	The IPv6 address for the primary DNS server in the DMZ configuration.
secondary_dns_server	*ipv6-address*	The IPv6 address of the secondary DNS server in the DMZ configuration.
lease_time	*seconds*	The duration in seconds for which an IP address is leased.

Command example:

```
FVS318N> net dmz ipv6 configure
net-config[dmz-ipv6]> enable_dmz Y
net-config[dmz-ipv6]> ip_address 2001:176::1
net-config[dmz-ipv6]> prefix_length 64
net-config[dmz-ipv6]> dhcp_enable Y
net-config[dmz-ipv6]> dhcp_mode Stateful
net-config[dmz-ipv6]> domain_name netgear.com
net-config[dmz-ipv6]> server_preference 210
net-config[dmz-ipv6]> dns_server_option useDnsProxy
net-config[dmz-ipv6]> 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 have issued 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 the order that you prefer.

Step 1	**Format**	**net dmz ipv6 pool configure** *<ipv6-address>*
	Mode	net

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

Command example:

```
FVS318N> net dmz ipv6 pool configure 2001::1100
net-config[dmz-ipv6-pool]> ending_ip_address 2001::1120
net-config[dmz-ipv6-pool]> prefix_value 56
net-config[dmz-ipv6-pool]> save
```

Related show command: *show net dmz ipv6 setup*

---

net dmz pool ipv6 delete < ipv6 address>

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

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

Related show command: *show net radvd dmz 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 have issued 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

preference {**Low** | **Medium** | **High**}
mtu <*number*>
life_time <*seconds*>

Mode net-config [radvd-dmz]

Keyword (might consist of two separate words)	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 wireless 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:

```
FVS318N> net radvd configure dmz
net-config[radvd-dmz]> enable Y
net-config[radvd-dmz]> mode Unicast-Only
net-config[radvd-dmz]> flags Managed
```

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 have issued 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`** {**`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 need to issue the **`sla_id`** keyword and specify the interface ID. • **`Global-Local-ISATAP`**. The prefix is for a global, local, or ISATAP address. This needs to be a global prefix, not the site-local or link-local prefix. You need to issue the **`prefix_address`** and **`prefix_length`** keywords and associated parameters.
`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.

		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:

```
FVS318N> 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 have issued 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** {**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]

		• **6To4**. The prefix is for a 6to4 address. You need to issue the **sla_id** keyword and specify the interface ID. • **Global-Local-ISATAP**. The prefix is for a global, local, or ISATAP address. This needs to be a global prefix, not the site-local or link-local prefix. You need to issue the **prefix_address** and **prefix_length** keywords and associated parameters.
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*

This command configures an IPv4 static route. After you have issued 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**}
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 or not the route 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 is applied. The DMZ, LAN, and WAN interfaces are self-explanatory. If you select the **custom_vlan** keyword, you also need to specify the VLAN name.
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:

```
FVS318N> 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
```

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 have issued 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

```
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.
direction	**None**, **In-only**, **Out-only**, or **Both**.	Specifies the RIP direction.
version	**Disabled**, **Rip1**, **Rip2B**, or **Rip2M**	Specifies the RIP version.

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:

```
FVS318N> 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 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*

This command configures an IPv6 static route. After you have issued 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 {**Dedicated-WAN** | **LAN** | **Sit0-WAN1**}
metric <*number*>

Mode net-config [static-routing-ipv6]

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.
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	**Dedicated-WAN**, **LAN**, or **Sit0-WAN1**	Specifies the physical or virtual network interface through which the route is accessible: • **Dedicated-WAN**. The dedicated WAN interface. • **LAN**. A LAN interface. • **Sit0-WAN1**. The 6to4-WAN 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.

```
net-config[static-routing-ipv6]> interface Dedicated-WAN
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:

IMPORTANT:

After you have issued a command that includes the word `configure`, add, or `edit`, you need to save (or cancel) your changes. For more information, see *Save Commands* on page 13.

This command configures a new firewall custom service. After you have issued 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*>}} **qos_priority** {**Normal-Service** | **Minimize-Cost** | **Maximize-Reliability** | **Maximize-Throughput** | **Minimize-Delay**}
	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 0 to 65535.
finish_port	*number*	For TCP and UDP, the end port number (integer) of the range used by the destination user. Valid numbers are from 0 to 65535.
icmp_type	*number*	The ICMP type (integer) used by the destination user.
qos_priority	**Normal-Service**, **Minimize-Cost**, **Maximize-Reliability**, **Maximize-Throughput**, or **Minimize-Delay**	Specifies the type of QoS priority that applies to the service. The keywords are self-explanatory.

Command example:

```
FVS318N> 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]> qos_priority Minimize-Delay
security-config[custom-service]> save
```

This command configures an existing firewall custom service. After you have issued 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>}}
qos_priority {Normal-Service | Minimize-Cost |
   Maximize-Reliability | Maximize-Throughput | Minimize-Delay}
```

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 0 to 65535.
`finish_port`	*number*	For TCP and UDP, the end port number (integer) of the range used by the destination user. Valid numbers are from 0 to 65535.
`icmp_type`	*number*	The ICMP type (integer) used by the destination user.
`qos_priority`	**`Normal-Service`**, **`Minimize-Cost`**, **`Maximize-Reliability`**, **`Maximize-Throughput`**, or **`Minimize-Delay`**	Specifies the type of QoS priority that applies to the service. The keywords are self-explanatory.

Related show command: *show security services setup*

Mode security

Related show command: *show security services setup*

Security Schedules Commands

security schedules edit {1 | 2 | 3}

This command configures one of the three security schedules. After you have issued 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 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 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.
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:

```
FVS318N> 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*

This command configures a new IPv4 LAN WAN outbound firewall rule. After you have issued 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 can 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** {**ANY** | **SINGLE_ADDRESS** {**wan_user_start_ip** <*ipaddress*>} | **ADDRESS_RANGE** {**wan_user_start_ip** <*ipaddress*>} {**wan_user_end_ip** <*ipaddress*>}} **qos_priority** {**Normal-Service** | **Minimize-Cost** | **Maximize-Reliability** | **Maximize-Throughput** | **Minimize-Delay**} **log** {**NEVER** | **ALWAYS**} **bandwidth_profile** <*profile name*> **nat_ip type** {**WAN_INTERFACE_ADDRESS** | **SINGLE_ADDRESS** {**address** <*ipaddress*>}}
	Mode	security-config [firewall-ipv4-lan-wan-outbound]

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**, or **SIP-UDP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you have configured 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 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*	There are two options: • 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**.

		keywords are set to **ADDRESS_RANGE**.
lan_users group_wise	*group name*	The name of the LAN group. The group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specified with the *net lan lan_groups edit <row id> <new group name>* command. The **address_wise** and **group_wise** keywords are mutually exclusive.
wan_users	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN address.
wan_user_start_ip	*ipaddress*	There are two options: • 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**.
QoS profile, logging, bandwidth profile, and NAT IP address		
qos_priority	**Normal-Service**, **Minimize-Cost**, **Maximize-Reliability**, **Maximize-Throughput**, or **Minimize-Delay**	Specifies the type of QoS that applies to the rule.
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.
bandwidth_profile	*profile name*	The profile that you have configured with the *security bandwidth profile add* command.

		• **WAN_INTERFACE_ADDRESS**. The IP address of the WAN (broadband) interface. • **SINGLE_ADDRESS**. Another IP address, which you need to configure using the **nat_ip address** keywords.
nat_ip address	*ipaddress*	The NAT IP address, if the **nat_ip type** keywords are set to **SINGLE_ADDRESS**.

Command example:

```
FVS318N> security firewall ipv4 add_rule lan_wan outbound
security-config[firewall-ipv4-lan-wan-outbound]> service_name default_services PING
security-config[firewall-ipv4-lan-wan-outbound]> action ALWAYS_ALLOW
security-config[firewall-ipv4-lan-wan-outbound]> lan_users address_wise ANY
security-config[firewall-ipv4-lan-wan-outbound]> wan_users ADDRESS_RANGE
security-config[firewall-ipv4-lan-wan-outbound]> wan_user_start_ip 10.120.114.217
security-config[firewall-ipv4-lan-wan-outbound]> wan_user_end_ip 10.120.114.245
security-config[firewall-ipv4-lan-wan-outbound]> qos_profile Normal-Service
security-config[firewall-ipv4-lan-wan-outbound]> log ALWAYS
security-config[firewall-ipv4-lan-wan-outbound]> nat_ip type WAN_INTERFACE_ADDRESS
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 have issued 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

```
   {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 {ANY | SINGLE_ADDRESS {wan_user_start_ip <ipaddress>}
   | ADDRESS_RANGE {wan_user_start_ip <ipaddress>}
   {wan_user_end_ip <ipaddress>}}

qos_priority {Normal-Service | Minimize-Cost |
   Maximize-Reliability | Maximize-Throughput | Minimize-Delay}
log {NEVER | ALWAYS}
bandwidth_profile <profile name>
nat_ip type {WAN_INTERFACE_ADDRESS | SINGLE_ADDRESS
   {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**, or **SIP-UDP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you have configured with the *security services add* command and to which the firewall rule applies.

	or **ALLOW_BY_SCHEDULE_ELSE_BLOCK**	
schedule	**Schedule1**, **Schedule2**, or **Schedule3**	Specifies the schedule, if any, that is applicable 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*	There are two options: • 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. The group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specified with the *net lan lan_groups edit <row id> <new group name>* command. The **address_wise** and **group_wise** keywords are mutually exclusive.
wan_users	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN address.
wan_user_start_ip	*ipaddress*	There are two options: • 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**.

		ADDRESS_RANGE.
QoS profile, logging, bandwidth profile, and NAT IP address		
qos_priority	**Normal-Service**, **Minimize-Cost**, **Maximize-Reliability**, **Maximize-Throughput**, or **Minimize-Delay**	Specifies the type of QoS that applies to the rule.
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.
bandwidth_profile	*profile name*	The profile that you have configured with the *security bandwidth profile add* command.
nat_ip type	**WAN_INTERFACE_ADDRESS** or **SINGLE_ADDRESS**	Specifies the type of NAT IP address: • **WAN_INTERFACE_ADDRESS**. The IP address of the WAN (broadband) interface. • **SINGLE_ADDRESS**. Another IP address, which you need to configure using the **nat_ip address** keywords.
nat_ip address	*ipaddress*	The NAT IP address, if the **nat_ip type** keywords are set to **SINGLE_ADDRESS**.

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 have issued 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 can you can apply to a rule.

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

{**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 {**WAN** | **OTHERS**
{**wan_destination_ip_address_start** <*ipaddress*>} | **RANGE**
{**wan_destination_ip_address_start** <*ipaddress*>}
{**wan_destination_ip_address_end** <*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_user {**ANY** | **SINGLE_ADDRESS** {**wan_user_start_ip** <*ipaddress*>}
| **ADDRESS_RANGE** {**wan_user_start_ip** <*ipaddress*>}
{**wan_user_end_ip** <*ipaddress*>}}

log {**NEVER** | **ALWAYS**}
bandwidth_profile <*profile name*>

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

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**, or **SIP-UDP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you have configured 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 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*	There are two options: • 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**.
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 port	*number*	The port number (integer) if port forwarding is enabled. Valid numbers are 0 through 65535.
wan_destination_ip_address	**WAN**, **OTHERS**, or **RANGE**	Specifies the type of destination WAN address for an inbound rule: • **WAN**. The default IP address of the WAN (broadband) interface. • **OTHERS**. Another public IP address, which you need to configure by issuing the **wan_destination_ip_address_start** keyword and specifying an IPv4 address. • **RANGE**. A range of public IP addresses, which you need to configure by issuing the **wan_destination_ip_address_start** and **wan_destination_ip_address_end** keywords and specifying IPv4 addresses.
wan_destination_ip_address_start	*ipaddress*	There are two options: • The IP address if the **wan_destination_ip_address** keyword is set to **OTHERS**. • The start IP address if the **wan_destination_ip_address** keyword is set to **RANGE**.
wan_destination_ip_address_end	*ipaddress*	The end IP address if the **wan_destination_ip_address** keyword is set to **RANGE**.
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.

		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. The group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specified with the *net lan lan_groups edit <row id> <new group name>* 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_user	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN address.
wan_user_start_ip	*ipaddress*	There are two options: • 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**.
Logging and bandwidth profile		
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.
bandwidth_profile	*profile name*	The profile that you have configured with the *security bandwidth profile add* command.

```
security-config[firewall-ipv4-lan-wan-inbound]> send_to_lan_server_start_ip 192.168.5.69
security-config[firewall-ipv4-lan-wan-inbound]> wan_destination_ip_address WAN
security-config[firewall-ipv4-lan-wan-inbound]> wan_user ANY
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 have issued 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 {WAN | OTHERS
   {wan_destination_ip_address_start <ipaddress>} | RANGE
   {wan_destination_ip_address_start <ipaddress>}
   {wan_destination_ip_address_end <ipaddress>}}
```

{wan_user_end_ip *<ipaddress>}}*

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**, or **SIP-UDP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you have configured 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.

send_to_lan_server	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of LAN address.
send_to_lan_server_start_ip	*ipaddress*	There are two options: • 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**.
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 65535.
wan_destination_ip_address	**WAN**, **OTHERS**, or **RANGE**	Specifies the type of destination WAN address for an inbound rule: • **WAN**. The default IP address of the WAN (broadband) interface. • **OTHERS**. Another public IP address, which you need to configure by issuing the **wan_destination_ip_address_start** keyword and specifying an IPv4 address. • **RANGE**. A range of public IP addresses, which you need to configure by issuing the **wan_destination_ip_address_start** and **wan_destination_ip_address_end** keywords and specifying IPv4 addresses.
wan_destination_ip_address_start	*ipaddress*	There are two options: • The IP address if the **wan_destination_ip_address** keyword is set to **OTHERS**. • The start IP address if the **wan_destination_ip_address** keyword is set to **RANGE**.

		keyword is set to **RANGE**.
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*	There are two options: • 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. The group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specified with the *net lan lan_groups edit <row id> <new group name>* command. For an inbound rule, this option is available only when the WAN mode is Classical Routing. The **address_wise** and **group_wise** keywords are mutually exclusive.
wan_user	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN address.
wan_user_start_ip	*ipaddress*	There are two options: • 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**.

		ADDRESS_RANGE.
Logging and bandwidth profile		
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.
bandwidth_profile	*profile name*	The profile that you have configured 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 have issued 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 can 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 {ANY | SINGLE_ADDRESS {wan_user_start_ip <ipaddress>}
   | ADDRESS_RANGE {wan_user_start_ip <ipaddress>}
   {wan_user_end_ip <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**, or **SIP-UDP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you have configured 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.
DMZ user addresses and WAN user addresses		
dmz_users	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of DMZ address.

		keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **dan_users** keyword is set to **ADDRESS_RANGE**.
dmz_user_end_ip	*ipaddress*	The end IP address if the **dan_users** keyword is set to **ADDRESS_RANGE**.
wan_users	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN address.
wan_user_start_ip	*ipaddress*	There are two options: • 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**.
QoS profile, logging, and NAT IP address		
qos_priority	**Normal-Service**, **Minimize-Cost**, **Maximize-Reliability**, **Maximize-Throughput**, or **Minimize-Delay**	Specifies the type of QoS that applies to the rule.
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.
nat_ip type	**WAN_INTERFACE_ADDRESS** or **SINGLE_ADDRESS**	Specifies the type of NAT IP address: • **WAN_INTERFACE_ADDRESS**. The IP address of the WAN (broadband) interface. • **SINGLE_ADDRESS**. Another IP address, which you need to configure using the **nat_ip address** keywords.
nat_ip address	*ipaddress*	The NAT IP address, if the **nat_ip type** keywords are set to **SINGLE_ADDRESS**.

