Fireware

Command Line Interface Reference v12.9.4

WatchGuard Fireboxes

About This Guide

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Guide revised: 6/27/2023

Copyright, Trademark, and Patent Information

Complete copyright, trademark, patent, and licensing information can be found in the *Copyright and Licensing Guide*, available online:
http://www.watchguard.com/wgrd-help/documentation/overview

Table of Contents

1 Introduction to the CLI

About the CLI Reference Guide

WatchGuard® Firebox devices include a Command Line Interface (CLI) installed on the hardware. You can connect to the Firebox and use the CLI as an alternative to the Web UI or WatchGuard System Manager software. You can use the CLI with any terminal client that supports SSH2.

This section provides information about how to use the command reference in this document.

Command Reference Format

The syntax section for each command uses this format:

A shaded area shows a single syntax for a command that uses the notation described in the subsequent section.

After each command, guidance and comments for the command are shown. For commands where a choice is available for a particular portion of the command, all possible options are described. In the case where a command requires no guidance or comments, this area contains the text “No options available.”

Command Reference Notation

The syntax section of each command uses a standardized format and notation:

Notation	Meaning
bold	Bold text indicates commands and keywords that you enter as shown
italic	Italic text indicates an argument that you provide. Examples include an account name, password, FTP location, or IP address.
[x]	Square brackets enclose an optional keyword or argument.
(x)	Parentheses enclose a required keyword or argument.
...	An ellipsis (three consecutive periods without spaces) after an element indicates that the element can be repeated.
|	A vertical line, called a pipe, that is enclosed within braces or square brackets indicates a choice within a set of keywords or arguments.
[x|y]	Square brackets around keywords or arguments separated by a pipe indicate an optional choice between separate, mutually exclusive options.
(x|y)	Parentheses around keywords or arguments separated by a pipe indicate a required choice between separate, mutually exclusive options.
[x(y|z)]	Parentheses and a pipe within square brackets indicate a required choice within an optional element.

Special Characters

If you must include special characters within a command argument, such as a password, you can enclose the argument in double quotes " " to remove (escape) the special meaning associated with those characters.

Example

```
restore image from usb flash-image backup.fxi "configpassfoo&"
```

Sample Command References

A command reference provides:

- The command
- A brief description of the command
- The command syntax
- Examples, where appropriate

The subsequent commands are two sample command references. Where appropriate, the example also includes sample output.

history

Description

Display the command history list with line numbers.

Syntax

history

No options available.

export

Description

Export information to an external platform or file.

Syntax

export (**blocked-site**|**allowed-site**) **to** (*location*)

Export the blocked site list or the allowed site list. The allowed site list is also known as the blocked site exceptions list.

blocked-site — blocked IP addresses
allowed-site — allowed IP addresses
location — the FTP or TFTP location of the import file.

export config to (*location*)

Export the device configuration.

location — the FTP or TFTP location to save the file

export muvpn *group-name* [**client-type** *client*] **to** (*location*)

Export a Mobile VPN with IPSec user configuration file.

group-name must be the name of an existing Mobile VPN with IPSec group
client must be one of these options:

- **watchguard** — export the .ini profile for use with the WatchGuard Mobile VPN with IPSec client. This is the default setting.
- **shrew-soft-client** — export the .vpn profile for use with the Shrew Soft VPN client.

location — the FTP or TFTP location of the import file.

export support to (*location*|[**usb** (*filename*)])

Export the support snapshot file.

location — the FTP or TFTP location to save the file

usb — save the support snapshot to the specified file on a USB drive connected to the Firebox

Examples

```
export blocked-site to ftp://joez:1pass@ftp.example.com:23/upload/blocked.dot

export muvpn client-type shrew-soft-client to
ftp://joez:1pass@ftp.example.com:23/upload/vpn-users.vpn

export support to usb support.tgz
```

Start the Command Line Interface

To connect to the CLI of a Firebox, you can use a terminal client located in the same secure environment as the Firebox. The terminal client must use SSH2 to connect to the Firebox with a serial cable. You can also connect to the Console port or with TCP/IP to a Trusted or Optional interface. You can use the CLI to manage the Firebox while it is in operation, though some configuration changes require a restart.

Every Firebox has two default user accounts: *admin* and *status*. Use the *admin* user account for read-write privileges. Use the *status* user account for read-only privileges.

The default password for the *admin* user account is *readwrite*. When you log in with the admin user account, or with another user account that has Device Administrator privileges, the WatchGuard CLI opens in the Main command mode with the prompt `WG#`.

The default password for the *status* user account is *readonly*. When you log in with the status user account, or with another user account that has Device Monitor privileges, the WatchGuard CLI opens in the Main command mode with the prompt `WG>`.

You can also log in with another user account that has Device Administrator or Device Monitor privileges.

Some commands are not available when you log in with a Device Management user account that has Device Monitor credentials.

You can specify authentication servers for the user account you use to log in to the CLI. For example, at the CLI login prompt, you can type:

- *RADIUS\username* for a RADIUS user
- *LDAP\username* for an LDAP user
- *DOMAIN\username* where DOMAIN is the Active Directory domain for a user, such as, *example.com\username*

Connect with a Serial Cable

To manage a Firebox with a serial cable connection, your computer must have an available serial port as well as an installed terminal client application, such as PuTTY.

1. Connect a serial cable from your computer to the Console port on the Firebox.
2. Open your terminal application. Open a new connection window.

3. Verify that the terminal is set to VT100.
   If the terminal is not set to VT100, some command and control key functions do not work. For example, Ctrl-C does not break, some special characters do not type, and ESC does not work.
4. Verify that your connection parameters are set to:
   - Port — The serial port on your management computer, usually COM1
   - Baud Rate — 115200
   - Data Bits — 8
   - Stop Bits — 1
   - Parity — No
   - Flow Control — None
5. Press **Enter**.
   The connection window displays a welcome message and the Firebox login prompt.
6. Type the user name for a Device Management user account. Press **Enter**.
   There are two default Device Management user accounts: admin and status. Use admin, or another Device Administrator user account, for read-write privileges. Use status, or another Device Monitor user account, for read-only privileges. You can use any Device Monitor or Device Administrator credentials that are configured on your Firebox.
7. Type the passphrase for the user account. Press **Enter**.

Connect with TCP/IP

The default WatchGuard policy allows you to connect to and manage a Firebox from any computer on a trusted or optional network on port 4118. For more information about how to modify the default policy to either restrict access to the CLI or enable access from an external network, see the *Fireware Help*.

For this procedure, you must have a terminal client that supports SSH2 and the IP address of a Firebox trusted or optional interface.

1. Open your terminal application. Open a new connection window.
2. Verify that the connection type is set to SSH.
3. Verify that your connection parameters are set to:
   - Host name — The IP address of the Firebox trusted or optional interface to connect to.
   - Port — 4118
4. Start the connection.
   The connection window displays a welcome message and the Firebox login prompt.
5. At the login prompt, type the user name. Press **Enter**.
   There are two default Device Management accounts: admin and status. Use admin, or another Device Administrator user account, for read-write privileges. Use status, or another Device Monitor user account, for read-only privileges. You can use any Device Monitor or Device Administrator credentials that are configured on your Firebox.
6. At the password prompt, type the passphrase for the user account. Press **Enter**.

Connect to the CLI on an XTMv Device

You can manage your XTMv device with the Fireware CLI.

- For an XTMv device on a VMware ESXi hypervisor, you can connect to the console in the VMware vSphere client, or you can connect through a serial port, if you have allocated a serial port to the XTMv virtual machine.

- For an XTMv device on a Microsoft Hyper-V hypervisor, connect to the XTMv device in Hyper-V Manager.

For more information, see the *XTMv Setup Guide* available on the Fireware Product Documentation page at http://www.watchguard.com/help/documentation.

Enter Commands in the CLI

To use the WatchGuard CLI, type a command at the prompt and press Enter on your keyboard. It is not necessary to type the command in full to have the CLI execute the command correctly.

Terminal Commands

The subsequent table includes a series of commands to move around in, and to operate in, the CLI.

Your terminal client might use different commands or operating system rules for the procedures in this section.

Keyboard Key(s)	Function
Backspace	Erase the character to the left of the cursor. If there is no character to the left of the cursor, erase the current character.
Ctrl-D	Erase the current character at the cursor.
Ctrl-K	Erase all characters from the cursor to the end of the current command line.
Esc-D	Erase from the cursor to the end of the current word.
Ctrl-W	Erase from the word to the left of the cursor.
Ctrl-B or Ctrl-f	Move the cursor to the left one character.
Ctrl-F or Ctrl-g	Move the cursor to the right one character.
Ctrl-A	Move the cursor to the start of the line.
Ctrl-E	Move the cursor to the end of the line.
Esc-B	Move the cursor to the left one word.
Esc-F	Move the cursor to the right one word.
Ctrl-P or Ctrl-h	Recall commands in the history buffer.
Ctrl-N or Ctrl-i	Recall recent commands.
Ctrl-T	Replace the character to the left of the cursor with the character at the cursor.
Ctrl-L	Show the current command line again.

Get Help

The WatchGuard® Command Line Interface (CLI) has an interactive Help system. To use the Help system, type `help` or `?` at the command line and press **Enter** on your keyboard.

help

Description

Show a numbered list of the available command formats for the specific command.

Syntax

help *command*

If *command* is not provided, describes general features of the Help system.

If *command* is provided, returns a list of all the possible syntaxes for the specified command.

If *command* is ?, returns a list of all commands for which help is available in the current command mode.

command must be a valid command for the current command mode.

Example

```
help arp
  [1] arp (flush)
help diagnose
  [1] diagnose [to(<ftp>|<tftp>)|cluster[to(<ftp>|<tftp>)]]
  [2] diagnose vpn<ident>
help export
  [1] export (blocked-site|allowed-site) to (<ftp>|<tftp>)
  [2] export (config) to (<ftp>|<tftp>|console)
  [3] export muvpn <ident> [client-type <WatchGuard|Shrew_Soft-Client>] to
  (<ftp>|<tftp>|console)
  [4] export support to (<ftp>|<tftp>|usb[<ident>])
help tcpdump
  [1] tcpdump [<mstring>]*
```

Syntax in Help Output

The help command uses a unique syntax to describe how to use CLI commands.

Element	Example	Usage
|	<ftp>|<tftp>	Indicates that the command allows any one of the options separated by the |.
[ ]	[to (<ftp>|<tftp>)]	Indicates that the text provided between the [and] can optionally be used in the command.
*	[<ident>]*	Indicates that multiple items can be added to the command.
( )	(blocked-site|allowed-site)	Indicates the text between the (and) is required.
< >	<alarm|event|traffic|debug>	Indicates that information or a selection identified by the text between the < and >, must be made by the user.
<ident>	(batch secret <ident>|secret)	Indicates that a specific piece of information is required to execute this command. This information could be an account name, a password, or the name of a certificate. Use the ? command to determine what the required information is, or refer to the command reference provided in this document. Must be enclosed by double quotes.
<ftp>	[to (<ftp>|<tftp>)]	Indicates that an FTP address in the required format is accepted by the command. See “Import and Export Files” on page 9 for the required format.
<tftp>	[to (<ftp>|<tftp>)]	Indicates that a TFTP address in the required format is accepted by the command. See the subsequent section for the required format.
int:x-y	<int:0-int_max>	Indicates that an integer between the specified range of X and Y must be provided. If Y is ‘int_max’ the maximum value allowed is 2147483647.
<ipaddr>	(<ipaddr> <ipmask>|<net>)	Indicates a Version 4 IP address (IPv4), or a dotted decimal notation in the form

Element	Example	Usage
		of nnn.nnn.nnn.nnn where nnn is 0–255 is required. Used with <ipmask>.
<ipmask>	(<ipaddr> <ipmask>|<net>)	Indicates a Netmask in the form of mmm.mmm.mmm.mmm where mmm is 0–255 is required. Used with <ipaddr>.
<net>	(<ipaddr> <ipmask>|<net>)	Indicates a Classless InterDomain Routing (CIDR) notation is required in the form of nnn.nnn.nnn.nnn/dd where nnn is 0–255 and dd is 0–32.
<macaddr>	<macaddr>	Indicates a physical address of a Firebox is required. Format must be 01:23:45:67:89:ab.
<cr>	<cr>	Indicates that the command line is complete and can be executed when you press “Enter”.
<mstring>	ping <mstring> where <mstring>: [-LRUbdfnqrvVaA] [-c count] [-i interval] [-w deadline][hop1...] [-p pattern] [-s packetsize] [-t ttl] [-I interface or address] [-M mtu discovery hint] [-S sndbuf][-T timestamp option] [-Q tos] [-i interface][-s snaplen][-T type][expression] traceroute <mstring> where <mstring>: [-adnruvAMOQ] [-w wait] [-S start_ttl] [-m max_ttl] [-p port#] [-q nqueries] [-g gateway] [-t tos] [-s src_addr] [-g router] [-I proto] host [data size] tcpdump <mstring> where <mstring>: [-adeflnNOpqStuvxX][-c count] [-i interface][-s snaplen] [-T type][expression][	

"?" Command

Description

Displays all possible options for the next part of a command.

Syntax

command **?**

command must be a valid command for the current command mode. If not a valid command, the CLI returns `Unrecognized command`.

To display a list of all available commands for the current command, leave command blank.

If the CLI returns `<cr> Carriage return`, it indicates that the command can be executed as entered.

Example

```
WG#show s?
  schedule          Schedule for use in the application of policies
  signature-update  Signature update configuration
  snat              Static NAT or server load balancing
  snmp              Simple Network Management Protocol
  sslvpn            Secure Sockets Layer Virtual Private Network
  static-arp        Static arp
  status-report     Display system status
  sysinfo           Display system information
```

Error Handling in the CLI

When you type a command that returns an error, the WatchGuard CLI shows:

- Where the error is in the syntax,
- The part of a command that is not recognized, or
- Other feedback on the error message.

There are five error message categories in the CLI: unrecognized, incomplete, execution, syntax, and ambiguous.

Unrecognized Command Error

If a command does not exist, the CLI returns an unrecognized command error.

For example, in the Main command mode, the user enters the command help acc. Because there are no commands in the Main mode which start with “acc”, the CLI returns the message `% Unrecognized command`.

Incomplete Command Error

If a user enters a command without all the required parameters, the CLI returns an incomplete command error.