```
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 Maximize-Reliability
security-config[firewall-ipv4-dmz-wan-outbound]> log Never
security-config[firewall-ipv4-dmz-wan-outbound]> nat_ip type WAN_INTERFACE_ADDRESS
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 have issued 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 {**ANY** | **SINGLE_ADDRESS** {**wan_user_start_ip** *<ipaddress>*} | **ADDRESS_RANGE** {**wan_user_start_ip** *<ipaddress>*} {**wan_user_end_ip** *<ipaddress>*}}

[**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**, or **SIP-UDP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you have configured 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.
DMZ user addresses and WAN user addresses		
dmz_users	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of DMZ address.

		keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **dan_users** keyword is set to **ADDRESS_RANGE**.
dmz_user_end_ip	*ipaddress*	The end IP address if the **dan_users** keyword is set to **ADDRESS_RANGE**.
wan_users	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN address.
wan_user_start_ip	*ipaddress*	There are two options: • 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**.
QoS profile, logging, and NAT IP address		
qos_priority	**Normal-Service**, **Minimize-Cost**, **Maximize-Reliability**, **Maximize-Throughput**, or **Minimize-Delay**	Specifies the type of QoS that applies to the rule.
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.
nat_ip type	**WAN_INTERFACE_ADDRESS** or **SINGLE_ADDRESS**	Specifies the type of NAT IP address: • **WAN_INTERFACE_ADDRESS**. The IP address of the WAN (broadband) interface. • **SINGLE_ADDRESS**. Another IP address, which you need to configure using the **nat_ip address** keywords.
nat_ip address	*ipaddress*	The NAT IP address, if the **nat_ip type** keywords are set to **SINGLE_ADDRESS**.

security firewall ipv4 add_rule dmz_wan inbound

This command configures a new IPv4 DMZ WAN inbound firewall rule. After you have issued 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 can 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 {**WAN** | **OTHERS**
{**wan_destination_ip_address_start** <*ipaddress*>}

dmz_users {**ANY** | **SINGLE_ADDRESS** {**dmz_user_start_ip** <*ipaddress*>}
| **ADDRESS_RANGE** {**dmz_user_start_ip** <*ipaddress*>}
{**dmz_user_end_ip** <*ipaddress*>}}
wan_users {**ANY** | **SINGLE_ADDRESS** {**wan_user_start_ip** <*ipaddress*>}
| **ADDRESS_RANGE** {**wan_user_start_ip** <*ipaddress*>}
{**wan_user_end_ip** <*ipaddress*>}}

log {**NEVER** | **ALWAYS**}

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

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**, or **SIP-UDP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you have configured 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.
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 65535.

		• **WAN**. The default IP address of the WAN (broadband) interface. • **OTHERS**. Another public IP address, which you need to configure by issuing the **wan_destination_ip_address_start** keyword and specifying an IPv4 address.
wan_destination_ip_address_start	*ipaddress*	The IP address if the **wan_destination_ip_address** keyword is set to **OTHERS**.
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*	There are two options: • 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	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN address.
wan_user_start_ip	*ipaddress*	There are two options: • 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**.
Logging		
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.

```
security-config[firewall-ipv4-lan-wan-inbound]> translate_to_port_number port 4500
security-config[firewall-ipv4-lan-wan-inbound]> wan_destination_ip_address OTHERS
security-config[firewall-ipv4-lan-wan-inbound]> wan_destination_ip_address_start 10.115.97.174
security-config[firewall-ipv4-lan-wan-inbound]> wan_users ANY
security-config[firewall-ipv4-lan-wan-inbound]> log Always
security-config[firewall-ipv4-lan-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 have issued 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 {WAN | OTHERS
   {wan_destination_ip_address_start <ipaddress>}


dmz_users {ANY | SINGLE_ADDRESS {dmz_user_start_ip <ipaddress>}
   | ADDRESS_RANGE {dmz_user_start_ip <ipaddress>}
   {dmz_user_end_ip <ipaddress>}}
wan_users {ANY | SINGLE_ADDRESS {wan_user_start_ip <ipaddress>}
   | ADDRESS_RANGE {wan_user_start_ip <ipaddress>}
   {wan_user_end_ip <ipaddress>}}
```

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**, or **SIP-UDP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you have configured 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.
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 65535.

		• **WAN**. The default IP address of the WAN (broadband) interface. • **OTHERS**. Another public IP address, which you need to configure by issuing the **wan_destination_ip_address_start** keyword and specifying an IPv4 address.
wan_destination_ip_address_start	*ipaddress*	The IP address if the **wan_destination_ip_address** keyword is set to **OTHERS**.
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*	There are two options: • 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	**ANY**, **SINGLE_ADDRESS**, or **ADDRESS_RANGE**	Specifies the type of WAN address.
wan_user_start_ip	*ipaddress*	There are two options: • 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**.
Logging		
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.

security firewall ipv4 add_rule lan_dmz outbound

This command configures a new IPv4 LAN DMZ outbound firewall rule. After you have issued 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 can 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]

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**, or **SIP-UDP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you have configured 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*	There are two options: • 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**.

		keywords are set to **ADDRESS_RANGE**.
lan_users group_wise	*group name*	The name of the LAN group. The group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specified with the *net lan lan_groups edit <row id> <new group name>* 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*	There are two options: • The IP address if the **dmz_users** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **dan_users** keyword is set to **ADDRESS_RANGE**.
dmz_user_end_ip	*ipaddress*	The end IP address if the **dan_users** keyword is set to **ADDRESS_RANGE**.
Logging		
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.

Command example:

```
FVS318N> 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 GROUP3
security-config[firewall-ipv4-lan-dmz-outbound]> dmz_users ADDRESS_RANGE
security-config[firewall-ipv4-lan-dmz-outbound]> dmz_user_start_ip 176.16.2.65
security-config[firewall-ipv4-lan-dmz-outbound]> dmz_user_end_ip 176.16.2.85
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*

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]

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**, or **SIP-UDP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you have configured 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*	There are two options: • 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**.

		keywords are set to **ADDRESS_RANGE**.
lan_users group_wise	*group name*	The name of the LAN group. The group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specified with the *net lan lan_groups edit <row id> <new group name>* 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*	There are two options: • The IP address if the **dmz_users** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **dan_users** keyword is set to **ADDRESS_RANGE**.
dmz_user_end_ip	*ipaddress*	The end IP address if the **dan_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 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 have issued 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

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**, or **SIP-UDP**	Specifies the default service and protocol to which the firewall rule applies.

		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*	There are two options: • 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. The group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specified with the *net lan lan_groups edit <row id> <new group name>* 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.

		keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **dan_users** keyword is set to **ADDRESS_RANGE**.
dmz_user_end_ip	*ipaddress*	The end IP address if the **dan_users** keyword is set to **ADDRESS_RANGE**.
Logging		
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.

Command example:

```
FVS318N> 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 192.168.4.109
security-config[firewall-ipv4-lan-dmz-inbound]> dmz_users SINGLE_ADDRESS
security-config[firewall-ipv4-lan-dmz-inbound]> dmz_user_start_ip 176.16.2.211
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 have issued 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

```
   {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**, or **SIP-UDP**	Specifies the default service and protocol to which the firewall rule applies.
service_name custom_services	*custom service name*	The custom service that you have configured 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.

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*	There are two options: • 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. The group name is either a default name (Group1, Group2, Group3, and so on) or a custom name that you specified with the *net lan lan_groups edit <row id> <new group name>* 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*	There are two options: • The IP address if the **dmz_users** keyword is set to **SINGLE_ADDRESS**. • The start IP address if the **dan_users** keyword is set to **ADDRESS_RANGE**.
dmz_user_end_ip	*ipaddress*	The end IP address if the **dan_users** keyword is set to **ADDRESS_RANGE**.
Logging		
log	**NEVER** or **ALWAYS**	Specifies whether logging is disabled or enabled.

IPv4 General Firewall Commands

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

Mode	security

Related show command: *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

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 have issued 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

```
   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.

	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**, or **SIP-UDP**	applies.
service_name custom_services	*custom service name*	The custom service that you have configured 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**	The type of source address.
source_start_address	*ipv6-address*	There are two options: • 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**.
source_end_address	*ipv6-address*	The end IPv6 address if the **source_address_type** keyword is set to **ADDRESS_RANGE**.

destination_start_address	*ipv6-address*	There are two options: • 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:

```
FVS318N> 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-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.

	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**, or **SIP-UDP**	applies.
service_name custom_services	*custom service name*	The custom service that you have configured 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*	There are two options: • 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**.
source_end_address	*ipv6-address*	The end IPv6 address if the **source_address_type** keyword is set to **ADDRESS_RANGE**.

destination_start_address	*ipv6-address*	There are two options: • 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*

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*

This command configures ipv4 WAN and LAN security attack checks. After you have issued 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** {**Y** | **N**} **enable_stealth_mode** {**Y** | **N**} **block_tcp_flood** {**Y** | **N**} **block_udp_flood** {**Y** | **N**} **disable_ping_reply_on_lan** {**Y** | **N**}
	Mode	security-config [attack-checks-ipv4]

Keyword	Associated Keyword to Select	Description
WAN security checks		
respond_to_ping_on_internet_ports	**Y** or **N**	Enables or disables the response to a ping from the WAN port.
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.
disable_ping_reply_on_lan	**Y** or **N**	Enables or disables ping replies from LAN ports.

Command example:

```
FVS318N> security firewall attack_checks configure ipv4
security-config[attack-checks-ipv4]> respond_to_ping_on_internet_ports 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
```

This command enables or disables multicast pass-through by enabling or disabling the IGMP proxy for IPv4 traffic. After you have issued the **`security firewall attack_checks igmp configure`** command, you enter the security-config [igmp] mode, and then you can enable or disable the IGMP proxy.

Step 1	**Format**	**`security firewall attack_checks igmp configure`**
	Mode	security
Step 2	**Format**	**`enable_igmp_proxy {Y | N}`**
	Mode	security-config [igmp]

Related show command: *show security firewall attack_checks igmp*

---

security firewall attack_checks jumboframe configure

This command enables or disables jumbo frames for IPv4 traffic. After you have issued the **`security firewall attack_checks jumboframe configure`** command, you enter the security-advanced-config [jumbo-frame] mode, and then you can enable or disable jumbo frames.

Step 1	**Format**	**`security firewall attack_checks jumboframe configure`**
	Mode	security
Step 2	**Format**	**`enable_jumboframe {Y | N}`**
	Mode	security-config [jumbo-frame]

Related show command: *show security firewall attack_checks jumboframe*

---

security firewall attack_checks vpn_passthrough configure

This command configures VPN pass-through for IPv4 traffic. After you have issued 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

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:

```
FVS318N> 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 have issued 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** {**Y** | **N**} **vpn_ipsec_passthrough** {**Y** | **N**}
	Mode	security-config [attack-checks-ipv6]

Keyword	Associated Keyword to Select	Description
respond_to_ping_on_internet_ports	**Y** or **N**	Enables or disables the response to a ping from the WAN port.
vpn_ipsec_passthrough	**Y** or **N**	Enables or disables IPSec VPN traffic that is initiated from the LAN to reach the WAN, irrespective of the default firewall outbound policy and custom firewall rules.

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

Session Limit, Time-Out, and Advanced Commands

security firewall session_limit configure

This command configures global session limits. After you have issued 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`**} **`conn_limit_type`** {**`Percentage_Of_MaxSessions`** | **`Number_Of_Sessions`**} **`user_limit`** <*number*>
	Mode	security-config [session-limit]

Keyword	Associated Keyword to Select or Parameter to Type	Description
`enable`	**`Y`** or **`N`**	Enables or disables session limits.
`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 wireless 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 wireless VPN firewall or an absolute number of maximum sessions.

```
security-config[session-limit]> user_limit 80
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 have issued 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*	The TCP session timeout period (integer) in seconds.
`udp_session_timeout`	*seconds*	The UDP session timeout period (integer) in seconds.
`icmp_session_timeout`	*seconds*	The ICMP session timeout period (integer) in seconds.

Command example:

```
FVS318N> security firewall session_settings configure
security-config[session-settings]> tcp_session_timeout 3600
security-config[session-settings]> udp_session_timeout 180
security-config[session-settings]> icmp_session_timeout 120
security-config[session-settings]> save
```

Related show command: *show security firewall session_settings*

---

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:

```
FVS318N> security firewall advanced algs
security-config[firewall-alg]> Sip N
security-config[firewall-alg]> save
```

Related show command: *show security firewall advanced algs*

This command configures the source MAC address filter. After you have issued 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 or Parameter to Type	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:

```
FVS318N> 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 have issued 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]

Command example:

```
FVS318N> 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 have issued 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]

mac_address	*mac address*	The MAC address to which the IP/MAC binding rule is applied.
ip_version	**IPv4** or **IPv6**	Specifies the type of IP address to which the IP/MAC binding rule is applied: • **IPv4**. You need to issue the **ip_address** keyword and specify an IPv4 address. • **IPv6**. You need to issue the **ip_address6** keyword and specify an IPv6 address.
ip_address	*ipaddress*	The IPv4 address to which the IP/MAC binding rule is applied.
ip_address6	*ipv6-address*	The IPv6 address to which the IP/MAC binding rule is applied.
log_dropped_packets	**Y** or **N**	Enables or disables logging for the IP/MAC binding rule.

Command example:

```
FVS318N> security address_filter ip_or_mac_binding add
security-config[ip-or-mac-binding]> name Rule1
security-config[ip-or-mac-binding]> mac_address 00:aa:23:be:03:a1
security-config[ip-or-mac-binding]> ip_version IPv4
security-config[ip-or-mac-binding]> ip_address 192.168.10.153
security-config[ip-or-mac-binding]> log_dropped_packets Y
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 have issued 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

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 is applied.
ip_version	**IPv4** or **IPv6**	Specifies the type of IP address to which the IP/MAC binding rule is applied: • **IPv4**. You need to issue the **ip_address** keyword and specify an IPv4 address. • **IPv6**. You need to issue the **ip_address6** keyword and specify an IPv6 address.
ip_address	*ipaddress*	The IPv4 address to which the IP/MAC binding rule is applied.
ip_address6	*ipv6-address*	The IPv6 address to which the IP/MAC binding rule is applied.
log_dropped_packets	**Y** or **N**	Enables or disables 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*

---

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 or IP/MAC Binding violations.