For example, in the Main command mode the user enters the command show. Because the show command requires an additional parameter to indicate what should be displayed, the command is incomplete, and the CLI returns the message `% Incomplete command`.

Execution Error

If a user enters a command with incorrect information, the CLI returns an execution error.

For example, in the Main command mode, the user enters the command `show users user1000`. Because there is no user1000, the command is inaccurate, and the CLI returns the message `% Error: Account 'user1000' not found`.

The error message includes information to help the user identify the error and correct the command.

Syntax Error

If a user enters a command incorrectly, the CLI returns a syntax error. The error message is:

`% Invalid input detected at '^' marker`, where the ^ marker denotes the start of the invalid command.

Ambiguous Command Error

If a user enters a truncated command that has more than one possible meaning, the CLI returns an ambiguous command error. The error message is: `% Ambiguous command input detected at '^' marker` where the ^ marker denotes the start of the ambiguous input.

Import and Export Files

You can use the WatchGuard CLI to export and import files between a Firebox and a remote server with either FTP or TFTP. The address must include a file name and the complete URL path, where appropriate.

The FTP address must use this syntax to identify the user, server, and file name:

Example:

ftp://[user[:passwd]@]host[:port]/[complete URL path]/filename

ftp://ftpuser:ftppassword@ourftpsite:23/files/upload/file.dot

ftp://ftpuser:ftppassword@ourftpsite:23/readme.txt

The TFTP address must use this syntax to identify the server and file name:

tftp://host/url-path

Example:

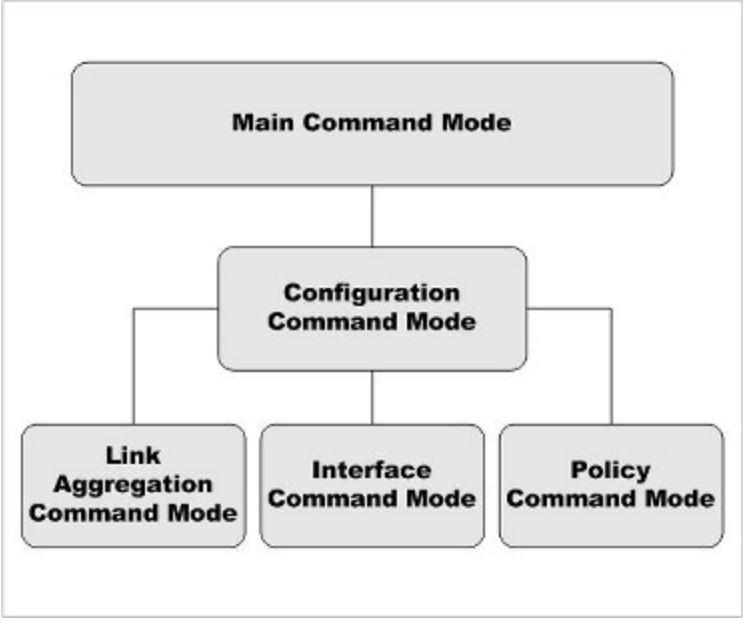
tftp://myftpsite/files/upload/file.dot

2 Command Modes Overview

About CLI Command Modes

The WatchGuard Command Line Interface (CLI) operates in five distinct command modes: Main, Configuration, Policy, Interface, and Link Aggregation. This section gives an overview of the command modes and how to use the command prompt to identify the working mode.

The command mode hierarchy describes the relationship between the four command modes. To get access to the Configuration command mode, you must be in the Main command mode. To get access to the Interface and Policy command modes, you must be in the Configuration command mode.



Main Command Mode

The Main command mode is the default command mode of the WatchGuard CLI. In Main mode, you can:

- Modify some higher level configuration settings
- See system logs
- Enter the Configuration command mode
- Restore or upgrade the software image
- Shut down or reboot the Firebox

Configuration Command Mode

The Configuration command mode is used to configure system and network settings for the Firebox. To get access to the Configuration command mode, open the CLI in the Main command mode, then use the **configure** command. You can use Configuration mode to perform these functions:

- Manage the logging performed by the Firebox
- Configure global network settings
- Enter Interface, Link-Aggregation, and Policy command modes
- Enter XTM wireless access point mode
- Enter VLAN and Bridge command modes

If the Firebox is has been configured to allow more than one user with Device Administrator credentials to connect at the same time, and a Device Administrator has unlocked the configuration file to make changes, you cannot make changes to the configuration file until that Device Administrator has either locked the configuration file again or has logged out.

Interface Command Mode

Interface command mode is used to configure the Ethernet interfaces of the Firebox. To get access to Interface command mode, open the CLI in Configuration command mode, then use the **interface** command. You can use Interface command mode to perform these functions on a single interface:

- Configure the IP address and addressing options for the interface
- Configure the interface as a gateway
- Control MTU and link speed preferences
- Configure the interface as a DHCP server or DHCP relay
- Configure the interface for QoS

Link Aggregation Command Mode

Link Aggregation command mode is used to configure link aggregation interfaces on the Firebox. A link aggregation interface can include one or more Ethernet interfaces. To get access to Interface command mode, open the CLI in Configuration command mode, then use the **link-aggregation** command. You can use link-aggregation command mode to perform these functions on a single link-aggregation interface:

- Add and remove link aggregation member interfaces
- Configure the link aggregation interface mode
- Configure the IP address and addressing options for the link aggregation interface
- Configure the link aggregation interface as a gateway
- Control link speed
- Configure the link aggregation interface as a DHCP server or DHCP relay

Policy Command Mode

Policy command mode is used to configure policies. To get access to Policy command mode, open the CLI in the Configuration command mode, then use the **policy** command. You can use Policy mode to perform these functions:

- Create and modify rules and schedules
- Manage user accounts
- Define users, groups, and aliases for use in policies
- Control branch office VPN gateways and tunnels
- Configure branch office and mobile user VPN policies

Common Commands

Many commands are available in all command modes. These are known as “common commands”. In this Reference Guide, the common commands are in a separate chapter. You can use common commands in all command modes with all optional commands and parameters unless otherwise noted. The types of commands available in all command modes include:

- Help and history
- Commands to display settings, log messages, and status

Command Line Interface Prompt

The prompt displayed by the WatchGuard Command Line Interface (CLI) changes to indicate the current command mode.

Command Mode	Command Set	Prompt
Main (read write)	Common and Main commands	WG#
Main (read only)	Common and Main commands	WG>
Configuration	Common and Configuration commands	WG(config)#
Interface	Common and Interface commands	WG(config/if-fe<if-number>)#
Link Aggregation	Common and Link Aggregation commands	WG(config/la-<la-name>)#
Policy	Common and Policy commands	WG(config/policy)#

The prompt for read/write access is preceded by the text `[Fault]` if a fault event has occurred on the Firebox and Fault Reports are available.

For example: `[Fault]WG#`

Use the **show fault-report** command to see more information about the fault event and available Fault Reports.

3 Common Commands

About Common Commands

Common commands are those commands that are available in all four of the WatchGuard Command Line Interface (CLI) command modes. Any minor differences in the behavior of these commands due to the working command mode are described in each individual command mode chapter.

Due to the complexity of the **show** command, the reference for this command is divided into individual command mode references for each variant of this command.

List of Common Commands

These commands are available in all command modes:

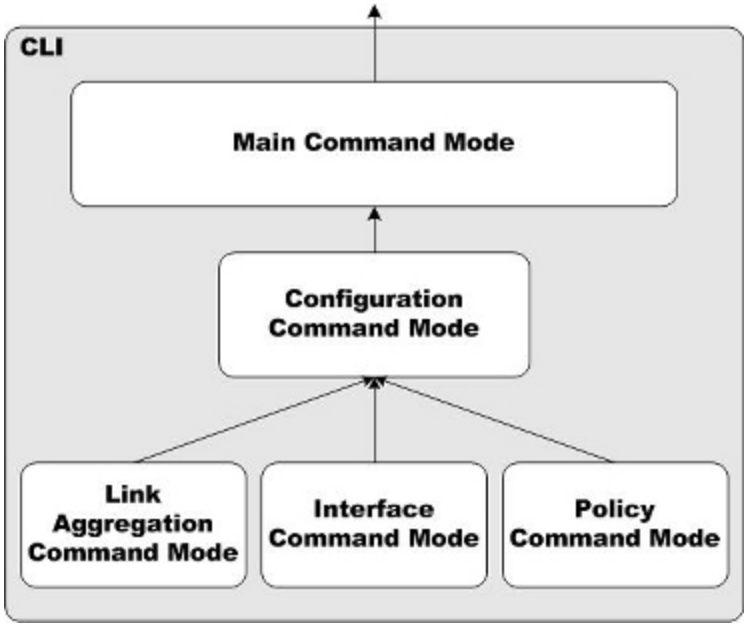
Command	Usage
exit	In Main mode, exit the CLI. Otherwise, return to the previous mode.
help	See general information or possible syntax for specified command.
history	See a list of the last 100 commands entered into the CLI.
!	Repeat a command from the CLI command history.
show	Display information about a component of the current configuration or status.

Common Command Reference

exit

Description

In Main mode, exit the CLI. In any other mode, return to the previous mode.



Syntax

exit

No options available.

help

Description

See general information or possible syntax for specified command.

Syntax

help [*command*]

If *command* is not provided, describes general features of the Help system.

If *command* is provided, returns a list of all the possible syntaxes for the specified command.

If *command* is **?**, returns a list of all commands for which help is available in the current command mode.

command must be a valid command for the current command mode.

Examples

```
help arp
 [1] arp (flush)
help export
 [1] export (blocked-site|allowed-site) to (<ftp>|<tftp>)
 [2] export (config) to (<ftp>|<tftp>|console) [html ((en|ja-JP|fr-FR|es-
 419|zh-CN|ko-KR|zh-TW))]
 [3] export l2tp to (<ftp>|<tftp>)
 [4] export muvpn <ident> [client-type <WatchGuard|Shrew-Soft-Client|iOS-
 Android-Client>] to (<ftp>|<tftp>)
 [5] export support to (<ftp>|<tftp>|usb [<ident>])
help tcpdump
 [1] tcpdump [<mstring>]*
```

The WatchGuard Mobile VPN App for iOS and the WatchGuard Mobile VPN App for Android are no longer available or supported.

history

Description

See a numbered list of the last 100 commands entered into the CLI.

Syntax

history

No options available.

Examples

```
history
```

!

Description

Repeat a recently used CLI command from the command history.

Syntax

!(*text-string*) [*arguments*]

Repeats the most recently used CLI command that begins with the specified text string.

text-string can be a single letter or the entire first word in a recently executed CLI command.

arguments can be any other command arguments that you want to append to the command from the history.

Examples

```
!show
```

```
!ex
```

show

Description

Display information about a component of the current configuration or status. Due to the complexity of the show command, individual components are detailed below.

Syntax

show [*component*]

component must be a valid configuration component.

If **?** is used for component, returns a list of all valid configuration components.

This table is a list of show command components for which no options are available.

Component	Display
arp	ARP table
apt-blocker	Show Advanced Persistent Threat (APT) status
clock	System clock
csfc	Show whether CSfC mode is enabled (Fireware v12.6.2 or higher)
default-packet-handling	Default packet handling
dns	DNS servers
dnswatch	Show the DNSWatch configuration
dynamic-nat	Dynamic NAT
factory-default	Show whether the device is in a factory default state
fault-report	Show the current setting for the Fault Reports feature
features	Active licensed software features
file_exceptions	Show file exceptions list
gwc	Display Gateway Wireless Controller access points, settings, and SSIDs.
ikev2-shared-settings	Show IKEv2 shared settings for NAT traversal and Phase 1 transforms
link-monitor	Show the link monitor configuration (Fireware v12.3 or higher)
l2tp	Mobile VPN with L2TP configuration settings
locked-out	List of management and user accounts that are locked out
login-user	List of management users logged on to the Firebox
logon-disclaimer	Show the Logon Disclaimer dialog box settings

Component	Display
loopback	Loopback interface configuration
managed-client	Configure this Firebox as a managed client
mobile-security	Show the Mobile Security configuration settings
multi-wan	Multiple wide area network settings
mvpn-ikev2	Mobile VPN with IKEv2
netflow	Show the NetFlow configuration (Fireware v12.3 or higher)
network-mode	WatchGuard security appliance system mode
ntp	Network Time Protocol
one-to-one-nat	1-to-1 NAT settings for the Firebox
pac	Show the PAC (Proxy Auto-Configuration) file settings
policy-tag	Policy tags
proxy-action	Default proxy actions
quarantine-server	Quarantine Server status
reputation-enabled-defense	Reputation Enabled Defense feedback setting
rps	Receive Packet Steering (RPS)
signature-update	Signature update configuration information for security services
snmp	Simple Network Management Protocol (SNMP) settings
sslvpn	Secure Sockets Layer Virtual Private Network
static-arp	Static ARP entries added to the static ARP table
status-report	System health status
sysinfo	System information
threat-detection	Threat Detection and Response

Component	Display
	status (enabled or disabled)
tlsv13	Show whether TLS v1.3 is enabled (Fireware v12.6.2 or higher)
tor-exit-node-blocking	Show Tor Exit Node Blocking status (Fireware v12.8.1 or higher)
upgrade	The audit trail of software upgrade (s)
user-name-conflicts	Show user name conflicts
watchguard-cloud	Show WatchGuard Cloud status

Command components not on the list above are in the subsequent sections, with supported options.

show access-portal

Description

Display a summary of the Access Portal settings.

Syntax

show access-portal [*component*]

component must be one of these options:

app-group — Shows the application groups configured on the Access Portal
portal — Shows the Access Portal settings
url-mappings — Shows the reverse proxy actions configured on the Access Portal
user-access — Shows all Access Portal and Mobile VPN with SSL users
users — Shows all Access Portal users

show alias

Description

Display the aliases configured on the Firebox.

Syntax

show alias [*aliasname*]

aliasname is the name of the alias.

If *aliasname* is provided, the Firebox displays information about the specified alias. Otherwise, it displays summary information for all configured aliases.

show antivirus

Description

Show AntiVirus settings and statistics.

Syntax

show antivirus *component*

component must be one of these options:

settings — (Fireware v12.2 and higher) Shows AntiVirus global settings on devices that support IntelligentAV.

statistics — Shows statistics for Gateway AntiVirus and IntelligentAV scans since the last Firebox restart.

show app-control

Description

Display information about the Application Control configuration.