Command example:

```
FVS318N> 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*

This command configures a new port triggering rule. After you have issued 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 0 to 65535.
outgoing_end_port	*number*	The end port number (integer) of the outgoing traffic range. Valid numbers are from 0 to 65535.
incoming_start_port	*number*	The start port number (integer) of the incoming traffic range. Valid numbers are from 0 to 65535.
incoming_end_port	*number*	The end port number (integer) of the incoming traffic range. Valid numbers are from 0 to 65535.

Command example:

```
FVS318N> security porttriggering_rules add
security-config[porttriggering-rules]> name AccInq
security-config[porttriggering-rules]> enable_rule Y
security-config[porttriggering-rules]> protocol TCP
security-config[porttriggering-rules]> outgoing_start_port 20020
security-config[porttriggering-rules]> outgoing_end_port 20022
```

Related show command: *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 have issued 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 0 to 65535.
outgoing_end_port	*number*	The end port number (integer) of the outgoing traffic range. Valid numbers are from 0 to 65535.
incoming_start_port	*number*	The start port number (integer) of the incoming traffic range. Valid numbers are from 0 to 65535.
incoming_end_port	*number*	The end port number (integer) of the incoming traffic range. Valid numbers are from 0 to 65535.

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 command: *show security porttriggering_rules setup* **and** *show security porttriggering_rules status*

UPnP Command

security upnp configure

This command configures Universal Plug and Play (UPnP). After you have issued 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 86400 seconds.
`advertisement time_to_live`	*number*	The advertisement time-to-live period in hops, from 1 to 255 hops.

```
security-config[upnp]> advertisement time_to_live 6
security-config[upnp]> save
```

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

Bandwidth Profile Commands

security bandwidth profile add

This command configures a new bandwidth profile. After you have issued 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** | **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.
inbound_minimum_rate	*kbps*	The minimum inbound bandwidth in kbps (0 to 100000) provided to the group or individual user.
inbound_maximum_rate	*kbps*	The maximum inbound bandwidth in kbps (110 to 100000) provided to the group or individual user.
outbound_minimum_rate	*kbps*	The minimum outbound bandwidth in kbps (0 to 100000) provided to the group or individual user.

		user.
is_group	**Individual** or **Group**	Specifies the type for the bandwidth profile: • **Individual**. The profile applies to an individual user. • **Group**. The profile applies to a group.

Command example:

```
FVS318N> security bandwidth profile add
security-config[bandwidth-profile]> name BW_Sales
security-config[bandwidth-profile]> direction Both _Directions
security-config[bandwidth-profile]> inbound_minimum_rate 1000
security-config[bandwidth-profile]> inbound_maximum_rate 10000
security-config[bandwidth-profile]> outbound_minimum_rate 1000
security-config[bandwidth-profile]> outbound_maximum_rate 10000
security-config[bandwidth-profile]> is_group Group
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 have issued 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** | **Group**}
	Mode	security-config [bandwidth-profile]

inbound_minimum_rate	*kbps*	The minimum inbound bandwidth in kbps (0 to 100000) provided to the group or individual user.
inbound_maximum_rate	*kbps*	The maximum inbound bandwidth in kbps (110 to 100000) provided to the group or individual user.
outbound_minimum_rate	*kbps*	The minimum outbound bandwidth in kbps (0 to 100000) provided to the group or individual user.
outbound_maximum_rate	*kbps*	The maximum outbound bandwidth in kbps (110 to 100000) 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. • **Group**. The profile applies to a group.

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*

This command globally enables or disables content filtering and configures web components. After you have issued 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:

```
FVS318N> 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*

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	Associated Keyword to Select	Description
group all	**Y**	Enables content filtering for all groups.
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:

```
FVS318N> 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
```

This command removes content filtering from selected groups or from all groups. After you have issued 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	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:

```
FVS318N> 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
```

This command configures a new blocked keyword for content filtering. After you have issued 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) that needs to be blocked.

Command example:

```
FVS318N> 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 have issued 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]

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 have issued 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 that needs to be blocked.

Command example:

```
FVS318N> 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
```

This command configures an existing trusted domain for content filtering. After you have issued 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 that needs 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*

---

5 System Mode Configuration Commands

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*

IMPORTANT:

After you have issued a command that includes the word `configure`, add, or `edit`, you need to save (or cancel) your changes. For more information, see *Save Commands* on page 13.

This command configures remote management over HTTPS. After you have issued 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**	Enables or disables remote management over HTTPS for an IPv4 connection.

		You do not need to configure any IP address. • **IP_Range**. Enables access to a range of IP addresses. You also need to configure the **from_address** and **end_address** keywords and associated parameters. • **To_this_PC_only**. Enables access to a single IP address. You also need to configure the **only_this_pc_ip** keyword and associated parameter.
from_address	*ipaddress*	The start IP address if you have set the **access_type** keyword to **IP_Range**.
end_address	*ipaddress*	The end IP address if you have set the **access_type** keyword to **IP_Range**.
only_this_pc_ip	*ipaddress*	The single IP address if you have 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**	Enables or disables 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 need to configure the **from_address6** and **end_address6** keywords and associated parameters. • **To_this_PC_only**. Enables access to a single IP address. You also need to configure the **only_this_pc_ipv6** keyword and associated parameter.
from_address6	*ipv6-address*	The start IP address if you have set the **access_type6** keyword to **IP_Range**.
end_address6	*ipv6-address*	The end IP address if you have set the **access_type6** keyword to **IP_Range**.
only_this_pc_ipv6	*ipaddress*	The single IP address if you have set the **access_type6** keyword to **To_this_PC_only**.
port	*number*	The number of the port through which access is allowed.

```
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 have issued 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		

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 need to configure the **from_address** and **to_address** keywords and associated parameters. • **To_this_PC_only**. Enables access to a single IP address. You also need to configure the **only_this_pc_ip** keyword and associated parameter.
from_address	*ipaddress*	The start IP address if you have set the **access_type** keyword to **IP_Range**.
to_address	*ipaddress*	The end IP address if you have set the **access_type** keyword to **IP_Range**.
only_this_pc_ip	*ipaddress*	The single IP address if you have set the **access_type** keyword to **To_this_PC_only**.
Telnet over an IPv6 connection		
enable_ipv6	**Y** or **N**	Enables or disables 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 need to configure the **from_address6** and **to_address6** keywords and associated parameters. • **To_this_PC_only**. Enables access to a single IP address. You also need to configure the **only_this_pc_ip6** keyword and associated parameter.
from_address6	*ipv6-address*	The start IP address if you have set the **access_type6** keyword to **IP_Range**.
to_address6	*ipv6-address*	The end IP address if you have set the **access_type6** keyword to **IP_Range**.
only_this_pc_ip6	*ipaddress*	The single IP address if you have set the **access_type6** keyword to **To_this_PC_only**.

Command example:

```
FVS318N> system remote_management telnet configure
system-config[telnet]> ip_version IPv6
```

Related show command: *show system remote_management setup*

SNMP Commands

system snmp trap configure <ip address>

This command configures a new or existing SNMP agent to which trap information is forwarded. After you have issued 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**	**`subnet_mask`** *<subnet mask>* **`port`** *<number>* **`community`** *<community name>* **`agent`** *<ipaddress>*
	Mode	system-config [snmp-trap]

Keyword	Associated Parameter to Type	Description
`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.
`port`	*number*	The SNMP port (integer) to which the trap messages are forwarded. Valid numbers are from 0 to 65535.
`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.
`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.

```
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 sys configure

This command configures the SNMP system information. After you have issued 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).

```
system-config[snmp-system]> sys_name FVS318N-Btd3
system-config[snmp-system]> save
```

Related show command: *show system snmp sys*

Time Zone Command

system time configure

This command configures the system time, date, and NTP servers. After you have issued 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**}
use_default_servers {**Y** | **N**}
configure_ntp_servers {**Y** | **N** {**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 keyword	For a list of time zones that you can enter, see *Table 12*.
auto_daylight	**Y** or **N**	Enables or disables automatic adjustment for daylight savings time.
resolve_ipv6_address	**Y** or **N**	Specifies whether or not the wireless 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.

configure_ntp_servers	**Y** or **N**	Enables or disables the use of custom NTP servers. If you enable the use of custom NTP servers, you need to specify the server IP addresses or domain names with the **ntp_server1** and **ntp_server2** keywords.
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 12. Timezone keywords

GMT time and location **Note:** Enter the keywords exactly as stated (you can use autocompletion keys). If there are two locations for the same time zone, enter the location exactly as stated. For example, either enter **GMT-11:00::Samoa** or enter **GMT-10:00::Hawaii**.
GMT::Edinburgh--London
GMT-12:00::Eniwetok--Kwajalein
GMT-11:00::Midway-Island
GMT-11:00::Samoa
GMT-10:00::Hawaii
GMT-09:30::Marquesas-Is
GMT-09:00::Alaska
GMT-08:00::Pitcairn-Is
GMT-08:00::Pacific-Time-Canada--Pacific-Time-US
GMT-08:00::Tijuana
GMT-07:00::Mountain-Time-Canada--Mountain-Time-US
GMT-06:00::Central-Time-Canada--Central-Time-US
GMT-05:00::Eastern-Time-Canada--Eastern-TimeUS
GMT-05:00::Eastern-Time-Lima
GMT-04:30::Caracas
GMT-04:00::Atlantic-Time-Canada

there are two locations for the same time zone, enter the location exactly as stated. For example, either enter **GMT-11:00::Samoa** or enter **GMT-10:00::Hawaii**.

GMT-03:30::Newfoundland
GMT-03:00::Brasilia
GMT-03:00::Buenos-Aires
GMT-02:00::Mid-Atlantic
GMT-01:00::Azores--Cape-Verde-Is
GMT+01:00::Europe
GMT+02:00::Athens--Istanbul
GMT+02:00::Minsk
GMT+02:00::Cairo
GMT+03:00::Baghdad--Kuwait
GMT+03:00::Moscow
GMT+03:30::Tehran
GMT+04:00::Abu-Dhabi--Muscat
GMT+04:00::Baku
GMT+04:30::Kabul
GMT+05:00::Ekaterinburg
GMT+05:00::Islamabad--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--Hanoi--Jakarta
GMT+08:00::Beijing--Chongqing--Hong-Kong
GMT+08:00::AWST-Perth
GMT+09:00::Osaka--Sapporo--Tokyo--Seoul
GMT+09:30::ACST-Adelaide

For example, either enter **GMT-11:00::Samoa** or enter **GMT-10:00::Hawaii**.
GMT+09:30::ACST-Darwin
GMT+09:30::ACST-Broken-Hill--NSW
GMT+10:00::AEST-Brisbane--Guam--Port-Moresby
GMT+10:00::AEST-Canberra--Melbourne--Sydney--Hobart
GMT+10:30::Lord-Howe-Is.
GMT+11:00::Magadan
GMT+11:00::Solomon-Is.--New-Caledonia
GMT+11:30::Norfolk-I.
GMT+12:00::Auckland--Wellington--New-Zealand
GMT+12:00::Fiji
GMT+13:00::Tonga
GMT+14:00::Kiribati

Command example:

```
FVS318N> system time configure
system-config[time]> timezone GMT-08:00::Pacific-Time-Canada--Pacific-Time-US
system-config[time]> auto_daylight Y
system-config[time]> resolve_ipv6_address N
system-config[time]> use_default_servers Y
system-config[time]> configure_ntp_servers N
system-config[time]> save
```

Related show command: *show system time setup*

WAN Traffic Meter Command

system traffic_meter configure

This command configures the traffic meter. After you have issued the **system traffic_meter configure** command, you enter the system-config [traffic-meter] mode,

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_meridian {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**. There is no traffic limit. • **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**	Enables or disables automatic increase of the limit after the meter has exceeded the configured limit. If you enable 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.

counter	**SpecificTime** or **RestartCounter**	Specifies how the traffic counter is restarted: • **SpecificTime**. Restarts the traffic counter on a specific day and time. You need to set the **day_of_month**, **time_hour**, **time_meridian**, and **time_minute** keywords and associated parameters. • **RestartCounter**. Restarts the traffic counter after you have saved 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 have 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 have set the **counter** keyword to **SpecificTime**.
time_meridian	**AM** or **PM**	Specifies the meridiem for the hour that the traffic counter restarts. This keyword applies only if you have 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 have 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 has exceeded the configured limit.
send_email_alert	**Y** or **N**	Specifies whether or not an email alert is sent when the traffic limit is reached.

```
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_meridian 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*

This command configures routing logs for accepted and dropped IPv4 and IPv6 packets, selected system logs, and logs for other events. After you have issued 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**} **wireless_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]

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 wireless 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 wireless 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.

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 has been exceeded.
bandwidth_limit_logs	**Y** or **N**	Enables or disables logging of packets that are dropped because the bandwidth limit has been exceeded.

Command example:

```
FVS318N> 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 command: *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 have issued 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>*

```
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_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**	Enables or disables 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.

		Plain or **CRAM-MD5**, you also need to 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 have set the **smtp_auth type** keyword type to **Plain** or **CRAM-MD5**.
smtp_auth password	*password*	The password for SMTP authentication if you have 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: • If you select **Never** or **Hourly**, you do not need to further configure the schedule. • If you select **Daily**, you also need to configure the **schedule time** and **schedule meridiem** keywords and their associated keywords. • If you select **Weekly**, you also need to 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 have 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 have set the **schedule unit** keyword to **Daily** or **Weekly**.
schedule meridiem	**AM** or **PM**	Specifies the meridiem for the start time if you have set the **schedule unit** keyword to **Daily** or **Weekly**.

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 with a severity that is equal to and higher than the severity that you specify are logged on the specified syslog server. For example, if you select **LOG_CRITICAL** as the severity, then the logs with the severities **LOG_CRITICAL**, **LOG_ALERT**, and **LOG_EMERG** are logged.

Command example:

```
FVS318N> system logging remote configure
system-config[logging-remote]> log_identifier FVS318N-Bld3
system-config[logging-remote]> email_logs_enable Y
system-config[logging-remote]> email_server SMTP.Netgear.com
system-config[logging-remote]> return_email FVS318N@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_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*

dot11 Mode Configuration Commands

6

This chapter explains the configuration commands, keywords, and associated parameters in the dot11 mode. The chapter includes the following sections:

- *Wireless Radio Commands*
- *Wireless Profile Commands*

IMPORTANT:

After you have issued a command that includes the word `configure`, add, or `edit`, you need to save (or cancel) your changes. For more information, see *Save Commands* on page 13.