Syntax

show app-control [*action-name*]

action-name is the name of the Application Control action.

If *action-name* is provided, the Firebox displays information about the specified action. Otherwise, it displays information for all configured Application Control actions.

show auth-portal

Description

Display the current settings for the Authentication Portal page.

Syntax

show auth-portal

Shows the current settings for the Authentication Portal page.

show auth-server

Description

Display the authentication server configuration and status.

Syntax

show auth-server [*server-name*]

[*server-name*] is the name of the authentication server.

If [*server-name*] is provided, the Firebox displays information about the specified authentication server. Otherwise, it displays information for all configured authentication servers.

The server listed first in the list is the default authentication server on the user authentication page. Use the **auth-setting default-auth-server** configuration command to change the default authentication server.

show auth-setting

Description

Display the authentication settings.

Syntax

show auth-setting [*component*]

If *component* is not specified, displays a summary of all authentication settings.

component must be one of these options:

account-lockout — Shows the Account Lockout settings for user accounts that use Firebox-DB for authentication

auth-user-idle-timeout — Shows the maximum length of time a user can stay authenticated when idle (not passing traffic to the external network)

auth-user-session-timeout — Shows the maximum length of time a user can send traffic to the external network.

auto-redirect — Shows whether the Firebox is configured to send users who are not already authenticated to the authentication page

default-auth-server — Shows the authentication server selected by default on the authentication page.

mgmt-user-idle-timeout — Shows the maximum length of time a management user can stay authenticated when idle (not passing traffic to the external network)

mgmt-user-session-timeout — Shows the maximum length of time a management user can send traffic to the external network

mgmt-user-lockout — Shows the lockout status for the "status" Device Administrator account. To see the account lockout status and settings for other Device Management accounts, use the **show device-mgmt-user** command.

min-password-length — Shows the minimum password length for a Firebox-DB account.

same-user-multi-login — Show whether a user can log in multiple times simultaneously

single-sign-on — Show authentication settings for Active Directory single sign-on (SSO)

single-sign-on radius — Show authentication settings for RADIUS single sign-on (SSO)

terminal-service — Show authentication settings for terminal services

show auth-user-group

Description

Display information about authorized users and user groups.

Syntax

show auth-user-group [*name*]

name is the name of an authorized user or user group.

If *name* is provided, the Firebox displays information for only the specified user or user group. Otherwise, it displays information for all authorized users and user groups.

show backup-list

Description

Display information about backup images stored on the Firebox or a connected USB drive.

Syntax

show backup-list [from usb]

Displays information about the backup images saved on the Firebox.

If **[from usb]** is specified, displays information for backup images stored on a USB drive connected to the Firebox.

show botnet

Description

Display information about Botnet Detection.

Syntax

show botnet [*status*] [*allowed site*]

status is the status of Botnet Detection activity.

allowed site is a list of sites defined in the Botnet Detection exceptions list.

show bovpn-gateway

Description

Display the branch office VPN gateway configuration and status.

Syntax

show bovpn-gateway [*gatewayname*]

gatewayname is the name of the branch office VPN gateway.

If *gatewayname* is provided, the Firebox displays information for only the specified branch office VPN gateway. Otherwise, it displays information for all configured branch office VPN gateways.

show bovpn-tunnel

Description

Display the branch office VPN tunnel configuration and status.

Syntax

show bovpn-tunnel [*tunnel-name*]

tunnel-name is the name of the branch office VPN tunnel.

If *tunnel-name* is provided, the Firebox displays information for only the specified branch office VPN tunnel. Otherwise, it displays information for all configured branch office VPN tunnels and the associated branch office VPN gateway.

show bovpn-vif

Description

Display the BOVPN virtual interface configuration and status.

Syntax

show bovpn-vif [*BOVPN-vif-name*]

bovpn-vif-name is the name of the branch office VPN virtual interface.

If *bovpn-vif-name* is provided, the Firebox displays information for only the specified BOVPN virtual interface. Otherwise, it displays a list of all configured BOVPN virtual interfaces.

show bovpntls-client

Description

Display BOVPN over TLS clients configured to connect to this BOVPN over TLS server.

Syntax

show bovpntls-client (client)

(client) is the name of a BOVPN over TLS client.

If *client* is provided, the Firebox displays information for only the specified BOVPN over TLS client. Otherwise, it displays information for all configured BOVPN over TLS clients.

show bridge

Description

Display the Bridge virtual interface configuration and status.

Syntax

show bovpn [*bridge-name*]

bridge-name is the virtual interface name.

If *bridge-name* is provided, the Firebox displays information for only the specified virtual interface. Otherwise, it displays information for all configured bridge interfaces.

show categories

Description

Display the Application Control categories and applications in each category.

Syntax

show categories [*category-name*]

category-name is the name of the Application Control category.

If *category-name* is provided, the Firebox displays information about applications in the specified category. Otherwise, it displays a list of all Application Control categories.

show certificate

Description

Display the certificates available in the Firebox.

Syntax

show certificate [*component*]

If *component* is not provided, shows information about all certificates on the Firebox. *component* must be one of these options:

int — Certificate ID <10000-99999>
fingerprint *ident* — Certificate fingerprint
name *certificate name* — Name of the entity
type common — Show certificates without the trusted CAs for HTTPS proxy
type trusted-https-proxy — Show the trusted CAs for the HTTPS Proxy

show cluster

Description

Display information about FireCluster status.

Syntax

show cluster status [**member** *name*]

Shows the current status and roles of the FireCluster members.

member (*name*) — Shows status information for the specified member. *name* must be the name of the cluster member. If member is not specified, the command shows the status of both members.

show cluster sync [*option*] [**member-id** *id-no*] [**timeout** *timeout*]

Show the status of cluster synchronization.

option must be one of these options:

cluster — cluster data, including the configuration, feature keys, certificates, password, alarms, and DHCP

gateway — external interface gateway status

host-mapping — related hosts (for a cluster configured in drop-in mode)

hostile-sites — blocked sites list

signatures [*sig-type*] — security service signatures. *sig-type* must be one of these options:

gav — Gateway AntiVirus signatures

ips — Intrusion Prevention Service and Application Control signatures

If *sig-type* is not specified, the signatures option shows the synchronization status of all signature types.

member-id(*id-no*) — If specified, shows synchronization status for the specified member. *id-no* must be the serial number of the cluster member. If member id is not specified, the command shows the synchronization status of all members.

timeout (*timeout*) — Specifies the amount of time in seconds to wait for a synchronization response. The default value is 10 seconds.

show connection

Description

Display the current connections to the Firebox.

Syntax

show connection count [**by policy** [*policy-name*]]

Show the current number of connections to the Firebox.

by-policy *policy-name* — If specified, shows the connection counts for all policies or for specified policies. *policy-name* is the name of a configured policy. The policy name is case sensitive. You can specify more than one policy name, separated by spaces. If *policy-name* is specified, the by-policy command option shows connection counts only for the specified policies.

show data-loss-prevention

Description

Display information about the configuration of the Data Loss Prevention (DLP) service.

Syntax

show data-loss-prevention [*component*]

If *component* is not specified, shows whether DLP is enabled.

component must be one of these options.

notifications — show the configured DLP notification settings.

sensors *sensor-name* — show information about configured DLP sensors. If *sensor-name* is specified, show the configuration details for the specified sensor. If *sensor-name* is not specified, shows a list of sensors.

statistics — show the installed signature version, the last update date, and the statistics about DLP activity that occurred after the last Firebox restart.

show ddns

Description

Display the dynamic DNS service configuration information.

Syntax

show ddns [*type*]

type is the dynamic DNS service type. The only valid string is DynDNS.

show device-mgmt-user

Description

Display the current list of Device Management user accounts configured on the Firebox.

Syntax

show device-mgmt-user

Displays a list of Device Management user accounts, the authentication server, user role, and lockout status. For Fireware v11.12 and higher, this command also shows the global account lockout settings configured for Device Management user accounts.

show dhcp

Description

Display the DHCP configuration information.

Syntax

show dhcp leases

In Fireware v12.7 or higher, use this command to see information about the IPv4 DHCP configuration. This includes the subnet configured for DHCP leases, the total number of DHCP leases ("count"), and the total number of DHCP leases in use ("leased").

show external-auth-hotspot

Description

Display the current hotspot settings for the Firebox.

Syntax

show external-auth-hotspot

Shows the current configuration settings for the hotspot when it is configured to use an external web server.

show feature-key

Description

Display information about the feature key on the Firebox.

Syntax

show feature-key [*feature-key-id*]

feature-key-id is the feature key ID.

If *feature-key-id* is provided, this command displays information about features enabled by the specified feature key. Otherwise, it displays the feature key ID and expiration dates for all feature keys.

show fqdn

Description

Display information about the FQDN (Fully Qualified Domain Name) feature.

Syntax

show fqdn [*cache*] [*limited*]

Displays the FQDN cache of domains and IP address mappings. For *limited* cache display, you can enter a full or partial domain name.

show fqdn [*status*]

Displays the status of the FQDN feature.

show geolocation

Description

Display the geolocation settings configured on the Firebox, or look up the geolocation of an IP address.

show geolocation [*component*]

If *component* is not specified, shows whether geolocation is enabled and a list of geolocation actions configured on the Firebox.

component must be one of these options.

action *(action-name)* — Show geolocation action details.

blocked-country — Show the list of blocked countries.

continent (*continent-name*) — Show the status of geolocation for all countries in the specified continent. *continent-name* is case-sensitive, and must be one of these options: Africa, Antarctica, Asia, Europe, "North America", Oceania, "South America".

country (*country-name*) — Show the status of geolocation for all countries or a specific country. *country-name* is case-sensitive.

exceptions — Show the configured exceptions for geolocation blocking.

ip-lookup (*address*) — Look up the geolocation of the specified IPv4 or IPv6 address.

status — Show geolocation activity since the last restart and geolocation signature version information.

show global-setting

Description

Display the global settings configured on the Firebox.

Syntax

show global-setting [*component*]

If *component* is not specified, shows all global settings configured on the Firebox.

component must be one of these options.

auto-reboot — Show whether automatic reboot is enabled, and the scheduled reboot day and time

device-admin-connections — Show whether more than one Device Administrator can log in at the same time: Enabled or Disabled.

fault-report — Show the current setting for the Fault Reports feature: Enabled or Disabled.

hostout-traffic-control — Show the current setting for the feature that allows you to control Firebox-generated (hostout) traffic: Enabled or Disabled.

icmp-message — Show global settings for ICMP error handling

quota — Show the current settings for bandwidth and time quotas: Enabled or Disabled.

report-data — Show the current setting for the Device Feedback feature: Enabled or Disabled.

tcp-close-timeout — Show the current settings for the TCP close timeout value.

tcp-connection-timeout — Show global settings for TCP connection timeout.

tcp-mss-adjustment — Show the current setting for the TCP maximum segment size adjustment.

tcp-mtu-probing — Show the current setting for TCP MTU probing: Enabled or Disabled.

tcp-syn-checking — Show the global settings for TCP SYN checking and TCP maximum segment size (MSS) adjustment

tcp-time-wait-timeout — Show the current setting for the interval to remove closed connections from the connection table.

traffic-flow — Show the current settings for the action to take to clear existing connections when the static NAT configuration changes

traffic-management — Show whether traffic management and QOS features are enabled

udp-stream-timeout — Show the current setting for the UDP stream timeout value.

udp-timeout — Show the current setting for the UDP timeout value.

webui-port — Show the port used to connect to Fireware Web UI.

show gwc

Description

Display the current Gateway Wireless Controller settings.

Syntax

show gwc settings

Shows the current settings for the Gateway Wireless Controller.

show gwc access-points *name*

Shows the current settings for the access points managed by this Gateway Wireless Controller. You can also specify an access point name.

show gwc ssids *name*

Shows the current settings for the Gateway Wireless Controller SSIDs. You can also specify an SSID name.

show hotspot

Description

Display the current hotspot settings for the Firebox.

Syntax

show hotspot [**name** *hotspot-name*]

Shows the current configuration settings for configured hotspots.

hotspot-name is the name of a hotspot.

If *hotspot-name* is provided, this command displays detailed information for only the specified hotspot.

If *hotspot-name* is not provided, the command displays summary information for all hotspots.

show hotspot users

Description

Display a list of the current users connected to the hotspot.

Syntax

show hotspot users

Shows the list of users who are currently connected through the hotspot.

show interface

Description

Display the physical interface configuration and status.

Syntax

show interface [*interface-number*]

interface-number is the network interface number. *interface-number* must represent a valid number for the Firebox.

If *interface-number* is provided, the Firebox displays detailed information for only the specified interface, including the IPv6 address, if IPv6 is enabled for that interface, and the interface is active.

If *interface-number* is not provided, the Firebox displays summary information for all interfaces.

show intrusion-prevention

Description

Display configuration settings and signatures for the Intrusion Prevention Service (IPS).

Syntax

show intrusion-prevention (*component*)

component is one of these options:

exception — Show configured IPS exceptions.

ips-statistic — Show Intrusion Prevention Service statistics and configured scan mode.

notification — Show IPS notification settings.

settings — Show IPS configuration settings.

signature-list all — Show information about all IPS signatures.

signature-list signature-id *idnum* — Show information about a specific IPS signature. *idnum* is the signature ID number.

show ip

Description

Display the Internet Protocol settings or routes for the selected component.

Syntax

show ip (*component*)

component is one of these options:

allowed-site — Show IP addresses on the blocked site exceptions list

blocked-port — Show the blocked ports list and alarm settings

blocked-site — Show IP addresses on the blocked sites list

dns — Show settings for IP domain name service resolver

dynamic-routing (*protocol*) — Show dynamic routing information for the specified dynamic routing protocol; *protocol* must be **bgp**, **ospf**, **ospf v3**, **rip**, or **rip ng**.

multicast — Show the multicast routing configuration

route— Show the multicast route table

route [*route-filter*] — Show the IPv4 route table. If you do not specify a *route-filter*, this command shows the first 100 routes. Specify a *route-filter* to show only routes of the specific type. *route-filter* must be one of these options:

destination — show only routes to the specified destination network address. *destination* must be an IPv4 network address in the format of A.B.C.D/# where # is in the range of 8 to 32.

connected — show only routes to directly connected subnets

dynamic — show only dynamic routes

ifname (*name*) — show only routes that use the specified interface. *name* must exactly match the interface name as it appears in the route table in the CLI. For example, eth1, bond0, vpn10, etc. The name is case sensitive.

static — Show only static routes

vpn — Show only BOVPN virtual interface routes

static-route — Show the configured static routes

vpn-routes — Show the configured BOVPN virtual interface routes

wins — Windows Internet Naming Service

show link-aggregation

Description

Display the link aggregation interface configuration and status.

Syntax

show link-aggregation [*interface-name*]

interface-name is the name of the link aggregation interface.

If *interface-name* is provided, the Firebox displays information about the specified link aggregation interface. Otherwise, it displays summary information for all configured link aggregation interfaces.

show link-monitor

Description

Display the Link Monitor configuration.

Syntax

show link-monitor

Show the Link Monitor settings for interfaces added to Link Monitor.

show log-cache

Description

Display the internal temporary log repository for Traffic Monitor.
You can use the command options together to limit the entries that appear.

Syntax

show log-cache [**count** *number*] [**key** *pattern*] [**sequence** *startpoint*] [**tail** *number*]

If no options are specified, shows the entire contents of the log cache.

count *number*

Limit the number of log entries to display. *number* is the number of log entries to include. It must be an integer from 1 to 10000.

key *pattern*

Show the log entries that include the specified pattern.

pattern is the pattern of text to match.

sequence *startpoint*

Show log entries from a specified start point of the log repository.

startpoint is the starting sequence number of the log entries to include.

tail *number*

Show log entries backward from the end of the internal log repository.

number is the maximum number of log entries to include. It must be an integer from 1 to 10000.

show log-setting

Description

Display the log settings for a specified component.

Syntax

show log-setting [*component*]

If *component* is not specified, shows the log settings for all components.

component is one of these options.

firebox-itself-logging — Enable logging of traffic sent by the Firebox
log-level — Diagnostic log level
ike-packet-trace — Internet Key Exchange packet trace
internal-storage — Internal storage
performance-statistics — Performance statistics to see in the log file
security-service-statistics — Statistics for security services
syslog-server — Syslog server
watchguard-log-server — WatchGuard Log Server

show modem

Description

Display information about the modem configuration.

Syntax

show modem

Show the modem configuration settings.

(Fireware v12.0.2 and lower) If *link-monitor* is specified, the Firebox displays the link monitor configuration settings the Firebox uses to check the status of each external interface.

show mvpn-ipsec

Description

Display information about the Mobile VPN with IPSec group configuration.

Syntax

show mvpn-ipsec [*group-name*]

group-name is the name of the Mobile VPN with IPSec user group.

If *group-name* is provided, the Firebox displays detailed configuration information for the specified group Mobile VPN with IPSec connection. Otherwise, it displays a list of all configured Mobile VPN with IPSec connections.show mvpn-ipsec

show mvpn-rule

Description

Display information about the Mobile VPN with IPSec policies

Syntax

show mvpn-rule [**mvpn-group** *group-name*]

Display configured Mobile VPN with IPSec connections for a Mobile VPN with IPSec group.

group-name is the name of the Mobile VPN with IPSec user group. It is case-sensitive.

show mvpn-rule [**name** *policy-name*]

Display settings for a Mobile VPN with IPSec policy.

policy-name is the name of the Mobile VPN with iPSec policy. It is case-sensitive.

show network-scan

Description

Display information about the scan configuration for the Network Discovery feature.

Syntax

show network-scan

show policy-type

Description

Display information about policy templates.

Syntax

show policy-type (*template-name*)

template-name is the name of the policy template. It is case-sensitive.

If *template-name* is provided, the Firebox displays information for only the specified policy template. Otherwise, it displays a list of all policy templates.

show pppoe

Description

Display information about external interfaces configured to use PPPoE authentication.

Syntax

show pppoe (*name*)

name is the name of an external interface configured to use PPPoE authentication.

To see a list of all external interfaces configured to use PPPoE authentication, type **show pppoe** and a carriage return only.

show proposal

Description

Display the settings for the specified branch office VPN IPSec proposal.

Syntax

show proposal (*proposal-number*) [*proposal-name*]

proposal-number must be one of these options:

p1 — Phase 1 proposal

p2 — Phase 2 proposal

proposal-name is the name of the proposal. It is case-sensitive. If proposal-name is specified, it displays the settings for that proposal. Otherwise it displays a list of proposals for the specified proposal number.

show proxy-action

Description

Display the configured proxy actions.

Syntax

show proxy-action

Show the default and configured proxy-actions.

show quota

Description

Display the settings for bandwidth and time quotas.

Syntax

show quota-action (*name)*

Show the quota action settings. You can specify a quota action name.

show quota-exception

Show the configured quota exceptions.

show quota-report

Show the run-time quota report.

show quota-rule (*name)*

Show the quota rule settings. You can specify a quota rule name.

show reputation-enabled-defense

Description

Display information about Reputation Enabled Defense feature.

Syntax

show reputation-enabled-defense

Show the status of the Reputation Enabled Defense feature.

show rule

Description

Display information about the policies configured for the Firebox.

Syntax

show rule [*rule-name*]

rule-name is the name of a policy. It is case-sensitive.

If *rule-name* is provided, the Firebox displays the configuration settings for the specified policy. Otherwise, it displays a list of all configured policies.

show sd-wan

Description

Display information about SD-WAN actions and status.

show sd-wanaction

Show a list of SD-WAN actions configured on the Firebox.

show sd-wan action *(action name)*

Show the configuration for the specified SD-WAN action.

show sd-wan status

Show the mode, interfaces, status, failover method, and failback method for each SD-WAN action.

The mode is automatically determined by the configured multi-WAN method. The mode can be one of these options: Routing Table, Failover, Interface Overflow, or Round Robin.

An interface can have one or more of these status indicators:

A — Active. This is the active interface.

Q —Qualified. An interface is qualified if it is up and has metrics that do not exceed the loss, latency, and/or jitter values you specified in the SD-WAN action.

P — Preferred. The primary interface is the preferred interface if it is up and has metrics that do not exceed the values you specified. The primary interface is the first interface in the list in the SD-WAN action. In the SD-WAN action configuration, you can move interfaces up or down in the list to change the primary interface.

Method indicates whether metric-based failover (M) is configured, and whether connections are configured to fail over immediately (I) or gradually (G). If metric-based failover is not configured, the up/down status of the interface is used for failover.

Failback indicates whether connections are configured to fail back immediately, gradually, or never.

show signature-update

Description

Display the status of signature updates for security services.

Syntax

show signature-update

Show information on signature-updates for IPS, Gateway AV, and DLP.

show snat

Description

Display information about configured static NAT or server load balancing SNAT actions.

Syntax

show snat [*snat-action*]

snat-action is the name of a configured SNAT action. It is case-sensitive.

If *snat-action* is provided, the Firebox displays configuration information for the specified SNAT action. Otherwise, it displays a list of all configured SNAT actions.

show spamblocker

Description

Display settings for the spamBlocker security service.

Syntax

show spamblocker [*component*]

component is the name of a component of the spamBlocker settings. If *component* is provided, the command output shows configuration settings for the specified configuration component. Otherwise, it displays all spamBlocker configuration settings.

component must be one of these options:

http-proxy-server — settings for connecting to the spamBlocker Server using an HTTP proxy server

settings — general spamBlocker settings

trusted-email-forwarders — host names or domain names for trusted SMTP or POP3 providers

show stp

Description

Display information about the Spanning Tree Protocol configuration.

Syntax

show stp [bridge-name]

[*bridge-name*] is the name of a bridge on the Firebox. For a Firebox configured for Bridge mode, specify the value `0`. For a network bridge, specify the name of the bridge.

show sys-storage

Description

Display system storage information for the Firebox.

Syntax

show sys-storage

Show the total storage capacity, the amount of storage used, and the amount of storage available on the Firebox.

show traffic-management

Description

Display settings for traffic management.

Syntax

show traffic-management [*action-name*]

action-name is the name of a configured traffic management action.

If *action-name* is provided, the Firebox displays information for only the specified traffic management action. Otherwise, it displays a list of all configured traffic management actions.

show trusted-ca-certificates

Description

Display the status of trusted CA certificate updates on the Firebox.

Syntax

show trusted-ca-certificates [*automatic-update*]

Indicates if automatic CA certificate updates are disabled or enabled.

show update-history

Description

Display the signature update history for signature-based security services.

Syntax

show update-history [*signature-type*]

signature-type must be one of these options:

av-sig — Gateway Anti-Virus signature update history
botnet — Botnet signature update history
dlp — Data Loss Prevention signature update history
ews — EWS signature update history
geolocation — Geolocation signature update history
ips — IPS and Application Control signature update history

show usb

Description

Display information about the attached USB drive.

Syntax

show usb [*component*]

component must be one of these options:

auto-restore — Show information about the auto-restore image stored on the USB drive.

diagnostic status — Show information about the diagnostic image stored on the USB drive.

flash-image — Show a list of saved backup image files stored on the USB drive.

support-file — Show information about the support snapshot stored on the USB drive.

show user-group

Description

Display information about Firebox authentication user groups.

Syntax

show user-group [*group-name*]

group-name is the name of a user group.

If *group-name* is provided, the Firebox displays a list of the users in the specified group. Otherwise, it displays a list of all user groups configured for Firebox authentication.

show users

Description

Display information about users configured for Firebox authentication.

Syntax

show users [*name*]

name is the name of a user.

If *name* is provided, the Firebox displays information for only the specified user. Otherwise, it displays information for all users configured for Firebox authentication.

show v6

Description

Display information about IPv6 network routes or route configuration.

Syntax

show v6 ip [*component*]

component is one of these options:

route (*route-filter*) — Show the IPv6 route table. If you do not specify a *route-filter*, this command shows the first 100 routes. Specify a *route-filter* to show only routes of the specific type. *route-filter* must be one of these options:

subnet — show only routes to the specified destination subnet. *subnet* must be an IPv6 subnet in the format A:B:C:D:E:F:G:H/I.

connected — show only routes to directly connected subnets

dynamic — show only dynamic routes

ifname (*name*) — show only routes that use the specified interface. *name* must exactly match the interface name as it appears in the route table in the CLI. For example, eth1, bond0, vpn10, etc. The name is case sensitive.

static — Show only static routes

vpn — Show only BOVPN virtual interface routes

static-route — Show the configured IPv6 static routes

vpn-routes — Show the configured IPv6 BOVPN virtual interface routes

show vlan

Description

Display information about a VLAN. Information about the Spanning Tree Protocol configuration is included.

Syntax

show vlan [*VLAN-name*]

Display information about the specified VLAN.

show vpn-setting

Description

Display global settings for virtual private networking.

Syntax

show vpn-setting [**ldap**]

Show the IPSec and LDAP VPN global settings.

If **ldap** is specified, the Firebox displays the LDAP server settings in the global VPN settings.

show vpn-status

Description

Display the status of VPN connections

Syntax

show vpn-status bovpn gateway [*gateway-name*]

Show the status of branch office VPN connections.

gateway-name is the name of a branch office VPN gateway. If *gateway-name* is specified, the Firebox displays status for the named branch office VPN gateway.

show vpn-status l2tp (**auth-user**|**session**)

Show the status of Mobile VPN with L2TP connections.

If **auth-user** is specified, the Firebox displays a list of L2TP authenticated users.

If **session** is specified, the Firebox displays a list of Mobile VPN with L2TP sessions.

Use the **no vpn-status l2tp** command to disconnect a Mobile VPN with L2TP session.

show web-server-cert

Description

Display information for the web server certificate on the Firebox.

Syntax

show web-server-cert

Show the web server certificate installed on the Firebox.

show wireless

Description

Display the wireless settings and status for a WatchGuard wireless device.

Syntax

show wireless

Show the configuration for all wireless interfaces.

show wireless ap (*number*)

Show the configuration for a wireless access point.

number must be **1**, **2**, or **3**.

show wireless client

Show the configuration of wireless client as an external interface.

show wireless status

Show the wireless network and radio settings.

show wireless rogue-ap

Description

Display the wireless rogue access point detection settings and status for a WatchGuard wireless device.

Syntax

show wireless rogue-ap (*component*)

component must be one of these options:

scan-result — Show the result of the most recent rogue access point detection scan.

scan-status — Show whether a scan is currently running.

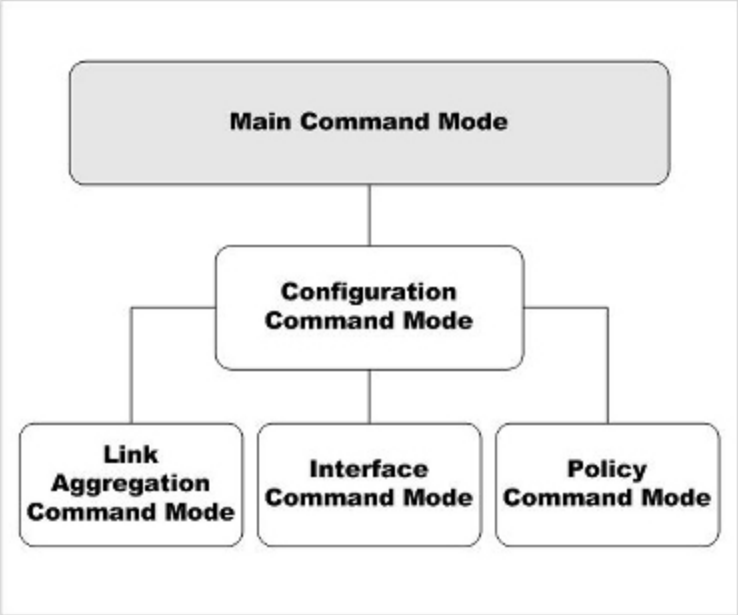
schedule — Show the schedule for automatic scans.

trust-ap (*index*) — Show a list of all trusted access points. *index* is the index number that appears in the list of trusted access points. If *index* is provided, the Firebox shows details about the specified trusted access point.

4 Main Command Mode

Main Commands

The Main command mode is the default mode of the WatchGuard Command Line Interface (CLI).



In the Main mode, you can:

- Modify some higher level configuration settings
- Enter the Configuration command mode
- Restore or upgrade the software image
- Shut down or reboot the Firebox

Enter the Main Command Mode

There are two methods to enter the Main command mode:

- Start the Command Line Interface
- Use the **exit** command while in the Configuration command mode

When you enter the Main mode, the prompt changes based on which type of user account you use to log in.