This command configures the basic radio settings. After you have issued the **dot11 radio configure** command, you enter the dot11-config [radio] mode, and then you can configure one keyword and associated parameter or associated keyword at a time. You first need to configure the geographical area and country of operation.

Step 1

Format **dot11 radio configure**

Mode dot11

Step 2

Format

```
country {africa <country> | asia <country> | europe <country> |
   middle_east <country> | oceania <country> | united_states
   <country>}

mode {g_and_b | g_only | ng {channel_spacing {20-40MHz |
   20MHz}} | n_only {channel_spacing {20-40MHz | 20MHz}}}
channel {Auto | <channel>}
default_transmit_power {Full | Half | Quarter | Eighth | Minimum}
transmission_rate {Best_Automatic | <rate>}
```

Mode dot11-config [radio]

Keyword	Associated Keyword to Select or Parameter to Type		Description
country	**africa**, **asia**, **europe**, **middle_east**, **oceania**, or **united_states**	country keyword	First, specifies a geographical region. Then, specifies a predefined country name within the specified region. For a list of countries that you can enter, see *Table 13*.

		• **g_and_b**. In addition to 802.11b- and 802.11g-compliant devices, 802.11n-compliant devices can connect to the wireless access point because they are backward compatible. • **g_only**. 802.11g- and 802.11n-compliant devices can connect to the wireless access point, but 802.11n-compliant devices function below their capacity in 802.11g mode. 802.11b-compliant devices cannot connect. • **ng**. This is the default setting. 802.11g- and 802.11n-compliant devices can connect to the wireless access point. 802.11b-compliant devices cannot connect. • **n_only**. Only 802.11n-compliant devices can connect to the wireless access point.
channel_spacing	**20-40MHz** or **20MHz**	For the ng and n_only modes, specifies the channel spacing: • **20-40MHz**. Select this option to improve the performance. Some legacy devices can operate only at 20 MHz. • **20MHz**. Select this option if your network includes legacy devices. **Note:** The channel spacing is fixed at 20 MHz for the g_and_b and g_only modes.
channel	**auto** or the keyword for a specific channel. **Note:** The available channels depend on the country selection and are displayed on the CLI screen.	Specifies the 2.4 GHz channel that is used by the radio. Either select **auto** to enable the wireless access point to select its own channel, or select a specific channel.
default_transmit_power	**Full**, **Half**, **Quarter**, **Eighth**, or **Minimum**	Specifies the default transmit power.

	MCS14-117[243], **MCS13-104[216]**, **MCS12-78[162]**, **MCS11-52[108]**,**MCS10-39[81]**, **MCS9-26[54]**, **MCS8-13[27]**, **MCS7-65[135]**, **MCS6-58.5[121.5]**, **MCS5-52[108]**, **MCS4-39[81]**, **MCS3-26[54]**, **MCS2-19.5[40.5]**, **MCS1-13[27]**,**MCS0-6.5[13.5]**, **54**, **48**, **36**, **24**, **18**, **12**, **11**, **9**, **6**, **5.5**, **2**, or **1**	the wireless access point to select its own data rate, or select a specific data rate. **Note:** The available transmission data rates depend on the country selection and are displayed on the CLI screen.

Table 13. Region and country keywords

Region	Country
Africa	**Algeria**
	Egypt
	Kenya
	Morocco
	SouthAfrica
	Tunisia
	Zimbabwe
Asia	**Azerbaijan**
	Bangladesh
	BruneiDarussalam
	China
	HongKong
	India
	Indonesia
	Japan
	Kazakhstan
	KoreaRepublic
	Macau

(continued)	**Nepal**
	NorthKorea
	Pakistan
	Philippines
	Singapore
	SriLanka
	Taiwan
	Thailand
	Uzbekistan
	Vietnam
Europe	**Albania**
	Armenia
	Austria
	Belarus
	Belgium
	BosniaAndHerzegowina
	Bulgaria
	Croatia
	Cyprus
	CzechRepublic
	Denmark
	Estonia
	Finland
	France
	Georgia **Note:** This keyword might be located under another region. The command syntax might change in a future release.
	Germany
	Greece

(continued)	**Iceland**
	Ireland
	Italy
	Latvia
	Liechtenstein
	Lithuania
	Luxembourg
	Macedonia_TheFormerYugoslavRepublicOfMacedonia
	Malta
	Monaco
	Netherlands
	Norway
	Poland
	Portugal
	Romania
	RussianFederation_RU1
	SerbiaAndMontenegro **Note:** This keyword might be located under another region. The command syntax might change in a future release.
	SlovakRepublic
	Slovenia
	Spain
	Sweden
	Switzerland
	Turkey
	Ukraine
	UnitedKingdom

	Israel
	Bahrain
	Jordan
	Kuwait
	Lebanon
	Oman
	Qatar
	SaudiArabia
	Syria
	UnitedArabEmirates
	Yemen
Oceania	Australia
	NewZealand
	PapuaNewGuinea
UnitedStates	Argentina
	Belize
	Bolivia
	Brazil
	Canada
	Chile
	Colombia
	CostaRica
	DominicanRepublic
	Ecuador
	ElSalvador
	Guatemala
	Honduras
	Jamaica

(continued)	
	Panama
	Peru
	PuertoRico
	TrinidadAndTobago
	UnitedStates_US
	Uruguay
	Venezuela

Command example:

```
FVS318N> dot11 radio configure
dot11-config[radio]> country united_states UnitedStates_US
dot11-config[radio]> 2.4mode ng
dot11-config[radio]> channel_spacing 20-40MHz
dot11-config[radio]> channel Auto
dot11-config[radio]> default_transmit_power Full
dot11-config[radio]> transmission_rate
dot11-config[radio]> transmission_rate Best_Automatic
dot11-config[radio]> save
```

Related show command: *show dot11 radio*

---

dot11 radio advanced configure

This command configures the advanced radio settings. After you have issued the **dot11 radio advanced configure** command, you enter the dot11-config [radio-advance] 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**	**dot11 radio advanced configure**
	Mode	dot11

protection_mode {**CTS-to-Self_Protection** | **None**}
power_save_enable {**Y** | **N**}

Mode dot11-config [radio-advance]

Keyword	Associated Keyword to Select or Parameter to Type	Description
beacon_interval	*milliseconds*	The time in milliseconds between the beacon transmissions.
dtim_interval	*milliseconds*	The time in milliseconds between each delivery traffic indication message (DTIM).
rts_threshold	*bytes*	The Request to Send (RTS) threshold in bytes.
fragmentation_threshold	*bytes*	The maximum length of the frame in bytes.
preamble_mode	**Long** or **Short**	Specifies the type of 802.11b preamble that is prepended to every frame: • **Long**. A long transmit preamble might provide a more reliable connection or a slightly longer range. • **Short**. A short transmit preamble gives better performance.
protection_mode	**CTS-to-Self_Protection** or **None**	Specifies the Clear to Send (CTS)-to-self protection mode: • **CTS-to-Self_Protection**. CTS-to-self protection mode is enabled. This mode increases the performance but reduces the throughput slightly. • **None**. CTS-to-self protection mode is disabled.
power_save_enable	**Y** or **N**	Enables or disables Wi-Fi Multimedia (WMM) power save.

Command example:

```
FVS318N> dot11 radio advanced configure
dot11-config[radio-advance]> beacon_interval 120
dot11-config[radio-advance]> dtim_interval 4
dot11-config[radio-advance]> rts_threshold 1820
dot11-config[radio-advance]> fragmentation_threshold 1820
dot11-config[radio-advance]> preamble_mode Short
dot11-config[radio-advance]> protection_mode CTS-to-Self_Protection
dot11-config[radio-advance]> power_save_enable Y
dot11-config[radio-advance]> save
```

dot11 profile add

This command configures a new wireless profile. After you have issued the **dot11 profile add** command, you enter the dot11-config [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** **dot11 profile add**

Mode dot11

Step 2 **Format** **profile_name** <*profile name*>
ssid <*ssid name*>
broadcast-ssid {**Y** | **N**}
security_type {**Open** | **WEP** | **WPA** | **WPA2** | **WPA+WPA2**}
vlan_profile <*vlan name*>

wep authentication {**Automatic** | **Open-System** | **Shared-Key**}
wep encryption {**64-bit-WEP** | **128-bit-WEP**}
wep {**passphrase** {{**1** | **2** | **3** | **4**} <*passphrase*>} | **wep key** {{**1** | **2** | **3** | **4**} <*key*>}}

wpa encryption {**TKIP** | **CCMP** | **TKIP+CCMP**}
wpa authentication {**PSK** {**wpa wpa-password** <*password*>} | **RADIUS** | **PSK+RADIUS** {**wpa wpa_password** <*password*>}}
pre-authentication {**Y** | **N**}
enable_active_time {**N** | **Y** {**start hour** <*hour*>} {**start meridiem** {**AM** | **PM**}} {**start minute** <*minute*>} {**stop hour** <*hour*>} {**stop meridiem** {**AM** | **PM**}} {**stop minute** <*minute*>}}
wlan_partition {**Y** | **N**}

Mode dot11-config [profile]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
profile name	*profile name*	The wireless profile name (alphanumeric string).
ssid	*ssid name*	The name of the 802.11 profile SSID.
broadcast_ssid	**Y** or **N**	Enables or disables the SSID broadcast.

		keywords and associated parameters and keywords you need to set.
vlan_profile	*vlan name*	The VLAN to which the wireless profile is allocated. If you do not specify a VLAN, the wireless profile is assigned to the default VLAN.
WEP		
wep authentication	**Automatic**, **Open-System**, or **Shared-Key**	Specifies the type of WEP authentication: • **Automatic**. A key is required to connect to this profile. You need to configure the **wep passphrase** keyword and its associated parameter and keyword for automatic generation of the WEP key. You also need to set the **wep encryption** keyword and its associated keyword. • **Open-System**. Anyone can connect to this profile. You need to set the **wep encryption** keyword and its associated keyword. • **Shared-Key**. A key is required to connect to this profile. You need to set the **wep key** keyword and its associated parameter and keyword for manual generation of the WEP key. You also need to set the **wep encryption** keyword and its associated keyword.
wep encryption	**64-bit-WEP** or **128-bit-WEP**	Specifies the type of WEP encryption.
wep passphrase	**1**, **2**, **3**, or **4** and *passphrase*	Specifies both the number of the WEP key (the index) and the passphrase to generate the WEP key from. You have to specify both.
wep key	**1**, **2**, **3**, or **4** and *key*	Specifies both the number of the WEP key (the index) and the actual key. You have to specify both. **Note:** If you have used the **wep passphrase** keyword and its associated parameter and keyword, you do not need to set the **wep key** keyword and its associated parameter and keyword.
WPA		
wpa encryption	**TKIP**, **CCMP**, or **TKIP+CCMP**	Specifies the WPA encryption type. Note the following: • WPA supports TKIP and TKIP+CCMP. • WPA2 supports CCMP and TKIP+CCMP. • WPA+WPA2 supports TKIP+CCMP.

		• **PSK**. Requires you to set the **wpa wpa_password** keyword and associated parameter. • **RADIUS**. Requires you to configure the RADIUS settings. • **PSK_RADIUS**. Requires you to set the **wpa wpa_password** keyword and associated parameter and to configure the RADIUS settings.
wpa wpa_password	*password*	The WPA password, which you need to set only if you have set the **wpa authentication** keyword to **PSK** or **PSK_RADIUS**.
pre-authentication	**Y** or **N**	Enables or disables RADIUS preauthentication, which is possible only if you have set the **security_type** keyword to **WPA2** and the **wpa authentication** keywords to **RADIUS**.
Active timer and WLAN partition		
enable_active_time	**Y** or **N**	Enables or disables the daily timer for the wireless profile. If you enable the timer, you need to set all **start** and **stop** keywords and associated parameters and keywords.
start hour	*hour*	The hour in the format H or HH (1 through 12) that the timer starts, if you have enabled the timer.
start meridiem	**AM** or **PM**	Specifies the meridiem that the timer starts, if you have enabled the timer.
start minute	*minute*	The minute in the format MM (00 to 59) that the timer starts, if you have enabled the timer.
stop hour	*hour*	The hour in the format H or HH (1 through 12) that the timer stops, if you have enabled the timer.
stop meridiem	**AM** or **PM**	Specifies the meridiem that the timer stops, if you have enabled the timer.
stop minute	*minute*	The minute in the format MM (00 to 59) that the timer stops, if you have enabled the timer.
wlan_partition	**Y** or **N**	Enables or disables WLAN partition.

Command example:

```
FVS318N> dot11 profile add
dot11-config[profile]> profile_name First_Floor
dot11-config[profile]> ssid WorkToDo
dot11-config[profile]> broadcast_ssid Y
```

```
dot11-config[profile]> start hour 7
dot11-config[profile]> start meridiem AM
dot11-config[profile]> start minute 00
dot11-config[profile]> stop hour 8
dot11-config[profile]> stop meridiem PM
dot11-config[profile]> stop minute 00
dot11-config[profile]> wlan_partition N
dot11-config[profile]> save
```

Related show command: *show dot11 profile [profile name]* **and** *show dot11 profile status <profile name>*

---

dot11 profile edit <row id>

This command configures an existing wireless profile. After you have issued the **dot11 profile edit** command to specify the row ID to be edited, you enter the dot11-config [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 wireless profile.