WG#

This prompt indicates that you have logged with the default **admin** user account, or another user account that has Device Administrator (read-write) permissions.

WG>

This prompt indicates that you have logged in with the default the read-only **status** user account, or another user account that has Device Monitor (read-only) privileges.

List of Main Mode Commands

You can use all common commands in the Main command mode. For more information, see *About Common Commands*.

In addition, these commands are available only in the Main mode:

Command	Usage
arp	Clear the ARP cache of all entries.
backup	Save a backup image to the Firebox or a connected USB drive.
cache-flush	Flush the scan cache for APT Blocker and Gateway AntiVirus services.
cert-request	Use the Firebox to create a security certificate.
clock	Manage and change the system clock.
configure	Enter the Configuration command mode.
debug-cli	Configure debugging options.
delete	Delete backup images from the Firebox.
device-mgmt-user	Configure Device Management user accounts on the Firebox.
diagnose	Show internal diagnostic information.
dnslookup	Domain name resolution.
exit	Exit the CLI or return to the previous command

Command	Usage
	mode.
export	Export information to an external platform or file.
fault-report	Show and manage the Fault Reports on the Firebox.
fqdn	Manage the FQDN (Fully Qualified Domain Names) feature.
gwc	Manage the Gateway Wireless Controller.
help	Descriptions of the available commands for the current mode.
history	Show the command history list with line numbers.
import	Import information from an external platform or file.
mgmt-user-unlock	Unlock a locked Device Management user account.
no	Negate a command or set the defaults for a command.
password	Change the passphrase for the Device Management user connected to the device.
ping	Send a ping request to the specified IP address.
policy-check	Check which policy in the configuration handles traffic for a specified interface, protocol, source, and destination.
quota-reset	Reset the quota for a user or quota action.
reboot	Stop all processing and do a cold restart of the device.
rps	Enable or disable Receive Packet Steering (RPS).
restore	Restore the device to a backup image or factory-default configuration.
show	Show current system information.
shutdown	Shut down the device.
signature-update	Signature update information. *Internal use only.*

Command	Usage
sync	Retrieve the feature key, RSS feed, or device wireless region from the WatchGuard LiveSecurity server.
sysinfo	Show the device system information.
tcpdump	Dump traffic on the network.
traceroute	Examine and display the route to a specified destination.
trusted-ca-certificates	Update and install the trusted CA certificates on your device.
unlock	Unlock locked user accounts
upgrade	Upgrade the Fireware OS.
upgrade certificate	Upgrade the default Firebox certificates to SHA-256.
usb	Save a back up a flash disk image or diagnostic file to the USB drive attached to the device.
vpn-tunnel	Force the rekey of a branch office VPN gateway.
who	Show a list of Device Management users who are logged in to the device.

Main Command Mode Reference

arp flush

Description

Clear the ARP cache of all entries.

Syntax

arp flush

No options available.

backup image

Description

Save a backup image to the Firebox or a USB drive.

Syntax

backup image (*filename*)

Save a backup image to the Firebox.

filename is the name to use for the saved backup image file.

backup image (*filename*) [**to usb** (*password*) **yes**|**no**]

Save a backup image to a connected USB drive.

filename — the name to use for the saved backup image file.

to usb — Specify **to usb** to save the backup image on the USB drive that is connected to the Firebox.

password — the password to use to encrypt the backup image saved to a USB drive.

Use **yes** or **no** to specify whether to include the Fireware OS in the backup image.

Examples

```
backup image backup-10-29-18.fxi
```

```
backup image backup-10-29-18.fxi to usb password yes
```

cache-flush scan

Description

Flush the scan cache for APT Blocker and Gateway AntiVirus services.

Syntax

cache-flush scan

No options available.

cert-request

Description

Use the Firebox to create a security certificate.

Syntax

cert-request (*purpose*) (*commonname*) (*companyname*) (*dnsname*) [**country** (*countryname*)] [**state** (*statename*)] [**city** (*cityname*)] [**department** (*deptname*)] [**address** (*deviceaddress*)] [**domain** (*domain*)] [**algorithm** (*key-type*)] [**length** (*key-length*)] [**usage** (*key-usage*)]

purpose must be one of these options: proxy-authority, proxy-server, ipsec-web-server-other.

commonname is the certificate common name.

companyname is a string that identifies the issuer of the certificate. This should be your company name.

dnsname is the fully qualified domain name.

countryname is a string that identifies the country of origin. The default is US.

statename is a string that identifies the state or province of origin, ST.

cityname is a string that identifies the city or location of origin.

deptname is a string that identifies the department of origin within a larger organization, OU.

deviceaddress is an IP address that identifies the device of origin.

domain is the domain name of the company of origin.

key-type must be either dsa or rsa. The default is RSA.

key-length must be either length-1024 or length-2048

key-usage is optional for ipsec-web-server-other only. If you use DSA encryption, the value must be signature. If RSA encryption, the value must be one of these options: encryption, signature, or both.

Examples

```
cert-request proxy-authority ExampleCompanyAcct ExampleCompany
www.example.com country US
```

```
cert-request proxy-server ExampleCompanyAcct ExampleCompany www.example.com
country US state Maine department Accounting address 200.202.12.3 domain
www.example.com algorithm dsa length 1024
```

clock

Description

Manage and change the system clock.

Syntax

clock [**time** *time*] [**date** *date*]

time is in the format: HH:MM:SS. The selection of AM or PM is not supported. The hours must be entered in the range 0 to 23.

date is in the format MM/DD/YYYY. Leading zeroes are not required in the month and day fields.

Examples

```
clock time 11:30:56 date 12/1/2012
```

cluster

Description

Control the operation of a FireCluster.

Syntax

cluster [*operation*]

Control the operation of the cluster.

operation is the command you want to send to the cluster. It must be one of these options.

discover — Discover a new cluster member. When the cluster master discovers a connected device that is operating in safe mode, it checks the serial number of the device. If the serial number matches the serial number of a cluster member in the FireCluster configuration, the cluster master loads the cluster configuration on the second device. That device then becomes active in the cluster. The second device synchronizes all cluster status with the cluster master.

failover — Force a failover of the cluster master. The cluster master fails over and the backup master becomes the cluster master.

reboot [*member-name*] — Restart a cluster member. *member-name* is the cluster member name. It is case sensitive.If *member-name* is not specified, this command restarts both members.

reset [*member-name*|**all**] — Reset a cluster member to factory-default settings. *member-name* is the cluster member name. It is case sensitive.Specify all to reset both cluster members. If you connect to the cluster master, you can reset either member or all members. If you connect to the backup master, you can reset only the backup master.

shutdown [*member-name*] — Shut down a cluster member. *member-name* is the cluster member name. It is case sensitive. If *member-name* is not specified, this command shuts down both members.

cluster sync [*sync-option*]

Force the synchronization of configuration and data from the cluster master to the backup master.

If *sync-option* is not specified, all items are synchronized.

sync-option specifies what to synchronize. It must be one of these options:

alarms — alarms and notifications

certificates — certificates

configuration — all device configuration settings

dhcp — DHCP leases

gateway — external interface gateway status

host-mapping — related hosts (for a cluster configured in drop-in mode)

hostile-sites — blocked sites list

licenses — feature keys

password — Firebox configuration and status passphrases

signatures [*sig-type*] — security service signatures. *sig-type* must be one of these options:

gav — Gateway AntiVirus signatures

ips — Intrusion Prevention Service and Application Control signatures

If *sig-type* is not specified, the signatures option synchronizes all signature types.

Use **show cluster sync** to see the current synchronization status.

Examples

```
cluster failover

cluster shutdown Member1

cluster sync

cluster sync configuration

cluster sync signatures gav
```

configure

Description

Enter the Configuration command mode.

Syntax

configure

No options available.

csfc

Description

Enable CSfC mode. CSfC mode supports operation of the Firebox in compliance with US National Security Agency (NSA) Commercial Solutions for Classified (CSfC) requirements. This command is available in Fireware v12.6.2 and higher.

Syntax

csfc enable

Enable the device to operate in CSfC mode. When you use this command, the Firebox automatically reboots.

When the device operates in CSfC mode, each time the device is powered on, it runs a set of integrity checks required for Common Criteria CSfC compliance. If a check fails, the Firebox writes a message to the log file and shuts down.

To disable CSfC mode, use **no csfc enable**.

Example

```
csfc enable

no csfc enable
```

debug-cli

Description

Configure debugging options.

Syntax

debug-cli (**critical**|**error**|**warning**|**info**|**debug**|**dump**)

Set debug logging to the specified level.

Examples

```
debug-cli critical
```

delete

Description

Delete a backup image.

Syntax

delete backup (*filename*) **[from usb]**

Delete a backup image file.

filename — the name of the backup image file to delete

from usb — Specify **from usb** to delete a backup image that is stored on a USB drive connected to the Firebox. Otherwise, the backup image is deleted from the Firebox.

Examples

```
delete backup backup_10_30_18
```

```
delete backup backup_10_30_18 from usb
```

device-mgmt-user

Description

Add, edit, and disable Device Management user accounts for users to connect to the Firebox to manage and monitor the device. You can add user accounts with the *Device Monitor* role (read-only privileges) or the *Device Administrator* role (read-write privileges). When you add a user account you specify the user name and password for the user account, and the authentication server to use for the account. You can also change the password or disable an existing user account. Passwords must have 8–32 characters.

Syntax

device-mgmt-user (*name*) (*authentication server*) **password** (*passphrase*) **role** (*Device-Administrator | Device-Monitor | or Disabled*)

Add or edit a Device Management user account on the Firebox.

name this is the user name for the user account.

authentication server this is the authentication server where the user account is stored:

- Firebox-DB
- Active Directory
- LDAP
- RADIUS

An external authentication server (any authentication server other than Firebox-DB) must be configured in the Authentication Server settings on the device before you can use it to authenticate Device Management users.

password is the passphrase for the user account. This option must only be specified if the authentication server is Firebox-DB. The password must be between 8 and 32 characters.

role must be Device-Administrator, Device-Monitor, or Disabled.

To edit an existing user account, specify an existing user name and change the password or role parameters.

Examples

```
device-mgmt-user admin Firebox-DB password readwrite role Device-
Administrator
```

```
device-mgmt-user JSmith Active Directory role Device-Administrator
```

```
device-mgmt-user JSmith Active Directory role Disabled
```

diagnose

Description

Display diagnostic information about a component. Because of the complexity of the diagnose command, individual components are detailed below.

The diagnose command supports additional parameters not documented here. Use those options only if a WatchGuard Support representative instructs you to do so.

Syntax

diagnose (*component*)

component must be a valid command parameter. If ? is used for component, returns a list of all valid strings for component.

diagnose to

Description

Specify an external location to send diagnostic information.

Syntax

diagnose to (*location*)

Send diagnostic information of a device to an external location.

location must be either an FTP or TFTP address.

diagnose auth-server

Description

Test the connection from the Firebox to an Active Directory or LDAP authentication server. You can also use this command to determine the authentication status of a user in the authentication server database, and to get authentication group information for that user.

Syntax

diagnose auth-server (*server*) [*username* [*password*]]

server is the authentication server. It must be **LDAP** for an LDAP server, or the domain name of an Active Directory server.

username is the name of the user on the authentication server.

password is the password on the authentication server for the specified *username*.

The command functions differently, depending on which parameters you include.

If only *server* is specified, this command tests only whether the Firebox can connect to the specified LDAP or Active Directory authentication server.

If only *server* and *username* are specified, this command tests the connection to the authentication server, searches for the specified user on the authentication server, and retrieves the group membership information for the specified user from the authentication server.

If *server*, *username*, and *password* are all specified, this command tests the connection to the authentication server, searches for the specified user, retrieves the group membership information, and tests whether the specified *password* is correct for this user on the authentication server.

Examples

```
diagnose auth-server ldap
diagnose auth-server example.org jsmith
diagnose auth-server example.org jsmith psw00rd159
```

diagnose cluster

Description

Specify an external location to send diagnostic information about a FireCluster.

Syntax

diagnose cluster to (*location*)

Send diagnostic information of a cluster of WatchGuard devices to an external location.

location must be either an FTP or TFTP address.

diagnose dynroute

Description

Display diagnostic information for dynamic routes. The **diagnose dynroute** command supports most Quagga vty shell commands. However, we recommend that you do not use **diagnose dynroute** with Quagga vty shell commands that modify the routing table. Instead, update the dynamic routing configuration file, and use the **import route-config** command to import the dynamic routing configuration to the Firebox.

The vtysh command must be enclosed in quotation marks.

For a list of Quagga commands, see Quagga Routing Suite.

Syntax

diagnose dynroute (*vtysh command*)

"show ip ospf" — Display information about OSPF dynamic routes currently in the route table.

"show ip route" — Display information about the dynamic routes currently in the route table.

Examples

```
diagnose dynroute "show ip ospf"
diagnose dynroute "show ip route"
```

diagnose fqdn

Description

Perform diagnostics for the FQDN (Fully Qualified Domain Names) feature.

Syntax

diagnose fqdn "*parameter*"

Perform diagnosis of the FQDN feature based on the specified parameter.

/fqdnd/status — Display the status of FQDN.

/fqdnd/cache/dump — Display the FQDN and IP mapping cache for all entries or a specific FQDN.

/fqdnd/policycheck — (Fireware v12.1.3 or lower) Check for conflicts in your current FQDN policy configuration.

/fqdnd/autodiag — Perform automatic diagnostic on FQDN services.

/fqdnd/dyninfo — Display DNS query information.

/fqdnd/keyevents — Display key FQDN events such as DNS query failures.

/fqdnd/log_filter/list — Display log levels for FQDN services.

/fqdnd/log_filter/set — Set log levels for FQDN services.

/fqdnd/running_parameter/list — Display DNS query parameters.

/fqdnd/running_parameter/set — Set DNS query parameters.

/fqdnd/policy_test_ip — (Fireware v12.3 or lower) Test your FQDN configuration for a specific source or destination IP address. In Fireware v12.3.1 or higher, this command was renamed to **fqdn /fqdnd/test_ip**.

/fqdnd/policy_test_domain — (Fireware v12.3 or lower) Test your FQDN configuration for a specific source or destination FQDN. In Fireware v12.3.1 or higher, this command was renamed to **fqdn /test_domain**.

/fqdnd/refresh — Refresh the FQDN and IP mapping cache for all entries or a specific FQDN.

/fqdnd/save_wildcard_domain_labels — Save domain and IP mappings to flash memory so they can be recovered after a system restart.

Example

```
diagnose fqdn "/fqdnd/status"
```

diagnose hardware

Description

Perform diagnostic tests and display hardware diagnostic information for a Firebox. Some command options do not apply to all Firebox models. This command is not available for XTMv virtual devices.

Some hardware diagnostic tests can take a long time to run. To run the command, you must specify **yes** on the command line, or select **yes** when prompted.

The flash and memory diagnostics commands can affect system performance while the test runs.

Syntax

diagnose hardwaredisk [*yes*]

Display diagnostic information about the Firebox storage media.

- Firebox T Series models T35 and higher
- Firebox M Series models M400 and higher

Use the **yes** parameter to avoid the confirmation prompt and immediately run the command.

diagnose hardware dsl (*component*) [*yes*]

Display diagnostic information about the DSL interface on a Firebox that supports DSL.

component must be one of these options:

fw-version — displays the DSL firmware version.
link-status — displays the link status (ADSL or VDSL) of the DSL interface.

diagnose hardware dualpoweralarm [*off*]

Temporarily disable the alarm on the Firebox M590/M690 if one of the power supplies is disconnected. When the Firebox reboots, the alarm will revert to the default configuration and the alarm will sound if one of the power supplies is disconnected.

diagnose hardware ethernet (*component*) [*yes*]

Display diagnostic information about Ethernet interfaces.

component must be one of these options:

nic-nums — displays the total number of Ethernet interfaces.
nic-errors *interface* — displays interface diagnostics error reports for the specified interface.
nic-stat *interface* — displays the status of the specified interface.

interface must be a valid Ethernet interface name on the device. For example, eth0.

Use the **yes** parameter to avoid the confirmation prompt and immediately run the command.

diagnose hardware fan-mode (*mode*) [*yes*]

Show and change the fan mode for a Firebox T80. This is supported in Fireware v12.6.2 U2 or higher. This command can be useful to test operation of the fan.

mode shows or changes the fan mode. It must be one of these options:

alwayson — Set the fan mode to always on.

auto — Set the fan mode to auto (this is the default)

show — show the current fan-mode

When the fan-mode is set to **auto**, the fan turns on for two minutes when the Firebox boots up. After two minutes, an internal temperature sensor automatically turns the fan on and off as needed to keep the Firebox temperature in the required operating range.

Use the **yes** parameter to avoid the confirmation prompt and immediately run the command.

To see the current fan speed, use the **diagnose hardware system** command.

diagnose hardware flash (*partition*) [*size*] [*yes*]

Perform a diagnostic check of the specified device partition.

partition is the partition to test. It must be one of these options:

boot — The boot partition.

sysa-data — The system data partition

sysa-kernel — The Fireware kernel partition (XTM 2 Series, 3 Series, and Firebox T10 models only)

sysa-program — The Fireware OS partition

sysb-kernel — The Fireware kernel partition for system recovery (XTM 2 Series, 3 Series, and Firebox T10 models only)

sysb-program — The Fireware OS partition for system recovery

size is the block size to use for the test. It must be an integer between 1 and 8; default is 2.

The block size is multiplied by 512 for the test.

Use the **yes** parameter to avoid the confirmation prompt and immediately run the command.

diagnose hardware lte [*yes*]

Display the status of a 4G LTE interface module or built-in LTE modem.

diagnose hardware memory (*size*) [*number*] [*yes*]

Perform diagnostic memory tests on available RAM.

size is the block size, in kilobytes, to use for the test.

number is the number of times to run the test. The default is 1.

The block size for the test must be less than 10% of the free memory on the device. If you specify a block size that is too large, a message shows the free memory and maximum block size you can use.

Use the **yes** parameter to avoid the confirmation prompt and immediately run the command.

diagnose hardware poe [*yes*]

Display the status of PoE interfaces for devices, such as the Firebox M440, that support Power over Ethernet. When a PoE device is connected to an interface that supports PoE, this command shows the power state and PoE class for the connected device.

For information about which interfaces support PoE, see the Hardware Guide for your device.

Use the **yes** parameter to avoid the confirmation prompt and immediately run the command.

diagnose hardware system [*yes*]

Display the CPU temperature, system fan speed, and voltage. This command option is not supported on XTM 2 Series, XTM 3 Series, and Firebox T10/T10-W, T20/T20-W, T30/T30-W, T40/T40-W, T50/T50-W, T15/T15-W, and T35/T15-W devices.

Use the **yes** parameter to avoid the confirmation prompt and immediately run the command.

diagnose hardware tpm [*yes*]

Display the status of TPM. This is supported in Fireware v12.5.3 and higher, for Firebox models that have a TPM (trusted platform module) chip.

Use the **yes** parameter to avoid the confirmation prompt and immediately run the command.

Firebox T10, T30, T50, T70 M200, M300, M400, M500, M440, M4600, and M5600 models do not have a TPM chip, and do not support the tpm option.

Examples

```
diagnose hardware ethernet nic-nums

diagnose hardware ethernet nic-stat eth0

diagnose hardware system

diagnose hardware fan-mode show

diagnose hardware flash boot

diagnose hardware memory 500

diagnose hardware poe yes
```

diagnose vpn

Description

Display detailed diagnostic information for configured VPNs.

To run a VPN diagnostic report for a branch office VPN gateway, use the vpn-tunnel diag-report command.

Syntax

diagnose vpn"/ike/tracelevel/set (*number*)**"**

Set the VPN diagnostic packet trace level of a device.

number must be one of these options: 0:restore, 1:err, 2:warn, 3:info, 4:debug.

diagnose vpn "/ike/pkttrace/set (*number*)**"**

Set the VPN diagnostic packet trace level of a device.

number must be one of these options: 0:off, 1:start and overwrite, 2:rotate, 3:append, 4:reset.

diagnose vpn "/ike/counters"

Display the VPN diagnostic global counters.

diagnose vpn "/ike/restart"

Restart the Internet Key Exchange of the VPN.

diagnose vpn "/ike/gateway/list"

Display the list of the configured gateways of a device.

diagnose vpn "/ike/gateway/info (*gw-name*) **"**

Display detailed information for the specified gateway.

gw-name is the specific gateway to be displayed.

diagnose vpn"/ike/param/set anti_replay=[number]"

(Fireware v12.2 or higher) Enable or disable anti-replay for VPN client connections.

number can be either 0 (replay window is 0) or 1 (replay window is 32).

The default value is enabled (1) with a window size of 32. Disable anti-relay (0) to troubleshoot issues only. With no anti-replay protection, the connection is susceptible to replay attacks.

diagnose vpn "/ike/param/set ikev2_eap_timeout=*(timeout-value)* **action=now"**

(Fireware v12.5.4 or higher) Configure a custom timeout value for Mobile VPN with IKEv2 client connections.

timeout-value is a number between 20 and 300 seconds.

If you specify **action=now**, you do not have to restart the Firebox for this setting to take effect and the tunnel will not be rekeyed. The new timeout value that you specify will apply to new IKEv2 connections.

This command does not appear in the list of available commands at the command line; however, it is available.

diagnose vpn "/ike/param/set mobile_ikev2_dfbit= (option-number) **action=now"**

(Fireware v12.8 or higher) Configure a custom Don't Fragment (DF) bit value for Mobile VPN with IKEv2 client connections. The DF bit is a flag in the header of a packet.

option-number is a number between 0 and 2 that corresponds to an option:

0 — Copy (default). Applies the DF bit setting of the original frame to the IPSec encrypted packet.

1 — Set. Instructs the Firebox to not fragment the frame regardless of the original bit setting.

2 — Clear. Breaks the frame into pieces that can fit in an IPSec packet with the ESP or AH header, regardless of the original bit setting.

If you specify **action=now**, you do not have to restart the Firebox for this setting to take effect and the tunnel will not be rekeyed. The new timeout value that you specify will apply to new IKEv2 connections.

diagnose vpn "/ike/policy/list"

Display the configured IKE policy list of a device.

diagnose vpn "/ike/policy/info (*ike-pol-name*) **"**

Display detailed information for the specified IKE policy.

ike-pol-name is the specific IKE policy to be displayed.

diagnose vpn "/ike/policy/conn (*ike-pol-name*)**"**

Start a Phase 1 negotiation for the specified IKE policy.

ike-pol-name is the specific IKE policy to be negotiated.

diagnose vpn "/ike/policy/counters (*ike-pol-name*)**"**

Display the counters for the specified IKE policy.

ike-pol-name is the specific IKE policy to be displayed.

diagnose vpn "/ike/sa/list"

Display the established Phase-1 security association list from all the internal hash tables.

diagnose vpn "/ike/sa/list/policy"

Display the Phase-1 Security association list from a single hash table.

diagnose vpn "/ike/sa/counters (*hash-id*) (*initcookie) (respcookie*)**"**

Display the Phase-1 SA counter information.

hash-id is the hash index.

initcookie is the initiator cookie.

respcookie is the responder cookie.

All of these parameters can be obtained from diagnose vpn "/ike/sa/list" command.

diagnose vpn "/ipsec/bovpn/rekey"

Initiate Phase-2 rekey for all available BOVPN tunnels.

diagnose vpn "/ipsec/bovpn/rekey gateway (*gw-name*)**"**

Initiate Phase-2 rekey for all the Tunnels for the specified Gateway.

gw-name is the gateway name.

diagnose vpn "/ipsec/bovpn/rekey ipsec_policy (*tnl-name*) (**spi_in***p2said-in*) (**spi_out***p2said-out*)**"**

Initiate Phase-2 rekey for the specified tunnel. If Phase-2 ID for either Inbound or Outbound, or both, are specified, only those will have a rekey.

tnl-name is the tunnel name.

p2said-in is the Inbound Phase-2 SA ID.

p2said-out is the Outbound Phase-2 SA ID.

Use **diagnose vpn "/ipsec/policy/rtinfo"** to get the p2said-in and p2said-out parameters.

diagnose vpn "/ipsec/cluster/topology"

Display cluster topology information.

diagnose vpn "/ipsec/counters"

Display global level encryption/decryption packet and byte counts.

diagnose vpn "/ipsec/policy/list"

Display the configured IPSec policy list.

diagnose vpn "/ipsec/policy/info (*ipsec-pol-name*)**"**

Display the detailed information of the specified IPSec policy.

ipsec-pol-name is the specific IPSec policy to be displayed.

diagnose vpn "/ipsec/policy/rtinfo"

Display the information about IPSec policies.

diagnose vpn "/ipsec/policy/rtinfo ike_policy (*gw-name*)**"**

Display the information about IPSec policies that are in the specified IKE policy.

gw-name is the gateway name.

diagnose vpn "/ipsec/policy/rtinfo ipsec_policy (*tnl-name*)**"**

Display the information about the specified IPSec policy.

tnl-name is the tunnel name.

diagnose vpn "/ipsec/sa/list"

Display all available IPSec security associations.

diagnose vpn "/ipsec/sa/list ike_policy (*gw-name*)**"**

Display all IPSec security associations for the specified IKE policy.

gw-name is the gateway name.

diagnose vpn "/ipsec/sa/list ipsec_policy (*tnl-name*)**"**

Display all IPSec security associations for the specified IPSec policy.

tnl-name is the tunnel name.

diagnose vpn "/ipsec/sa/list cluster_id (*id*)**"**

Display all IPSec SA for the specified Cluster ID.

id is the Cluster ID. Use the **diagnose vpn "/ipsec/sa/list"** command to get the ID.

diagnose vpn "/ipsec/sa/list local (*num*)**"**

num is one of these options:

"0" to display all IPSec SA including SAs of other cluster members
"1" to display all IPSec SA local to the box.

diagnose vpn "/ipsec/sa/ikepcy/list ike_policy (*gw-name*)**"**

Display all IPSec SA for the specified IKE policy.

gw-name is the gateway name.

diagnose vpn "/ipsec/sa/ipsecpcy/list" (*ipsec-pol-name*)

Display all IPSec SA for the specified IPSec policy.

ipsec-pol-name is the name of the IPSec policy.

diagnose vpn "/ipsec/sp/list"

Display all available security policies.

diagnose vpn "/ipsec/sp/list ike_policy (*gw-name*)**"**

Display all security policies for the specified IKE policy.

gw-name is the gateway name.

diagnose vpn "/ipsec/sp/list ipsec_policy (*tnl-name*)**"**

Display all security policies for the specified IPSec policy.

tnl-name is the tunnel name.

diagnose vpn "/ipsec/sp/info (**dir** *direction*) (**index** *idx*)"

Display detailed information about the specified security policy.

direction can be either "in", "out" or "fwd".

idx is Security Policy index.

Use the diagnose vpn "/ipsec/sp/list" command to get both of these parameters.

diagnose vpn "/ipsec/spi/hashtable"

Display entries in IKEd's SPI hash table.

diagnose vpn "/ipsec/vif/mtu/set \"*(interface name)***\" MTU"**

(Fireware v12.5 or higher) Specify a custom MTU value for a BOVPN virtual interface.

Examples

```
diagnose vpn "/ike/sa/list"
diagnose vpn "/ike/tracelevel/set 2"
diagnose vpn "/ipsec/bovpn/rekey ipsec_policy tunnel.1 spi_in 0x349c2b2
diagnose vpn "/ipsec/vif/mtu/set \"BovpnVif.1\" 1400"
diagnose vpn "/ike/param/set ikev2_eap_timeout=40 action=now"
```

dnslookup

Description

Look up a domain name.

Syntax

dnslookup (*domainname*)

Resolve a domain name.

domainname must be a Fully Qualified Domain Name (FQDN).

Example

```
dnslookup www.example.com
```

export

Description

Export information to an external platform or file.