Step 1	**Format**	**dot11 profile edit** *<row id>*
	Mode	dot11
Step 2	**Format**	**ssid** *<ssid name>* **broadcast-ssid** {**Y** | **N**} **security_type** {**Open** | **WEP** | **WPA** | **WPA2** | **WPA+WPA2**} **vlan_profile** *<vlan name>* **wep authentication** {**Automatic** | **Open-System** | **Shared-Key**} **wep encryption** {**64-bit-WEP** | **128-bit-WEP**} **wep** {**passphrase** {{**1** | **2** | **3** | **4**} *<passphrase>*} | **wep key** {{**1** | **2** | **3** | **4**} *<key>*}} **wpa encryption** {**TKIP** | **CCMP** | **TKIP+CCMP**} **wpa authentication** {**PSK** {**wpa wpa-password** *<password>*} | **RADIUS** | **PSK+RADIUS** {**wpa wpa_password** *<password>*}} **pre-authentication** {**Y** | **N**} **enable_active_time** {**N** | **Y** {**start hour** *<hour>*} {**start meridiem** {**AM** | **PM**}} {**start minute** *<minute>*} {**stop hour** *<hour>*} {**stop meridiem** {**AM** | **PM**}} {**stop minute** *<minute>*}} **wlan_partition** {**Y** | **N**}

ssid	*ssid name*	The name of the 802.11 profile SSID.
broadcast_ssid	**Y** or **N**	Enables or disables the SSID broadcast.
security_type	**Open**, **WEP**, **WPA**, **WPA2**, or **WPA+WPA2**	Specifies the type of security and associated encryption. Your selection determines which other keywords and associated parameters and keywords you need to set.
vlan_profile	*vlan name*	The VLAN to which the wireless profile is allocated. If you do not specify a VLAN, the wireless profile is assigned to the default VLAN.
WEP		
wep authentication	**Automatic**, **Open-System**, or **Shared-Key**	Specifies the type of WEP authentication: • **Automatic**. A key is required to connect to this profile. You need to configure the **wep passphrase** keyword and its associated parameter and keyword for automatic generation of the WEP key. You also need to set the **wep encryption** keyword and its associated keyword. • **Open-System**. Anyone can connect to this profile. You need to set the **wep encryption** keyword and its associated keyword. • **Shared-Key**. A key is required to connect to this profile. You need to set the **wep key** keyword and its associated parameter and keyword for manual generation of the WEP key. You also need to set the **wep encryption** keyword and its associated keyword.
wep encryption	**64-bit-WEP** or **128-bit-WEP**	Specifies the type of WEP encryption.
wep passphrase	**1**, **2**, **3**, or **4** and *passphrase*	Specifies both the number of the WEP key (the index) and the passphrase to generate the WEP key from. You have to specify both.
wep key	**1**, **2**, **3**, or **4** and *key*	Specifies both the number of the WEP key (the index) and the actual key. You have to specify both. **Note:** If you have used the **wep passphrase** keyword and its associated parameter and keyword, you do not need to set the **wep key** keyword and its associated parameter and keyword.

wpa encryption	**TKIP**, **CCMP**, or **TKIP+CCMP**	Specifies the WPA encryption type. Note the following: • WPA supports TKIP and TKIP+CCMP. • WPA2 supports CCMP and TKIP+CCMP. • WPA+WPA2 supports TKIP+CCMP.
wpa authentication	**PSK**, **RADIUS**, or **PSK+RADIUS**	Specifies the WPA authentication type. Note the following: • **PSK**. Requires you to set the **wpa wpa_password** keyword and associated parameter. • **RADIUS**. Requires you to configure the RADIUS settings. • **PSK_RADIUS**. Requires you to set the **wpa wpa_password** keyword and associated parameter and to configure the RADIUS settings.
wpa wpa_password	*password*	The WPA password, which you need to set only if you have set the **wpa authentication** keyword to **PSK** or **PSK_RADIUS**.
pre-authentication	**Y** or **N**	Enables or disables RADIUS preauthentication, which is possible only if you have set the **security_type** keyword to **WPA2** and the **wpa authentication** keywords to **RADIUS**.
Active timer and WLAN partition		
enable_active_time	**Y** or **N**	Enables or disables the daily timer for the wireless profile. If you enable the timer, you need to set all **start** and **stop** keywords and associated parameters and keywords.
start hour	*hour*	The hour in the format H or HH (1 through 12) that the timer starts, if you have enabled the timer.
start meridiem	**AM** or **PM**	Specifies the meridiem that the timer starts, if you have enabled the timer.
start minute	*minute*	The minute in the format MM (00 to 59) that the timer starts, if you have enabled the timer.
stop hour	*hour*	The hour in the format H or HH (1 through 12) that the timer stops, if you have enabled the timer.
stop meridiem	**AM** or **PM**	Specifies the meridiem that the timer stops, if you have enabled the timer.

wlan_partition	**Y** or **N**	Enables or disables WLAN partition.

Related show command: *show dot11 profile [profile name]* **and** *show dot11 profile status <profile name>*

---

dot11 profile delete <row id>

This command deletes a wireless profile by specifying its row ID. You cannot delete the default wireless profile (row ID 1).

Format	**dot11 profile delete** *<row id>*
Mode	dot11

Related show command: *show dot11 profile [profile name]*

---

dot11 profile disable <row id>

This command disables a wireless profile by specifying its row ID.

Format	**dot11 profile disable** *<row id>*
Mode	dot11

Related show command: *show dot11 profile [profile name]*

---

dot11 profile enable <row id>

This command enables a wireless profile by specifying its row ID.

Format	**dot11 profile enable** *<row id>*
Mode	dot11

This command adds a MAC address to or deletes a MAC address from an access control list (ACL) and configures the ACL setting for a selected wireless profile. After you have issued the **dot11 profile acl configure** command to specify the row ID to be edited, you enter the dot11-config [profile-acl] mode, and then you can configure one keyword and associated parameter or associated keyword at a time in the order that you prefer. You can add multiple MAC addresses to the ACL for a profile.

Step 1	**Format**	**dot11 profile acl configure** *<profile name>*
	Mode	dot11
Step 2	**Format**	**mac_address** {**add** *<mac address>* | **delete** *<mac address>*} **acl_policy** {**Open** | **Allow** | **Deny**}
	Mode	dot11-config [profile-acl]

Keyword (might consist of two separate words)	Associated Keyword to Select or Parameter to Type	Description
mac_address add	*mac address*	The mac address that is added to the ACL.
mac_address delete	*mac address*	The mac address that is deleted from the ACL.
acl_policy	**Open**, **Allow**, or **Deny**	Specifies the default ACL policy for the profile: • **Open**. All MAC addresses are allowed to connect to the profile. • **Allow**. Only MAC addresses that you have added to the ACL are allowed to connect to the profile. • **Deny**. MAC addresses that you have added to the ACL are denied access to the profile.

Command example:

```
FVS318N> dot11 profile acl configure Employees
dot11-config[profile-acl]> mac_address add a1:23:04:e6:de:bb
dot11-config[profile-acl]> mac_address add c2:ee:d2:10:34:fe
dot11-config[profile-acl]> acl_policy Allow
dot11-config[profile-acl]> save
```

Related show command: *show dot11 acl <profile name>*

keyword at a time in the order that you prefer.

Step 1	**Format**	**dot11 profile wps configure**
	Mode	dot11
Step 2	**Format**	**ap_ssid** <*ssid name*> **wps_status** {**Enable** | **Disable**} **configure_via_pbc** {**Y** | **N**} **configure_via_pin** {**N** | **Y** {**station_pin** <*pin*>}}
	Mode	dot11-config [profile-wps]

Keyword	Associated Keyword to Select or Parameter to Type	Description
ap_ssid	*ssid name*	The name of the SSID for which you configure WPS.
wps_status	**Enable** or **Disable**	Enables or disables WPS.
configure_via_pbc	**Y** or **N**	Enables or disables the push button configuration (PBC) method.
configure_via_pin	**Y** or **N**	Enables or disables the PIN method. If you enable the PIN method, you also need to set the **station_pin** keyword and associated parameter.
station_pin	*pin*	The pin for the PIN method, if the PIN method is enabled.

Command example:

```
FVS318N> dot11 profile wps configure
dot11-config[profile-wps]> ap_ssid CompanyWide
dot11-config[profile-wps]> wps_status Enable
dot11-config[profile-wps]> configure_via_pin Y
dot11-config[profile-wps]> station_pin 3719
dot11-config[profile-wps]> save
```

Related show command: *show dot11 wps*

VPN Mode Configuration Commands

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

IMPORTANT:

After you have issued a command that includes the word `configure`, add, or `edit`, you need to save (or cancel) your changes. For more information, see *Save Commands* on page 13.

This command configures the IPSec VPN wizard for a gateway-to-gateway or gateway-to-VPN client connection. After you have issued 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*>
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_ipv6address <*ipv6-address*>
remote_lan_prefixLength <*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 need to issue the **remote_lan_ipaddress** and **remote_lan_netMask** keywords and specify the associated parameters. • **IPv6**. Both endpoints use IPv6 addresses. For the remote LAN IP address, you need to issue the **remote_lan_ipv6address** and **remote_lan_prefixLength** keywords and specify the associated parameters.
conn_name	*connection name*	The unique connection name (alphanumeric string).

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**.
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_ipv6address	*ipv6-address*	The IPv6 remote LAN address when the **ip_version** keyword is set to **IPv6**.
remote_lan_prefixLength	*prefix length*	The IPv6 remote LAN prefix length when the **ip_version** keyword is set to **IPv6**.

Command example:

```
FVS318N> vpn ipsec wizard configure Gateway
vpn-config[wizard]> ip_version IPv6
vpn-config[wizard]> conn_name FVS318N-to-Peer44
vpn-config[wizard]> preshared_key 2%sgd55%!@GH
vpn-config[wizard]> remote_wan_ipaddress peer44.com
vpn-config[wizard]> local_wan_ipaddress fe80::a8ab:bbff:fe00:2
vpn-config[wizard]> remote_lan_ipv6address fe80::a4bb:ffdd:fe01:2
vpn-config[wizard]> remote_lan_prefixLength 64
vpn-config[wizard]> save
```

Related show command: *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:

```
FVS318N> show vpn ipsec vpnpolicy setup
Status  Name              Type        IPSec Mode  Local                                  Remote                          Auth  Encr
_______ _________________ ___________ __________ ______________________________________ ______________________________ _____ ____
Enabled FVS318N-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
```

List of IKE Policies

Name	Mode	Local ID	Remote ID	Encryption	Authentication	DH Group
FVS318N-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

vpn ipsec ikepolicy configure <ike policy name>

This command configures a new or existing manual IPSec IKE policy. After you have issued 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. You cannot change the name of an existing policy.

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}
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>}}
```

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 the Mode Config record that should 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 wireless VPN firewall initiates the connection to the remote endpoint. • **Responder**. The wireless VPN firewall responds only to an IKE request from the remote endpoint. • **Both**. The wireless 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 needs to be set to Aggresive.

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 need to specify IPv4 addresses for the **local_identifier** and **remote_identifier** keywords. • **IPv6**. Both endpoints use IPv6 addresses. You need to specify IPv6 addresses for the **local_identifier** and **remote_identifier** keywords.
local_ident_type	**Local_Wan_IP**, **FQDN**, **User-FQDN**, or **DER_ASN1_DN**	Specifies the ISAKMP identifier to be used by the wireless VPN firewall: • **Local_Wan_IP**. The WAN IP address of the wireless VPN firewall. The setting of the **ip_version** keyword determines if you need to specify an IPv4 or IPv6 address for the **local_identifier** keyword. • **FQDN**. The domain name for the wireless VPN firewall. • **User-FQDN**. The email address for a local VPN client or the wireless VPN firewall. • **DER_ASN1_DN**. A distinguished name (DN) that identifies the wireless VPN firewall in the DER encoding and ASN.1 format.
local_identifier	*identifier*	The identifier of the wireless VPN firewall. The setting of the **local_ident_type** and **ip_version** keywords determines the type of identifier that you need to specify.

	DER_ASN1_DN	• **Remote_Wan_IP**. The WAN IP address of the remote endpoint. The setting of the **ip_version** keyword determines if you need to specify an IPv4 or IPv6 address for the **local_identifier** keyword. • **FQDN**. The domain name for the wireless VPN firewall. • **User-FQDN**. The email address for a local VPN client or the wireless VPN firewall. • **DER_ASN1_DN**. A distinguished name (DN) that identifies the wireless 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 need to specify.
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.

		shared between the wireless VPN firewall and the remote endpoint. You also need to 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.
enable_dead_peer_detection	**Y** or **N**	Enables or disables dead peer detection (DPD). When DPD is enabled, you also need to 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 wireless VPN firewall tears down the connection and then attempts to reconnect to the peer.

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 wireless VPN firewall functions as a VPN client of the remote gateway. In this configuration the wireless VPN firewall is authenticated by a remote gateway. You need to issue the **xauth_username** and **xauth_password** keywords and specify the associated parameters. • **EdgeDevice**. The wireless VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. You need to issue the **extended_authentication_type** keyword and select an associated keyword.
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 wireless 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.

```
vpn-config[ike-policy]> exchange_mode Main
vpn-config[ike-policy]> ip_version ipv4
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*

This command configures a new or existing auto IPSec VPN policy or manual IPSec VPN policy. After you have issued 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. You cannot change the name of an existing policy.

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_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_auto_initiate_policy {N | Y}
general_enable_keep_alive {N | Y {general_ping_ipaddress
   <ipaddress> | {general_ping_ipaddress6 <ipv6-address>}
   {general_keep_alive_detection_period <seconds>}
   {general_keep_alive_failureCount <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_encryption_key_out *<key>*

manual_spi_out *<number>*
manual_authentication_algorithm {**MD5** | **SHA-1**}
manual_authentication_key_in *<key>*
manual_authentication_key_out *<key>*

auto_sa_lifetime {**bytes** *<number>* | {**seconds** *<seconds>*}
auto_encryption_algorithm {**None** | **DES** | **3DES** | **AES-128** | **AES-192** | **AES-256**}
auto_authentication_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 have issued the keywords and associated parameters that are listed in the Auto policy settings section of this table. All other VPN policy settings need to be specified manually. • **Manual-Policy**. All settings need to be specified manually, excluding the ones in the Auto policy settings section of this table.