Syntax

export (**blocked-site**|**allowed-site**) **to** (*location*)

Export the blocked site list or the allowed site list. The allowed site list is also known as the blocked site exceptions list.

blocked-site — Blocked IP addresses.

allowed-site — Allowed IP addresses.

location — The FTP or TFTP location to save the file.

export config to (*location*) [**html**]

Export the device configuration.

location — The FTP or TFTP location to save the file.

html — Exports the device configuration to an HTML file. The HTML file contains the *XTM Configuration Report* which is an easy to read, printable view of the device configuration. If **html** is not specified, the device configuration is exported as an XML file that can be opened by Policy Manager.

export image (*filename*) (*password*) **to** (*location*)

Export a backup image file that is saved on the Firebox.

filename — The name of the backup image file to export from the Firebox.

password — The password to use to encrypt the exported backup image file.

location — The FTP or TFTP location to save the file.

export l2tp to (*location*)

The **export l2tp** command is a legacy command for the WatchGuard Mobile VPN App for iOS. This app is no longer available or supported.

Export a Mobile VPN with L2TP .wgm user configuration file for use with the WatchGuard Mobile app for iOS

location — the FTP or TFTP location to save the file.

In the location, make sure to use the .wgm file extension, which is required for the WatchGuard Mobile VPN app for iOS.

export muvpn *group-name* [**client-type** *client*] **to** (*location*)

Export a Mobile VPN with IPSec user configuration file.

group-name must be the name of an existing Mobile VPN with IPSec group.

client must be one of these options:

- **watchguard** — export the .ini profile for use with the WatchGuard Mobile VPN with IPSec client. This is the default setting.
- **shrew-soft-client** — export the .vpn profile for use with the Shrew Soft VPN client.

The **ios-android-client** option is a legacy option for the WatchGuard Mobile VPN App for iOS and the WatchGuard Mobile VPN App for Android. These apps are no longer available or supported.

location — the FTP or TFTP location to save the file.

In the location, use the file extension for the selected client type. Use .ini for the WatchGuard Mobile VPN with IPSec client, and .vpn for the Shrew Soft client.

export support to (*location*|[**usb** (*filename*)])

Export the support snapshot file.

location — the FTP or TFTP location to save the file.

usb(*filename*) — save the support snapshot to the specified file on a USB drive connected to the device.

Examples

```
export blocked-site to
ftp://joez:1pass@ftp.example.com:23/upload/blocked.dot

export config to ftp://joez:1pass@ftp.example.com:21/upload/exportconfig.xml

export config to
ftp://joez:1pass@ftp.example.com:21/upload/configreport.html html

export image backupimage.fxi password to
ftp://joez:1pass@ftp.example.com:21/upload/backupimage.fxi

export muvpn client-type shrew-soft-client to
ftp://joez:1pass@ftp.example.com:23/upload/vpn-users.vpn

export support to usb support.tgz
```

fault-report

Description

Send all Fault Reports on the device to WatchGuard and delete all Fault Reports from the device.

Syntax

fault-report send

Send all available Fault Reports on the device to WatchGuard immediately.

no fault-report

Delete all Fault Reports from the device, whether or not they have been sent to WatchGuard.

Example

```
fault-report send
no fault-report
```

fqdn

Description

Manage the FQDN (Fully Qualified Domain Names) feature.

Syntax

fqdn policy-check

(Fireware v12.1.3 or lower) Check for conflicts in your current FQDN policy configuration.

fqdn policy-test [*ipaddr*|*fqdn*] [**source**|**destination**]

(Fireware v12.3 or lower) Test your FQDN configuration for a specific source or destination IP address or FQDN.

In Fireware v12.3.1 or higher, this command was renamed as **fqdn test**.

fqdn refresh [*fqdn*]

Refresh the FQDN IP address mapping cache. You can refresh the entire cache, or refresh only for a specific FQDN.

fqdntest [*fqdn*]

(Fireware v12.3.1 or higher) Test your FQDN configuration for a specific source or destination IP address or FQDN.

Example

```
fqdn refresh example.com
fqdn policy-check
fqdn policy-test example.com destination
fqdn test example.com destination
```

gwc

Description

Manage the Gateway Wireless Controller.

Syntax

gwc (**reboot**|**upgrade**|**flash-power-led**|**restart-wireless** | **factory-reset** | **show-password** | **trust**) *serial-num*

Manage the Gateway Wireless controller.

reboot — Reboot the WatchGuard AP device.
upgrade — Upgrade the WatchGuard AP device firmware.
flash-power-led — Flash the power LED of the WatchGuard AP device.
factory-reset — Reset the AP device to factory default settings.
show-password — Show the auto-generated dynamic passphrase for the AP device.
trust — Trust the AP device.
serial-num — The serial number of the WatchGuard AP device.

gwc (**kick-off** *serial-num mac-addr ssid radio*)

Disconnect a user from a WatchGuard AP device.

.**kick-off** — Disconnect a user.
serial-num — The serial number of the WatchGuard AP device the user is connected to.
mac-addr — MAC address of the user to disconnect.
ssid — The SSID to disconnect the user from.
radio — The radio to disconnect the user from.

gwc reset-trust-store

Reset the Trust Store so that all AP devices are untrusted.

gwc (**site-survey**|**log-message**|**network-statistics**) *serial-num*

Display the site survey, log messages, and network statistics information.

site-survey — Perform a site survey.
log-message — Display the log messages.
network-statistics — Display network statistics.
serial-num — The serial number of the WatchGuard AP device.

gwc status

Display the status of the Gateway Wireless Controller.

gwc status access-points

Display the status of WatchGuard AP devices.

gwc status wireless-clients

Display the status of wireless clients.

gwc uninstall-firmware

Remove all AP firmware from the Gateway Wireless Controller.

gwc unpaired-access-points

Display the status of unpaired WatchGuard AP devices.

gwc network-statistics *serial-num*

Display network statistics for the specified WatchGuard AP device.

Example

```
gwc reboot 123456789ABCD
gwc site-survey 123456789ABCD
gwc status
```

import

Description

Import information from an external platform or file.

Syntax

import (**blocked-site**|**allowed site**) **action** (**override**|**merge**) **from** (*location*)

Import entries to the blocked sites or allowed sites list. Choose one of these actions:

override — replace the list with the imported information.
merge — merge the imported entries into the current list

location — the FTP or TFTP location of the import file.

import (**crl**|**config**|**feature-key**) **from** (*location*)

Import information of the specified type from an external platform or file.

location — the FTP or TFTP location of the import file.

import certificate (*cert-function*) **from** (*location*) *(certificate password)*

Import a certificate from an external location.

cert-function — The function of the certificate. It must be one of these options:

proxy-authority — Import a CA certificate to use for a proxy policy that manages web traffic requested by users on trusted or optional networks from a web server on an external network. This must be a CA certificate. Make sure you have imported the CA certificate used to sign this certificate with the **ipsec-web-server-other** category before you import the CA certificate used to re-encrypt traffic with a proxy.

proxy-server — Import a certificate to use for a proxy policy that manages web traffic requested by users on an external network from a web server protected by the Firebox. Make sure you have imported the CA certificate used to sign this certificate with the **ipsec-web-server-other** category before you import the CA certificate used to re-encrypt traffic from a web server.

proxy-trusted — Import a certificate used to trust traffic that is not re-encrypted by a proxy, such as a root certificate or intermediate CA certificate used to sign the certificate of an external web server

ipsec-web-server-other — Import a certificate to use for authentication or other purposes. Specify this category if you want to create a chain of trust to a certificate used to re-encrypt network traffic with a proxy.

location — The FTP or TFTP location of the import file.

certificate password — If you specify a PFX certificate file for import, type the password for the file.

import image (*filename*) (*password*)**from** (*location*)

Import a backup image file to the Firebox.

filename — The name of the backup image file to import to the Firebox.

password — The password that was used to encrypt the backup image file.

location — The FTP or TFTP location from which to import the file.

import route-config (*protocol*) **from** (*location* |**console**)

Import a dynamic routing configuration.

protocol is the dynamic routing protocol to import a configuration for. It must be one of these options:

bgp — import a BGP configuration
rip — import a RIP configuration
rip ng — import a RIPng configuration.
ospf — import an OSPF configuration
ospf v3 — import an OSPFv3 configuration

location — the FTP or TFTP location of the import file.

console — type the dynamic routing configuration in the command line console.

Example

```
import blocked-site action merge from tftp://myftpsite/files/upload/site.dot

import certificate proxy-authority from
tftp://myftpsite/files/upload/cert.dot

import bulk-license from tftp://myftpsite/files/upload/keys.dot

import image backupimage.fxi password from
ftp://myftpsite/files/upload/backupimage.fxi

import route-config rip from console

import route-config ospf v3 from tftp://myftpsite/files/ospfv3config.txt
```

mgmt-user-unlock

Description

Unlock the **status** Device Management user account if it has been locked by consecutive incorrect login attempts that equal the number set by the **auth-setting mgmt-user-lockout** command.

Syntax

mgmt-user-unlock (*user name*)

The command unlocks the status Device Management account when the account is locked based on the auth-setting mgmt-user-lockout setting.

user name must be **status**.

To unlock a Device Management user account locked based on the account lockout settings configured with the **device-mgmt-user** command, use the **unlock device-mgmt-users** command.

no vpn-status

Description

End a Mobile VPN with L2TP user session.

Syntax

no vpn-status l2tp((**ppp-if** *interface-name*)|(**virtual-ip** *ip-address*))

End a Mobile VPN with L2TP user session, based on the PPP interface name or virtual IP address.

interface-name is the PPP interface name of the L2TP session.

ip-address is the virtual IP address of the L2TP session. It must be a IPv4 address in the format A.B.C.D.

Use the **show vpn-status l2tp session** command to see the PPP interface name and virtual IP address for all connected Mobile VPN with L2TP user sessions.

password

Description

Change the administrator read-write or read-only password.

Syntax

password

No options available. The command prompts you to specify the admin or status user and then for the new password.

ping

Description

Send an IPv4 ping request to the specified IPv4 address.

Syntax

ping [*mstring*] (*host*)

host is the host name or IPv4 address in the format A.B.C.D.

[*mstring*] represents all of these optional attributes of the ping command

[-LRUbdfnqrvVaA] [-c count] [-i interval] [-w deadline][hop1...]
[-p pattern] [-s packetsize] [-t ttl] [-I interface or address]
[-M mtu discovery hint] [-S sndbuf][-T timestamp option] [-Q tos]
[-i interface][-s snaplen][-T type][expression]

Example

```
ping 74.125.19.147
```

```
ping -c 5 74.125.19.147
```

ping -6

Description

Send an IPv6 ping request to the specified IPv6 address.

Syntax

ping -6 [*mstring*] (*address*) (**-I** *interface*)

Send an IPv6 ping request to an IPv6 address or domain.

address is the IPv6 address in the format A:B:C:D:E:F:G:H.

interface must be a valid Ethernet interface name on the device. For example, **eth0**, **eth1**, **eth2**.

[*mstring*] represents these optional attributes of the ping command:

[-LRUbdfnqrvVaA] [-c count] [-i interval] [-w deadline][hop1...]
[-p pattern] [-s packetsize] [-t ttl] [-I interface or address]
[-M mtu discovery hint] [-S sndbuf][-T timestamp option] [-Q tos]
[-i interface][-s snaplen][-T type][expression]

Example

```
ping -6 2001::2045:fe21 -I eth1
```

```
ping -6 -c 5 -i 10 2001::2045:fe21 -I eth0
```

policy-check

Description

Check which policy in the configuration handles traffic for a specified interface, protocol, source, and destination.

For a FireCluster, this command is only available on the cluster master.

Syntax

policy-check (*interface-name*) (**ping**|**tcp**|**udp**) (*source-ip*) (*destination-ip*) (*source-port*) (*destination-port*)

Check which policy in the configuration handles traffic that matches the specified interface, protocol, source, and destination. The result of this command shows which policy handles the specified traffic, and what action the policy takes for this traffic.

interface-name is the name of an active Firebox interface. It is case sensitive. It must be the name of an active Firebox physical, VLAN or bridge interface, or SSL-VPN, Any-BOVPN, or Any-MUVPN.

You must specify one of these protocols:

ping — test the ICMP protocol.
tcp — test the TCP protocol.
udp — test the UDP protocol.

source-ip is the source IP address for the traffic.

destination-ip is the destination IP address for the traffic.

source-port is the port for the traffic source. It is not applicable for the ping protocol.

destination-port is the port for the traffic destination. It is not applicable for the ping protocol.

Example

```
policy-check External tcp 203.0.113.1 10.0.1.2 25 25
policy-check Trusted ping 10.0.1.2 198.51.100.1
policy-check SSL-VPN ping 10.0.1.2 198.51.100.1
```

quota-reset

Description

Reset the quota for a quota action or user.

Syntax

quota-reset action [*action name*]

Reset the quota for the specific quota action or user.

action — Reset the quota for a specific quota action.

action name — The name of the quota action to reset.

quota-reset user [*user*]

Reset the quota for the specific user.

user — Reset the quota for a specific user.

user — Specify the user name.

Example

```
quota-reset action action1
quota-reset user user1
```

reboot

Description

Stop all processing and do a cold restart of the device.

Syntax

reboot

No options available.

restore

Restore the device to a backup image or factory-default configuration.

Syntax

restore factory-default [**all**]

Restore the device to its factory default configuration.

all — Restore the factory default configuration, remove all configuration data, backup images, feature key, and certificates from the device, and restore the device to the default configuration after the next system reboot.

If **all** is not specified, the device is restored to the factory default configuration, but the backup images, feature key, and certificates are not removed, and a system reboot is not required.

restore image (*imagename*)

Restore a backup image stored on the Firebox.

imagename — Name of a backup image stored on the Firebox.

restore image (*imagename*) **from usb** (*password*)

Restore a backup image stored on a USB drive that is connected to the Firebox.

imagename — Name of a backup image stored on the USB drive.

from usb — Specify **from usb** to restore a backup image from the attached USB drive.

password — The password that was used to encrypt the backup file.

Example

```
restore image backup-2018-09-30
restore image backup-2018-09-30 from usb configpassword
```

rps

Description

Enable or disable Receive Packet Steering (RPS), which is a software-based version of RSS. RPS distributes received packets across CPUs. Use this command only if a WatchGuard technical support representative directs you to do so for specific Firebox platform. This is a CLI-only command.

Syntax

rps enable

To disable, specify **no rps enable**.

shutdown

Description

Shut down the Firebox.

Syntax

shutdown

No options available.

signature-update

Description

Signature update information.