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_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 need to either issue the **general_remote_end_point ip_address** keyword and specify an IPv4 address or issue the **general_remote_end_point ipv6_adress** keyword and specify an IPv6 address. • **FQDN**. You need to 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.

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**	Enables or disables NetBIOS broadcasts to travel over the VPN tunnel.
general_enable_auto_initiate_policy	**Y** or **N**	Enables or disables the automatic establishment of the VPN tunnel when there is no traffic. **Note:** You cannot enable 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**	Enables or disables the wireless VPN firewall to send keep-alive requests (ping packets) to the remote endpoint to keep the tunnel alive. If you enable keep-alives, you also need to issue the following keywords: • Either **general_ping_ipaddress** to specify an IPv4 address or **general_ping_ipaddress6** 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_ipaddress	*ipaddress*	The IPv4 address to send keep-alive requests to.
general_ping_ipaddress6	*ipv6-address*	The IPv6 address to send keep-alive requests 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.
general_keep_alive_failue_count	*number*	The maximum number of keep-alive request failures before the wireless 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 wireless 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.

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.

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.
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**. • **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_authentication_algorithm	**MD5** or **SHA-1**	Specifies the 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.
manual_authentication_key_in	*key*	The encryption key for the inbound policy. The length of the key depends on setting of the **manual_authentication_algorithm** keyword.
manual_authentication_key_out	*key*	The encryption key for the outbound policy. The length of the key depends on setting of the **manual_authentication_algorithm** keyword.
Auto policy settings		
auto_sa_lifetime bytes	*number*	The lifetime of the security association (SA) is the period or the amount of transmitted data after which the SA becomes invalid and needs to be renegotiated. Either issue the **auto_sa_lifetime bytes** keywords and specify the number of bytes, or issue the **auto_sa_lifetime seconds** keywords and specify the period in seconds.
auto_sa_lifetime seconds	*seconds*	
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**. • **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_authentication_algorithm	**MD5** or **SHA-1**	Specifies the 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 need to issue the **auto_dh_group** keyword to specify a group.
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*	Select an existing IKE policy that defines the authentication negotiation.

Command example:

```
FVS318N> 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_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 seconds 3600
vpn-config[vpn-policy]> auto_encryption_algorithm 3DES
vpn-config[vpn-policy]> auto_authentication_algorithm SHA-1
vpn-config[vpn-policy]> auto_select_ike_policy FVS-to-Paris
vpn-config[vpn-policy]> save
```

Related show command: *show vpn ipsec vpnpolicy setup* **and** *show vpn ipsec vpnpolicy status*

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 command: *show vpn ipsec vpnpolicy setup* **and** *show vpn ipsec vpnpolicy status*

Format	**vpn ipsec vpnpolicy drop** *<vpn policy name>*
Mode	vpn

Related show command: *show vpn ipsec vpnpolicy setup* **and** *show vpn ipsec vpnpolicy status*

IPSec VPN Mode Config Commands

vpn ipsec mode_config configure <record name>

This command configures a Mode Config record. After you have issued 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]

first_pool_start_ip	*ipaddress*	The start IP address for the first Mode Config pool.
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 need to 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.

		• **None**. • **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.
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:

```
FVS318N> vpn ipsec mode_config configure iphone
vpn-config[modeConfig]> first_pool_start_ip 10.100.10.1
vpn-config[modeConfig]> first_pool_end_ip 10.100.10.12
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*

Mode vpn

Related show command: *show vpn ipsec mode_config setup*

SSL VPN Portal Layout Commands

vpn sslvpn portal_layouts add

This command configures a new SSL VPN portal layout. After you have issued 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.

		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:

```
FVS318N> 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 have issued 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 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*

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*

This command configures a new authentication domain that is not limited to SSL VPN users. After you have issued 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*.

	Radius-MSCHAP, **Radius-MSCHAPv2**, **WIKID-PAP**, **WIKID-CHAP**, **MIAS-PAP**, **MIAS-CHAP**, **NTDomain**, **ActiveDirectory**, or **LDAP**	• For all selections with the exception of **LocalUserDatabase**, you need to issue the **authentication_server1** keyword and specify an IP address. • For all PAP and CHAP selections, you need to issue the **authentication_secret** keyword and specify a secret. • For the **NTDomain** selection, you need to issue the **workgroup** keyword and specify the workgroup. • For the **ActiveDirectory** selection, you need to issue the **active_directory_domain** keyword and specify the Active Directory. • For the **LDAP** selection, you need to 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).
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:

```
FVS318N> vpn sslvpn users domains add
vpn-config[user-domains]> active_directory_domain 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*

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 Keyword to Select or 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.
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*

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*

This command configures a new authentication group that is not limited to SSL VPN users. After you have issued 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:

```
FVS318N> 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 have issued 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 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*

This command configures a new user account. The command is not limited to SSL VPN users. After you have issued 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**} **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**, or **L2TPUser,**	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 need to 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:

```
FVS318N> vpn sslvpn users users add
vpn-config[users]> user_name PeterBrown
vpn-config[users]> user_type SSLVPNUser
```

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 have issued 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**} **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**, and **L2TPUser**	Specifies the user type. **Note:** You cannot change an existing user from the **L2TPUser** user type to another type or from another type to the **L2TPUser** type.
password	*password*	The password (alphanumeric string) that is assigned to the user. You need to 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*

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 have issued 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**	Enables or disables login from the WAN interface.
disable_login	**Y** or **N**	Enables or disables login from any interface.

Command example:

```
FVS318N> vpn sslvpn users users login_policies 5
vpn-config[user-login-policy]> disable_login Y
vpn-config[user-login-policy]> save
```

Related show command: *show vpn sslvpn users users* **and** *show vpn sslvpn users login_policies <row id>*

---

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 need to issue the **source_address** keyword and specify an IPv4 address. For a network address, you also need to 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 need to issue the **source_address6** keyword and specify an IPv6 address. For a network address, you also need to issue the **prefix_length** keyword and specify a prefix length.

		setting of the **ip_version** keyword determines whether you need to 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 need to 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**.
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:

```
FVS318N> vpn sslvpn users users ip_policies configure 5
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 command: *show vpn sslvpn users users* **and** *show vpn sslvpn users ip_policies <row id>*

Mode	vpn	

Related show command: *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 have issued 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 or Parameter to Type	Description
add_browser	**InternetExplorer**, **NetscapeNavigator**, **Opera**, **Firefox**, or **Mozilla**	Adds a browser to the browser list. By default, there are no browsers on the browser list.
delete_browser	**InternetExplorer**, **NetscapeNavigator**, **Opera**, **Firefox**, or **Mozilla**	Removes a browser from the browser list (after you first have added the browser to the browser list).

		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:

```
FVS318N> vpn sslvpn users users browser_policies 5
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 command: *show vpn sslvpn users users* **and** *show vpn sslvpn users browser_policies <row id>*

This command configures a new SSL port forwarding application. After you have issued 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:

```
FVS318N> 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*

---

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 needs to 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:

```
FVS318N> 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*

This command configures the SSL client IP address range. After you have issued 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 need to 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 has been established.
secondary_dns	*ipaddress*	The IP address of the secondary DNS server. This setting is optional.

end_client_address	*ipaddress*	The end IP address of the IPv4 client range. The default address is 192.168.251.254.

Command example:

```
FVS318N> vpn sslvpn client ipv4
vpn-config[sslvpn-client-ipv4-settings]> enable_full_tunnel N
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 192.168.200.50
vpn-config[sslvpn-client-ipv4-settings]> end_client_address 192.168.200.99
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 have issued 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 need to 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).

end_client_address	*ipv6-address*	The end IP address of the IPv6 client range. The default address is 4000::200.

Command example:

```
FVS318N> 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 have issued 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 clients routes to be operable, split-tunnel support should be enabled.

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]

		• **IPv4**. The network address is an IPv4 address. You need to 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 need to 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:

```
FVS318N> 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*

This command adds a new resource. After you have issued 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:

```
FVS318N> 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

This command configures a resource object. (You first need to add a resource with the *vpn sslvpn resource add* command.) After you have issued 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]

		ip_version keyword determines whether you need to 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 need to 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 need to issue the **object_address** keyword and specify an IPv4 address. For a network address, you also need to 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 need to issue the **object_address6** keyword and specify an IPv6 address. For a network address, you also need to 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 depend 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.

```
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>*

This command configures a new SSL VPN policy. After you have issued 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**}

```
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 need to 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 need to 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.

	All	turn, which keywords you need to issue to specify the policy: • **NetworkResource**. The policy is applied to an existing IPv4 or IPv6 resource. For information about how to create and configure network resources, see *SSL VPN Resource Commands*. You need to 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**. • **IPAddress**. The policy is applied to a single IPv4 or IPv6 address. You need to 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**.

	All (continued)	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 is applied to all addresses. You need to 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.
policy_permission	**Permit** or **Deny**	Specifies whether the policy permits or denies access.

		• **IPv4**. The policy is for an IPv4 network resource, IPv4 address, IPv4 network, or for all IPv4 addresses. For an IP address or IP network, you need to issue the **policy_address** keyword and specify an IPv4 address. For a network address, you also need to 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 for all IPv6 addresses. For an IP address or IP network, you need to issue the **policy_address6** keyword and specify an IPv6 address. For a network address, you also need to 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 is applied only to a VPN tunnel. • **PortForwarding**. The policy is applied only to port forwarding. • **All**. The policy is applied both to a VPN tunnel and to port forwarding.

Command example:

```
FVS318N> vpn sslvpn policy add
vpn-config[sslvpn-policy-settings]> policy_name RemoteWorkers
```

```
vpn-config[sslvpn-policy-settings]> save
vpn-config[sslvpn-policy-settings]> policy_name Management
vpn-config[sslvpn-policy-settings]> ip_version IPv4
vpn-config[sslvpn-policy-settings]> policy_type Group
vpn-config[sslvpn-policy-settings]> policy_owner Headquarter
vpn-config[sslvpn-policy-settings]> destination_object_type All
vpn-config[sslvpn-policy-settings]> start_port 15652
vpn-config[sslvpn-policy-settings]> end_port 15658
vpn-config[sslvpn-policy-settings]> service_type VPNTunnel
vpn-config[sslvpn-policy-settings]> policy_permission Permit
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 have issued 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**}

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:

```
SRX5308> vpn sslvpn policy edit 2
vpn-config[sslvpn-policy-settings]> resource_name ManagementAlternate
vpn-config[sslvpn-policy-settings]> start_port 35502
```

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

vpn ipsec radius configure

This command configures a RADIUS server. After you have issued 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]

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:

```
FVS318N> vpn ipsec radius configure
vpn-config[radius-config]> enable Y
vpn-config[radius-config]> radius-server 192.168.1.2
vpn-config[radius-config]> secret Hlo0ole1H12aaq43
vpn-config[radius-config]> nas_identifier FVS318N-Bld3
vpn-config[radius-config]> backup_server_enable Y
vpn-config[radius-config]> backup_radius-server 192.168.1.3
vpn-config[radius-config]> backup_server_secret Hduo0oplH54bqX91
vpn-config[radius-config]> backup_server_nas_identifier FVS318N-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]*

This command configures the L2TP server. After you have issued 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	Associated Keyword to Select or Parameter to Type	Description
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.

Command example:

```
FVS318N> 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]> save
```

Related show command: *show vpn l2tp server setup* **and** *show vpn l2tp server connections*

This chapter provides an overview of all show commands for the five configuration command modes. The chapter includes the following sections:

Network Settings (Net Mode) 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 14. 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 {interface name | all}*	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.

lan (continued)	*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 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.
radvd	*show net radvd dmz setup*	Display the DMZ RADVD configuration.
	show net radvd lan setup	Display the LAN RADVD configuration.
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 {interface name | all}*	Display the network statistics for a single or all Ethernet interfaces.
wan	*show net wan mode*	Display the WAN mode configuration.
	show net wan port_setup	Display the configuration of the WAN port.
	show net wan wan1 ipv4 setup	Display the IPv4 WAN configuration.
	show net wan wan1 ipv4 status	Display the IPv4 WAN connection status.
	show net wan wan1 ipv6 setup	Display the IPv6 WAN configuration.
	show net wan wan1 ipv6 status	Display the IPv6 WAN connection status.
wan_settings	*show net wan_settings wanmode*	Display the IPv4 WAN routing mode.

alphabetical order:

Table 15. 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 SIP ALG is enabled.
	show security firewall attack_checks igmp	Display whether the IGMP proxy is enabled.
	show security firewall attack_checks jumboframe	Display whether jumbo frames are 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 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.

(continued)	*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 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 (System Mode) 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 16. Show commands: show system mode

Submode	Command Name	Purpose
not applicable	*show sysinfo*	Display system information, including MAC addresses, serial number, and 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.
snmp	*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.
status	*show system status*	Display the system status information.

		configuration of the NTP server.
traffic_meter	*show system traffic_meter setup*	Display the configuration of the traffic meter and the Internet traffic statistics.

Wireless Settings (Dot11 Mode) Show Commands

Enter the **`show dot11 ?`** command at the CLI prompt to display the submodes in the show dot11 mode. The following table lists the submodes and their commands in alphabetical order:

Table 17. Show commands: show dot11 mode

Submode	Command Name	Purpose
acl	*show dot11 acl <profile name>*	Display the ACL policy and MAC addresses for a specified profile.
profile	*show dot11 profile [profile name]*	Display basic information for all profiles or basic and advanced information for a specified profile.
	show dot11 profile status <profile name>	Display traffic statistics for a specified profile.
radio	*show dot11 radio*	Display the basic and advanced radio configuration.
statistics	*show dot11 statistics*	Display cumulative wireless traffic statistics for all profiles.
wps	*show dot11 wps*	Display the WPS configuration.

Table 18. Show commands: show vpn mode

Submode	Command Name	Purpose
ipseci	*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 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.

		addresses for a specific user.
sslvpn (continued)	*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.

9 Show Commands

This chapter explains the show commands and associated parameters for the five configuration command modes. The chapter includes the following sections:

- *Network Settings (Net Mode) Show Commands*
- *Security Settings (Security Mode) Show Commands*
- *Administrative and Monitoring Settings (System Mode) Show Commands*
- *Wireless Settings (Dot11 Mode) Show Commands*
- *VPN Settings (VPN Mode) Show Commands*

WAN (IPv4 and IPv6) Show Commands

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 mode

This command displays the WAN mode configuration:

```
WAN MODE Setup

_______________

Routing Mode: NAT
IP Mode: IPv4/IPv6 mode
```

show net wan port_setup

This command displays the configuration of the WAN port:

```
WAN Port Setup

_______________
MTU Type:       Default
Port Speed:     Auto Sense
Router's MAC Address:   Use Default Address
```

```
_________________

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 wan1 ipv4 status

This command displays the IPv4 WAN connection status:

```
WAN Status

__________

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
Gateway: 10.139.54.225
Primary DNS: 10.80.130.23
Secondary DNS:
```

show net wan wan1 ipv6 setup

This command displays the IPv6 WAN configuration:

```
IPv6 WAN1 Setup

_________________

Dynamic IPv6 (DHCP) Configuration:
Stateless Address Auto Configuration: Enabled
```

```
_________________

IPv6 Connection Type: Dynamic IPv6 (DHCP)
IPv6 Connection State: Not Yet Available
IPv6 Address: fe80::a8ab:bbff:fe00:2
IPv6 Prefix Length: 64
Default IPv6 Gateway:
Primary DNS Server:
Secondary DNS Server:
```

IPv6 Mode and IPv6 Tunnel Show Commands

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::
```

```
sit0-WAN1   2002:408b:36e4::408b:36e4/64, ::127.0.0.1/96, ::192.168.1.1/96,
::10.139.54.228/96
isatap1-LAN fe80::5efe:421:1d0a/64, fe80::5efe:a1d:2104/64,
fe80::fe5e:0: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    192.168.4.118
```

LAN DHCP Show Commands

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:

```
Jan  1 00:02:26 FVS318N local7.info dhcpd: Sending on
LPF/bdg1/aa:ab:bb:00:00:01/192.168.1.0/24
Jan  1 00:02:26 FVS318N local7.info dhcpd: Sending on
Socket/fallback/fallback-net
Jan  1 00:02:34 FVS318N local7.info dhcpd: Wrote 0 leases to leases file.
Jan  1 00:02:34 FVS318N local7.info dhcpd: Listening on
LPF/bdg1/aa:ab:bb:00:00:01/192.168.1.0/24
Jan  1 00:02:34 FVS318N local7.info dhcpd: Sending on
LPF/bdg1/aa:ab:bb:00:00:01/192.168.1.0/24
Jan  1 00:02:34 FVS318N local7.info dhcpd: Sending on
Socket/fallback/fallback-net
```

```
List of DHCP Reserved Addresses

_____________________________________

Name: IPAD_227
IP Address: 192.168.1.23
MAC Address: aa:11:bb:22:cc:33
Group: 1
```

Dynamic DNS Show Commands

show net ddns setup

This command displays the Dynamic DNS configuration:

```
Dynamic DNS service currently disabled
```

IPv4 LAN Show Commands

show net lan ipv4 setup

This command displays the IPv4 LAN configuration:

```
LAN Setup (IPv4)

__________________

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   DHCP Server 192.168.70.100 - 192.168.70.254
Enabled Marketing    40      192.168.90.5 255.255.255.128 Disabled    Not Applicable

Default VLAN

_____________

Port1: Default
Port2: Default
Port3: Marketing
Port4: Default
```

show net lan ipv4 detailed setup <vlan id>

This command displays the detailed configuration for a VLAN:

```
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 {interface name | all}

This command displays the MAC address and VLAN status for a single or all Ethernet interfaces:

```
FVS318N> show net ethernet eth1

MAC Address: AA:AB:BB:00:00:02
VLAN ID: 1
Interface Name: eth1
VLAN Enabled: N
Native VLAN: N

FVS318N> show net ethernet all
```

```
_______ _____________ ____________ ___________
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: Same
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       GROUP3
4       GROUP4
5       Management
6       SalesEMEA
7       SalesAmericas
8       GROUP8
```

```
_____________________

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
```

IPv6 LAN Show Commands

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: Enable DHCPv6 Server
DHCP Mode: Stateless
Domain Name: netgear.com
Server Preference: 255
DNS Servers: Use DNS from ISP
Lease/Rebind Time: 86400


List of IPv6 Address Pools
__________________________

Start Address      End Address
_________________ _________________
FEC0::db8:2       FEC0::db8:199
FEC0::db8:10a1:100 FEC0::db8:10a1:300
```

```
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
```

DMZ Show Commands

show net dmz ipv4 setup

This command displays the IPv4 DMZ configuration:

```
DMZ Setup

_________
DMZ Disabled.
```

show net dmz ipv6 setup

This command displays the IPv6 DMZ configuration:

```
DHCP Setup Configuration

_________________________

IPv6 Address: 2001:176::1
Prefix Length: 64
DHCP Status: DHCP Server Enabled
Mode: Stateful
Domain Name: netgear.com
DNS Server: Use DNS Proxy
Lease Time in Sec : 43200
Starting IP Address : 2001::1100
Ending IP Address   : 2001::1120
Pool Prefix Length  : 56
```

show net radvd dmz setup

This command displays the DMZ RADVD configuration:

```
Router Advertisement Daemon ( RADVD )

_____________________________________
RADVD Status: Enabled
Advertise Mode: Unicast only
Advertise Interval: 30
RA Flags

Managed: Disabled
```

```
List of Available Prefixes to Advertise
_______________________________________

ROW ID IPv6 Prefix IPv6 Prefix Length Life Time
_______ ___________ ____________________ _________
1       2002:3a2b   64                   3600
2       2002:3a2b   64                   3600
```

Routing Show Commands

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
```

```
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 Commands

show net statistics {interface name | all}

This command displays the network statistics for a single or all Ethernet interfaces:

```
FVS318N> show net statistics eth0

Interface Statistics
____________________

IFACE: eth0
PktRx: 5688
ktTx: 5651
ByteRx: 654963
ByteTx: 4834187
ErrRx: 0
ErrTx: 0
DropRx: 0
DropTx: 0
Mcast: 0
Coll: 0
FVS318N> show net statistics all
```

```
_____ ______ ______ ________ ________ _____ _____ ______ ______ _____ ____
eth0  20802  31569  2148358  38409384 0     0     0      0      0     0
eth1  359059 186965 61156441 28586367 0     0     0      0      0     0
```

Security Settings (Security Mode) Show Commands

This section contains the following subsections:

Services Show Command

show security services setup

This command displays the configured custom services:

```
List of Available Custom Services
_________________________________

ROW ID Name              Type   ICMP Type / Port Range QoS
______ ________________ ______ ______________________ ____________________
74     Ixia             TCP    10115-10117            Normal-Service
75     RemoteManagement TCP    8888-8888              Maximize-Throughput
```

```
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 Command

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                       Priority       Bandwidth Profile Log
_____ _______ ____________ ____________ ________ ____________________________ _______________ _________________ _____
103   Enabled CU-SEEME:TCP BLOCK Always Any      Any                          Normal-Service NONE              Never
104   Enabled PING         ALLOW Always Any      10.120.114.217 - 10.120.114.245 Normal-Service NONE              Always

LAN WAN Inbound Rules.
_____________________________

ROWID: 102
Status: Enabled
Service Name: HTTP
Filter: ALLOW Always
LAN Server IP Address: 192.168.5.69
LAN User:
WAN User: Any
Destination: Broadband
Bandwidth Profile: NONE
Log: Never
```

```
DMZ WAN Outbound Rules.
_____________________________

ROWID: 105
Status: Enabled
Service Name: FTP
Filter: ALLOW by schedule,otherwise block
DMZ User: Any
WAN User: Any
Priority: Maximize-Reliability
Log: Never


DMZ WAN Inbound Rules.
_____________________________

ROWID Status  Service Name Filter       DMZ Server IP Address DMZ User WAN User Destination   Log
 _____ _______ ____________ ____________ _____________________ ________ ________ _____________ ______
106   Enabled Traceroute   ALLOW Always 176.21.214.2                  Any      10.115.97.174 Always
107   Enabled TELNET       ALLOW Always 176.21.214.2                  Any      Broadband     Always
```

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: 100
Status: Enabled
Service Name: FTP
Filter: ALLOW Always
LAN User: GROUP3
DMZ User: 176.16.2.65 - 176.16.2.85
Log: Never
```

```
Status: Enabled
Service Name: SSH:UDP
Filter: BLOCK by schedule,otherwise allow
DMZ User: 176.16.2.211
LAN User: 192.168.4.109
Log: Always
```

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 Show Commands

show security firewall attack_checks igmp

This command displays whether the IGMP proxy is enabled:

```
IGMP Configuration

_________________________
Igmp Proxy: Disabled
```

show security firewall attack_checks jumboframe

This command displays whether jumbo frames are enabled:

```
Jumbo Frame Configuration

_____________________________
Jumbo Frame Support: Enabled
```

```
_____________

WAN Security Checks:

_____________________
Respond to ping on Wan            : Yes
Enable Stealth mode               : Yes
Block TCP Flood                   : Yes

LAN Security Checks:

_____________________
Block UDP Flood                   : Yes
Disable Ping Reply on LAN Ports   : No
```

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           : Yes
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  : Enabled
L2TP Passthrough  : Enabled
```

```
Session Settings

_________________

Session Limit Enable:   Enabled
Connection Limit Type:  1
User Connection Limit:  6
TCP Session Timeout Duration:   1800(Secs)
UDP Session Timeout Duration:   120(Secs)
ICMP Session Timeout Duration:  60(Secs)
```

show security firewall session_settings

This command displays the session time-out settings:

```
Session Settings

_________________

TCP Session Timeout Duration:1800(Secs)
UDP Session Timeout Duration:120(Secs)
ICMP Session Timeout Duration:60(Secs)
```

Advanced Firewall Show Commands

show security firewall advanced algs

This command displays whether SIP ALG is enabled:

```
ALGs

____

Sip: Disabled
```

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      Rule1 00:aa:23:be:03:a1 192.168.10.153          Enabled             IPv4
2      CFO   a1:b2:c3:d4:ee:da 2001:3063:21a2:28e4::   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
_______________

List of Available Port Triggering Rules
_____________________________________

ROW ID: 1
Name: AccInq
Enable: Yes
Type: TCP
Interface: LAN
Outgoing Start Port: 20020
Outgoing End Port: 20022
Incoming Start Port: 30030
Incoming End Port: 30040
```

show security porttriggering_rules status

This command displays the port triggering status:

```
PortTriggering Rules Status
___________________________
```

UPnP Show Commands

show security upnp portmap

This command displays the UPnP portmap table:

```
UPnP Portmap Table
__________________
```

```
____________________

Advertisement Period: 30
Advertisement Time To Live: 4
```

Bandwidth Profiles Show Command

show security bandwidth profile setup

This command displays the configured bandwidth profiles:

```
List of Available Bandwidth Profiles
_____________________________________

ROW ID Name     Direction       Outbound Bandwidth Range Inbound Bandwidth Range Is Group
______ ________ _______________ ________________________ ________________________ ________
1      BW1      Outbound        500-1500                 NA                       0
2      BW_Sales Both Directions 1000-10000               1000-10000               1
```

Content Filtering Show Commands

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 : Enabled
Java : Enabled
ActiveX : Enabled
Cookies : Disabled
```

```
_____________
List of Blocked Groups

Blocked Groups:
Unblocked Groups : GROUP1, GROUP2, GROUP3, GROUP4, Management, SalesEMEA,
SalesAmericas, GROUP8
```

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
```

This section contains the following subsections:

- *Remote Management Show Command*
- *SNMP Show Commands*
- *Time Show Command*
- *Firmware Version Show Command*
- *Status Show Command*
- *Traffic Meter Show Command*
- *Logging Configuration Show Commands*
- *Logs Show Commands*

Note: The VPN logs and RADIUS logs are part of the VPN Mode show commands (see *VPN Settings (VPN Mode) Show Commands* on page 299).

Remote Management Show 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
```

```
Trap Agent IP Address
_____________________

IP Address: 10.118.33.245
Subnet Mask: 255.255.255.255
Port: 162
Community: public
```

show system snmp sys

This command displays the SNMP system configuration of the wireless VPN firewall:

```
SNMP System Configuration
_________________________

SysContact: AdminFVS@netgear.com
SysLocation: San Jose
SysName: FVS318N-Bld3
```

Time Show Command

show system time setup

This command displays the time configuration and the configuration of the NTP server:

```
Time Zone & NTP Servers Configuration
_____________________________________

Current Time: Friday, April 13, 2012, 01:22:40 (GMT -0700)
Timezone: (GMT-08:00) Pacific Time(Canada), Pacific Time(US)
Automatically Adjust for Daylight Savings Time: Yes
Default NTP servers used : Yes
```

This command displays the firmware version.

```
Firmware Version :   4.1.1-8
```

Status Show Command

show system status

This command displays the system status (also referred to as router status) information:

```
System Info
_____________

System Name: FVS318N
Firmware Version: 4.1.1-8

Lan Port 1 Information
_____________________
VLAN Profile:   Default
VLAN ID:        1
MAC Address:    E0:46:9A:1D:1A:9C
IP Address:     192.168.1.1
Subnet Mask:    255.255.255.0
DHCP Status:    Enabled

Lan Port 2 Information
_____________________
VLAN Profile:   Default
VLAN ID:        1
MAC Address:    E0:46:9A:1D:1A:9C
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
```

```
Lan Port 4 Information

_________________________
VLAN Profile:   Default
VLAN ID:        1
MAC Address:    E0:46:9A:1D:1A:9C
IP Address:     192.168.1.1
Subnet Mask:    255.255.255.0
DHCP Status:    Enabled

Lan Port 5 Information

_________________________
VLAN Profile:   Sales
VLAN ID:        20
MAC Address:    E0:46:9A:1D:1A:9C
IP Address:     192.168.70.1
Subnet Mask:    255.255.255.0
DHCP Status:    Enabled

Lan Port 6 Information

_________________________
VLAN Profile:   Sales
VLAN ID:        20
MAC Address:    E0:46:9A:1D:1A:9C
IP Address:     192.168.70.1
Subnet Mask:    255.255.255.0
DHCP Status:    Enabled

Lan Port 7 Information

_________________________
VLAN Profile:   Sales
VLAN ID:        20
MAC Address:    E0:46:9A:1D:1A:9C
IP Address:     192.168.70.1
Subnet Mask:    255.255.255.0
DHCP Status:    Enabled

Lan Port 8/DMZ  Information
```

```
IP Address:     192.168.1.1
Subnet Mask:    255.255.255.0
DHCP Status:    Enabled

Broadband Information
_____________________

MAC Address: AA:AB:BB:00:00:02
IPv4 Address: 10.139.54.228 / 255.255.255.248
IPv6 Address: fe80::a8ab:bbff:fe00:2 / 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
Gateway: 10.139.54.225
Primary DNS: 10.80.130.23
Secondary DNS: 10.80.130.24
Gateway (IPv6):
Primary DNS(IPv6):
Secondary DNS(IPv6):

Wireless LAN Information
________________________

Wireless Status: Enable
SSID: FVS318N_1
Mode: N Only
Security Setting: WPA+WPA2
Region: North America
Channel: 1-2.452 GHz
AP MAC Address: E0:46:9A:1D:1A:AE
```

```
Enable Traffic Meter

_____________________
Traffic Meter is Enabled

Limit Type Download only
Monthly Limit in (MB): 150000
Increase this month limit: Enabled
Increase limit by in (MB): 50000
This month limit:

Traffic Counter

_________________
Traffic Counter: Specific Time

Restart Time (HH/MM-Day of Month): 12/0-1
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 Dec  9 18:09:49 2011
Outgoing Traffic Volume: 2057
Incoming Traffic Volume: 2070
Average per day: 4127
% of Standard Limit: 0
% of this Month's Limit: 0
```

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
```

```
Reboots:                              Enabled
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: FVS318N-BLD3

Enable E-Mail Logs
__________________

E-Mail Server Address: SMTP.Netgear.com
Return E-Mail Address: FVS318N@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
____________________
```

Logs Show Commands

show system logs

This command displays the system logs (the following example shows only part of the command output):

```
Wed Dec 7 14:06:23 2011(GMT) [FVS318N][System][NTP] Looking Up
time-g.netgear.com


Wed Dec 7 14:06:252011(GMT)[FVS318N][System][NTP]Requestingtimefromtime-g
.netgear.com


Wed Dec 7 14:06:262011(GMT)[FVS318N][System][NTP]Synchronizedtimewithtime
-g.netgear.com


Wed Dec 7 14:06:26 2011(GMT) [FVS318N][System][NTP] Timezone difference :480


Wed Dec 7 14:06:272011(GMT)[FVS318N][System][NTP]NextSynchronizationafter
2 Hours


Wed Dec 7 15:13:362011(GMT)[FVS318N][System][SSLVPN]SSL_INFO:useradmin2is
Logged-Out successfully from host 74.116.205.101


Wed Dec 7 15:31:00 2011(GMT) [FVS318N][Kernel][KERNEL] WAN_PING[DROP]IN=eth1
OUT= MAC=aa:ab:bb:00:00:02:00:22:10:9c:23:10:08:00 SRC=10.136.73.53 DST=
10.139.54. 228 LEN=92 TOS=0x00 PREC=0x20 TTL=108 ID=8004 PROTO=ICMP TYPE=8
CODE=0 ID=512 SEQ=5702
```

show sysinfo

This command displays system information, including MAC addresses, serial number, and firmware version:

```
System - Manufacturer Information
*************************
hwver: 00:00:A0:03reginfo: 0x0005
numofimages : 1


currimage: 1
mac address : E0469A1D1A9C
```

```
wireless MAC[3] : e0469a1d1ab1
vlan[0] MAC : e0469a1d1a9f
vlan[1] MAC : e0469a1d1aa0
vlan[2] MAC : e0469a1d1aa1
vlan[3] MAC : e0469a1d1aa2
vlan[4] MAC : e0469a1d1aa3
vlan[5] MAC : e0469a1d1aa4
vlan[6] MAC : e0469a1d1aa5
vlan[7] MAC : e0469a1d1aa6
vlan[8] MAC : e0469a1d1aa7
vlan[9] MAC : e0469a1d1aa8
vlan[10] MAC : e0469a1d1aa9
vlan[11] MAC : e0469a1d1aaa
vlan[12] MAC : e0469a1d1aab
vlan[13] MAC : e0469a1d1aac
vlan[14] MAC : e0469a1d1aad
WAN MAC : e0469a1d1a9d

pcbasn number : S.YX218U00E0
serial number : 2JF119BY001B0

image 0 : 4.1.1-8
image 1 : 0
productId : FVS318N

maccnt0: 0x22
maccnt1: 0x0
maccnt2: 0x0
maccnt3: 0x0
*************************
```

Radio Show Command

show dot11 radio

This command displays the configuration information for the radio:

```
Radio Configuration
_____________________

Region: North America
Country: US
Operating Frequency: 2.4 GHz
Mode: n only
Channel Spacing: 20/40 MHz
Current Channel: 9-2.452 GHz
Channel: 1-2.412GHz
Default Transmit Power: Half(dBm)
Transmit Power: 15 dBm
Transmit Rate: Best(Automatic)

Radio Advanced Configuration
_____________________________

Beacon Interval: 100 (Milliseconds)
DTIM Interval: 2
RTS Threshold: 2346 (Bytes)
Frag Threshold: 2346 (Bytes)
Preamble Mode: Long
Protection Mode: None
Power save enable: N
```

for a specified profile:

- All profiles:

```
FVS318N> show dot11 profile
Status   Profile Name SSID      Broadcast Security Encryption Authentication Active Time Start Time Stop Time
________ ____________ ________ _________ ________ __________ ______________ ___________ __________ _________
Enabled  default1     FVS318N_1 Y         WPA+WPA2 TKIP+CCMP  PSK            Disabled    -          -
Disabled 1st_Floor    WorkToDo  Y         WPA+WPA2 TKIP+CCMP  PSK            Enabled     7:0 AM     8:0 PM
```

- A specified profile

```
FVS318N> show dot11 profile 1st_Floor

Profile Configuration
_____________________

Profile Name: 1st_Floor
SSID: WorkToDo
Broadcast SSID: Enabled
Security: WPA+WPA2
Authentication: PSK
Encryption: TKIP+CCMP
WPA Password: **********
Profile Advanced Configuration:
Association Timeout Interval (in Seconds): 10
Authentication Timeout Interval (in Seconds): 10
Group Key Refresh Interval (in Seconds): 3600
PMKSA LifeTime (in Seconds): 3600
802.1X Re-authentication Interval (in Seconds): 3600
```

show dot11 profile status <profile name>

This command displays traffic statistics for the specified profile (note that the profile is called an access point and that, in this example, it is indicated by ap2):

```
Access Point Status
___________________

AP Name: ap2
Radio: 1
PktRx: 0
```

```
ErrTx: 0
DropRx: 0
DropTx: 11301
MCast: 0
#Coll: 0

Connected Clients
_____________________
```

show dot11 acl <profile name>

This command displays the ACL policy and MAC addresses for the specified profile:

```
Default ACL Policy
_____________________
ACL Policy Status: Allow

List of MAC Address
_____________________

_____________________
a1:23:04:e6:de:bb
c2:ee:d2:10:34:fe
```

show dot11 wps

This command displays the WPS configuration:

```
Access Point Name: ap1
WPS Enabled: Y
```

that the profiles are indicated by ap1, ap2, ap3, and so on):

```
Wireless Statistics
_____________________

AP Name Radio PktRx PktTx ByteRx ByteTx ErrRx ErrTx DropRx DropTx MCast #coll
_______ _____ _____ _____ _______ _______ _____ _____ _______ _______ _____ _____
ap1     1     0     0     0       0       0     0     0       83      0     0
ap2     1     0     0     0       0       0     0     0       0       0     0
ap3     1     0     0     0       0       0     0     0       80      0     0
```

VPN Settings (VPN Mode) 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*
- *L2TP Server Show Commands*

IPSec VPN Show Commands

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)
FVS318N-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)
```

```
Enabled FVS318N-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 (this example does not relate to the previous two examples):

```
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      100.10.10.1     100.153.46.20                 7.01      31            IPsec SA Established     Drop
4      100.10.10.2     100.153.46.20                 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
___________ ___________________ ___________________
Beijing     192.168.2.100       192.168.2.150
iphone      10.100.100.1        100.10.100.12
```

show vpn ipsec logs

This command displays the IPSec VPN logs (the following example shows only part of the command output):

```
Tue Apr 10 12:24:36 2012 (GMT -0700): [FVS318N] [IKE] INFO:  Using IPsec SA
configuration: anonymous
Tue Apr 10 12:24:36 2012 (GMT -0700): [FVS318N] [IKE] INFO:  Re-using previously
generated policy: 100.10.10.2/32[0] 0.0.0.0/0[0] proto=any dir=in
Tue Apr 10 12:24:36 2012 (GMT -0700): [FVS318N] [IKE] WARNING:  less key length
proposed, mine:128 peer:256.  Use initiaotr's one.
Tue Apr 10 12:24:36 2012 (GMT -0700): [FVS318N] [IKE] INFO:  IPsec-SA
established: ESP/Tunnel 173.11.109.158->64.139.54.228 with spi=
73255174(0x45dc906)
Tue Apr 10 12:24:36 2012 (GMT -0700): [FVS318N] [IKE] INFO:  IPsec-SA
established: ESP/Tunnel 64.139.54.228->173.11.109.158 with spi=
7343706(0x700e5a)
```

show vpn sslvpn client

This command displays the SSL VPN client ranges and configurations:

```
SSL VPN Client(IPv4)
_____________________

Enable Full Tunnel Support: No
DNS Suffix:
Primary DNS Server: 192.168.10.5
Secondary DNS Server: 192.168.10.6
Client Address Range Begin: 192.168.200.50
Client Address Range End: 192.168.200.99

SSL VPN Client(IPv6)
_____________________

Enable Full Tunnel Support: No
DNS Suffix:
Primary DNS Server: 192.168.10.5
Secondary DNS Server: 192.168.10.6
Client Address Range Begin: 4000::1000:2
Client Address Range End: 4000::1000:50
```

show vpn sslvpn logs

This command displays the SSL VPN logs:

```
Fri Dec  9 20:19:03 2011(GMT) [FVS318N][System][SSLVPN] SSL_INFO :user admin2
is Logged-Out successfully from host 10.116.205.103
Sat Dec 10 09:12:50 2011(GMT) [FVS318N][System][SSLVPN]  SSL_INFO : Login
Successful for Local Admin user admin2 from host 10.116.205.103
Sat Dec 10 14:07:32 2011(GMT) [FVS318N][System][PLATFORM]
platformHandleDBUpdate:SSLVPNUserLoginPolicyDefinedBrowser op=18 row=2
Sat Dec 10 14:12:10 2011(GMT) [FVS318N][System][PLATFORM]
platformHandleDBUpdate:SSLVPNUserLoginPolicyDefinedAddress op=18 row=1
Sat Dec 10 14:12:26 2011(GMT) [FVS318N][System][SSLVPN] Edit operation done on
user PeterBrown
```

```
Sat Dec 10 18:09:50 2011(GMT) [FVS318N][System][PLATFORM]
platformHandleDBUpdate:SSLVPNPortalLayout op=23 row=1
Sat Dec 10 18:09:51 2011(GMT) [FVS318N][System][SSLVPN] Portal 'SSL-VPN' is set
as default
Sat Dec 10 18:09:53 2011(GMT) [FVS318N][System][SSLVPN] Domain Headquarter is
successfully added. Authentication Type: ldapPortal Layout Name: SSL-VPN
Sat Dec 10 18:10:21 2011(GMT) [FVS318N][System][SSLVPN] Group Sales is
successfully added. Domain Name:Headquarter
```

show vpn sslvpn policy

This command displays the SSL VPN policies:

```
SSL VPN Policies
_________________

Row Id Policy Name   Service Type    Destination Object  Permission
______ _____________ _______________ ____________________ __________
1      RemoteWorkers Port Forwarding TopSecure            Permit
2      Management    VPN Tunnel      0.0.0.0:15652-15658 Permit
```

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://64.139.54.228/portal/SSL-VPN https://[fe80::e246:9aff:fe1d:1a9d]/portal/SSL-VPN
2      CSup       In case of login difficulty... 1         https://64.139.54.228/portal/CSup    https://[fe80::e246:9aff:fe1d:1a9d]/portal/CSup
```

```
_____________________________________________

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: 1
Server IP: 192.168.51.227
FQDN Name: RemoteDesktop
```

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
```

```
_________________

Row Id: 1
Object Type: IP Network
Object Address: 192.168.30.56
Mask Length: 24
Start Port: 3391
End Port: 3393
```

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

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
```

```
_____________

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
```

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
```

```
LoginAddress: : 10.116.205.166
LoginTime: : Fri Apr 13 11:55:33 2012 (GMT -0700)
```

RADIUS Server Show Command

show vpn ipsec radius [ipaddress]

This command displays the configuration of all RADIUS servers or of a specified RADIUS server:

- All RADIUS Servers:

```
FVS318N> show vpn ipsec radius

Configured RADIUS Client
_________________________

Server IP   Server Port Timeout Retries NAS Identifier
___________ ___________ _______ _______ _______________
192.168.1.2 1812        30      4       FVS318N
192.168.1.3 1812        30      4       FVS318N
```

- A specified RADIUS server:

```
FVS318N> show vpn ipsec radius 192.168.1.2

RADIUS Configuration
____________________

Auth Server IP Address: 192.168.1.2
Auth Port: 1812
Timeout (in seconds): 30
Retries: 4
Secret: sharedsecret
NAS Identifier: FVS318N
```

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
_________________________
```

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 19. Utility commands in the util mode

Command Name	Purpose
util backup_configuration	Back up the configuration file of the wireless 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 wireless 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 wireless VPN firewall.
util restore_factory_defaults	Restore the wireless 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 wireless VPN firewall from a TFTP server

This command backs up the configuration file of the wireless 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 wireless 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 wireless VPN firewall from a TFTP server.

Format	**`util firmware_upgrade`** *`<source file name> <tftp server address>`*
Mode	util

---

util reboot

This command reboots the wireless VPN firewall. It takes about 3 minutes for the wireless VPN firewall to come back up.

Format	**`util reboot`**
Mode	util

Format	**util restore_factory_defaults**
Mode	util

Diagnostic Commands

util dns_lookup

This command looks up the IP address of a domain name.

Format	**util dns_lookup** *<domain name>*
Mode	util

```
FVS318N> util dns_lookup netgear.com
Server:    66.80.130.23
Address 1: 66.80.130.23 ns1.megapath.net
Name:      netgear.com
Address 1: 206.16.44.90
```

util ping

This command pings an IP address with 56 data bytes and displays the ping information.

Format	**util ping** *<ipaddress>*
Mode	util

```
FVS318N> 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
```

Format	**util ping_through_vpn_tunnel** *<ipaddress>*
Mode	util

```
FVS318N> 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

```
FVS318N> 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

CLI Command Index

U

V