Internal use only.

sync

Description

Retrieve the feature key, RSS feed, or wireless region from the WatchGuard LiveSecurity server. The RSS feed is available from the LiveSecurity® Service

Syntax

sync ([**feature-key** [**apply**]]|**rss-feed**|**wireless**)

Retrieve information from the WatchGuard LiveSecurity server.

feature-key — Retrieve the feature key from the LiveSecurity server. Use **apply** if you want the Firebox to use the new feature key immediately. If **apply** is not specified, the Firebox does not use the new feature key until you reboot the device.

rss-feed — Retrieve the RSS feed from the LiveSecurity server.

wireless — Retrieve the country doce, country name, and channel set from the Live Security server. Applies only to wireless XTM devices.

Example

```
sync feature-key apply
sync wireless
```

sysinfo

Description

Display the Firebox system information.

Syntax

sysinfo

No options available.

tcpdump

Description

Dump a description of traffic on the network.

Syntax

tcpdump [*mstring]*]

mstring represents these standard tcpdump command options:

[-adeflnNOpqStuvxX][-c count][-i interface][-s snaplen][-T type][expression]

Example

```
tcpdump -d -q
```

tlsv13

Description

Enable Transport Layer Security (TLS) v1.3 on the Firebox. This command is available in Fireware v12.6.2 and higher.

*TLS v1.3 is enabled by default, unless you use the CLI command **csfc enable** to configure the Firebox in CSfC mode.*

Syntax

tlsv13 enable

Enable the Firebox to use TLS v1.3. When you use this command, the Firebox reboots immediately.

Example

```
tlsv13 enable

no tlsv13 enable
```

traceroute

Description

Examine and display the route to a specified destination.

Syntax

traceroute [*mstring*] (*host*)

mstring represents these standard traceroute command options:

[-anruvAMOQ] [-w *wait*] [-S *start_ttl*] [-m *max_ttl*] [-p *port#*] [-q *nqueries*] [-g *gateway*] [-t *tos*] [-s *src_addr*] [-g *router*] [-I *proto*] *host* [*data size*]

host is the name or IP address of the destination to trace.

Command options are case sensitive.

-a — Abort after 10 consecutive drops
-g — Use this gateway as an intermediate hop (uses LSRR)
-S — Set start TTL (default 1)
-m — Set maximum TTL (default 30)
-n — Report IP addresses only (not host names)
-p — Use an alternate UDP port
-q — Set the number of queries at each TTL (default 3)
-r — Set Don't Route option
-s — Set your source address
-t — Set the IP TOS field (default 0)
-u — Use microsecond time stamps
-v — Verbose
-w — Set timeout for replies (default 5 sec)
-A — Report AS# at each hop (from GRR)
-I — Use this IP protocol (currently an integer) instead of UDP
-M — Do RFC1191 path MTU discovery
-O — Report owner at each hop (from DNS)

-P — Parallel probing
-Q — Report delay statistics at each hop (min/avg+-stddev/max) (ms)
-T — Terminator (line end terminator)
-U — Go to next hop on any success

Example

```
traceroute 74.125.19.147
```

trusted-ca-certificates

Description

Download the new versions of trusted CA certificates and install the new certificates.

Syntax

trusted-ca-certificates update

Update and install the new trusted CA certificates on the device.

unlock

Description

Unlock a locked user account.

Syntax

unlock (**device-mgmt-users** | **firebox-db**) (*username*)

Unlock a locked user account.

Specify **device-mgmt-users** to unlock a Device Management user account.

Specify **firebox-db** to unlock the account for any other user who uses Firebox-DB for authentication.

username is the name of the account to unlock. You can include more than one user name, separated by spaces.

Example

```
unlock device-mgmt-users status
unlock firebox-db user1 user2 user3
```

upgrade

Description

Upgrade Fireware OS. For a FireCluster upgrade from 11.11 or higher, this command upgrades both cluster members one at a time.

Syntax

upgrade system from (*location*) [**yes**|**no**]

Upgrade the version of Fireware OS on the device.

location — the FTP or TFTP location of the OS upgrade file.

Use **yes** to upgrade immediately. This avoids the yes/no upgrade confirmation prompt.

The OS upgrade file is a .sysa-dl file for your specific device model. Use **upgrade system from ?** to see the exact name of the upgrade file to use.

If you use this command to install an OS file for a version of Fireware OS that is older than the OS version the device currently uses, this downgrades the OS. The downgrade process automatically resets the device configuration to factory-default settings, unless you select a backup image stored on the Firebox or a connected USB drive to restore. This is necessary because some of the configuration settings are not compatible with older OS versions. The downgrade does not happen automatically; you must confirm that you want to downgrade and choose whether to restore a backup image or reset the device to factory-default settings.

Example

```
upgrade system from ftp://test:testing@1.2.3.4/xtm5_b0.sysa-dl yes
```

upgrade certificate

Description

Upgrade the default Firebox certificates to SHA-256.

Syntax

upgrade certificate (*proxy*| *8021x*| *web*)

Upgrade the default Firebox certificates to SHA-256.

proxy — The Proxy Server and Proxy Authority certificates.
8021x — The 802.1x certificates.
sslvpn — The SSLVPN certificates.
web — The Firebox web server certificates.

Example

```
upgrade certificate proxy
```

usb

Description

Control operations related to a USB storage device attached to the Firebox.

Syntax

usb format

Format the USB drive attached to the device as a FAT32 partition.

usb auto-restore (*password*) (*filename*)

Select a saved backup image on the USB drive to use as the image for auto-restore.

password is the password used to encrypt the backup image.

filename is the filename of the saved backup image. This backup image must include the Fireware OS.

To create the backup image file, use the **backup image** command.

no usb auto-restore

Delete the auto-restore image from the USB drive.

no usb image (*filename*)

Delete a saved backup image from the USB drive.

filename specifies the file name of the backup image to delete.

usb diagnostic enable (*interval*)

Enable the device to automatically save a diagnostic support snapshot to an encrypted file on the USB drive at the specified time interval.

interval is the number of seconds between diagnostic snapshots. It must be an integer between 900 and 2147483647.

The support snapshot contains device configuration and status information that can help WatchGuard technical support troubleshoot issues. A maximum of 48 support snapshots are stored on the USB drive in the \wgdiag directory. When the number of stored snapshots reaches 48, the Firebox automatically removes the oldest snapshot file when it saves a new support snapshot.

The number at the end of the file name is incremented for each snapshot. For example, the first two files have the names support1.tgz and support2.tgz.

Use **no usb diagnostic enable** to disable this feature.

When usb diagnostic is disabled, the USB device automatically stores one support snapshot on the USB drive in the \wgdiag directory when the Firebox starts, or when the USB drive is first connected to the device.

Example

```
usb format

usb auto-restore mypassw0rd backup_2018-10-29.fxi

no usb auto-restore
```

```
no usb image backup_2018-10-29.fxi
usb diagnostic enable 1800
no usb diagnostic enable
```

vpn-tunnel diag-report

Description

Run a VPN diagnostic report for a branch office VPN gateway and all associated VPN tunnels.

vpn-tunnel diag-report gateway (*gateway-name*) [*report-duration*]

Run a VPN diagnostic report to see configuration and status information about the specified gateway and associated branch office VPN tunnels.

gateway-name is the name of a configured branch office VPN gateway.

report-duration is the length of time, in seconds, to collect detailed report data about the VPN tunnels associated with this gateway. The maximum duration is 60 seconds. The default duration is 20 seconds.

For information about the content of the VPN diagnostic report, see the Fireware online help available on the Product Documentation page at http://www.watchguard.com/help/documentation/.

Example

```
vpn-tunnel diag-report gateway ChicagoSeattle 60
```

vpn-tunnel rekey

Description

Force the rekey of a branch office VPN gateway.

vpn-tunnel rekey (*gateway-name*)

gateway-name is the name of a configured branch office VPN gateway.

Example

```
vpn-tunnel rekey ChicagoSeattle
```

who

Description

Shows a list of current Device Management users who are connected to the Firebox. Details include:

- **User** — The user name assigned to the user account.
- **Auth Domain** — The name of the authentication server for the user account. For an Active Directory server, the domain name appears. For a Firebox managed by an instance of Dimension, **Dimension** appears.
- **Role** — The Device Management role assigned to the user account: Device Administrator or Device Monitor.
- **Start Time** — The time the user logged in to the device.

- **Last Activity** — The number of days and time that has elapsed since the user last connected to the device.
- **IP Address** — The IP address where the user connection originates.

Syntax

who

No options available.

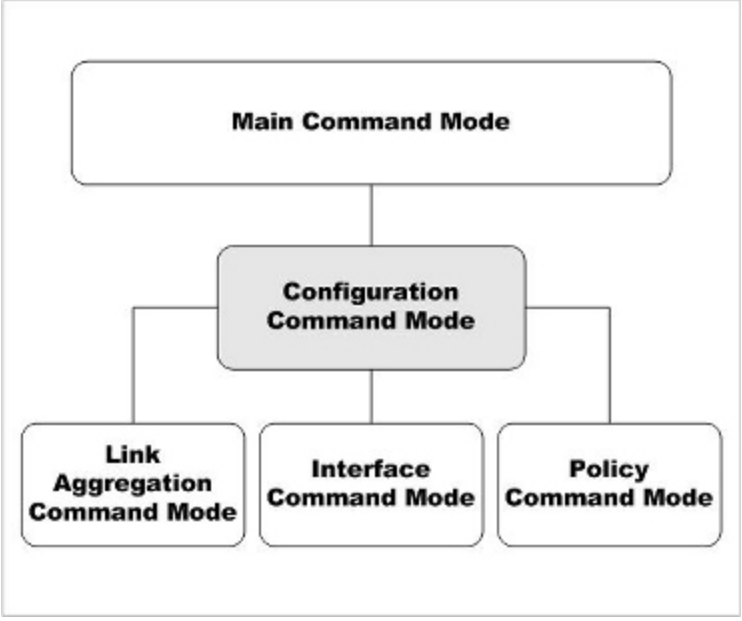
Example

```
WG#who
--
-- Total 2 User(s)
--
User Name                 Auth Domain     Role                      Start Time
                        Last Activity        IP Address      Session ID
    admin                     Firebox-DB      Device Administrator      0  days 00:0
                  1:46     0  days 00:00:01     192.168.43.2    4
    admin                     Dimension       Device Administrator      0  days 00:0
                  0:06     0  days 00:00:02     203.0.113.121   5
```

5 Configuration Command Mode

Configuration Commands

The WatchGuard Command Line Interface (CLI) Configuration command mode is used for system and network configuration of your Firebox.



Bridge and **VLAN** are two other command modes within Configuration command mode. These modes are documented under the **bridge** and **vlan** configuration mode commands.

In the Configuration mode, you can:

- Manage user accounts
- Manage the logging performed by the WatchGuard device

- Configure global network settings
- Control branch office VPN gateways and tunnels
- Configure bridge virtual interfaces
- Configure VLAN settings
- Enter the Policy, Interface, and Link-Aggregation command modes

Enter the Configuration Command Mode

There are two methods to enter the Configuration command mode:

- Use the configure command while in the Main command mode
- Use the exit command while in the Policy, Interface, or Link-Aggregation command modes.

When you get access to the Configuration command mode, the CLI prompt changes to `WG(config)#`.

List of Configuration Mode Commands

You can use all common commands in the Configuration command mode.

In addition, these commands are available only in the Configuration mode:

Command	Usage
access-portal	Configure settings for the Access Portal.
app-control	Configure settings for Application Control.
auth-portal	Configure settings for the authentication portal page.
auth-setting	Configure settings for user authentication.
botnet	Configure settings for Botnet Detection.
bridge	Create or edit a bridge virtual interface on the device.
cluster	Configure settings for FireCluster.
data-loss-prevention	Enable or disable the Data Loss Prevention service.
ddns	Configure settings for dynamic DNS.
default-packet-handling	Configure the default packet handling settings.
device-mgmt-user	Configure global settings that apply to Device Management user accounts.
external-auth-hotspot	Configure the settings for the external hotspot authentication page.
feature-key	Configure automatic feature key synchronization and expiration alarm notification.
garp	Enable or disable gratuitous ARP (GARP) on Ethernet-like interfaces in

Command	Usage
	Mixed Routing Mode.
geolocation	Configure the geolocation settings for the Firebox.
global-setting	Configure the global settings for the device.
gwc	Configure the Gateway Wireless Controller.
hotspot	Configure the hotspot custom page settings.
interface	Enter the Interface command mode for the specified interface.
intrusion-prevention	Configure the Intrusion Prevention Service.
ip	Configure IP settings for firewall features such as block sites and ports.
link-aggregation	Configure link aggregation interfaces.
link-monitor	Configure link monitoring targets to monitor interfaces.
log-setting	Define how and where the device sends log messages.
logon-disclaimer	Configure the Logon Disclaimer dialog box that appears when a user logs in to the device.
managed-client	Configure the device to be a managed client.
mobile-security	Configure Mobile Security.
modem	Configure a modem interface.
multi-wan	Configure the device with multiple external interfaces.
netflow	Configure the Firebox as a NetFlow exporter.
network-mode	Change the system configuration mode to either Mixed Routed, Drop-in, or Bridge.
network-scan	Configure network scanning for the Network Discovery feature.
ntp	Configure the device to use an NTP server.
policy	Enter the Policy command mode.
pppoe	Create or edit a secondary PPPoE interface.
quota-action	Configure a quota action.
quota-exception	Configure a quota exception.
quota-rule	Configure a quota rule.
signature-update	Configure updates to Gateway AV, IntelligentAV, IPS, and Application Control signatures.

Command	Usage
sd-wan	Configure an SD-WAN action.
snat	Configure static NAT and server load balancing SNAT actions.
snmp	Configure the device to inter-operate with SNMP tools.
static-arp	Hard code a static-arp binding.
system	Set the system properties.
tor-exit-node-blocking	Configure the Tor Exit Node Blocking service.
trusted-ca-certificates	Enable automatic update of trusted CA certificates on the device.
v6	Configure IPv6 static routes.
vlan	Create and configure a VLAN interface on the device.
vpn-setting	Configure global VPN settings.
web-server-cert	Configure the web server certificate to use for Firebox authentication.
wireless	Configure WiFi settings. For wireless Firebox devices only.

Configuration Command Mode Reference

access-portal

Description

Configure the Access Portal service.

Syntax

[no] **access-portal enable**

enable is the option to enable the Access Portal.

access-portal app-group *(application group name)* **web** *(application name) (application URL)* **description** *[description]*

If the application group does not exist, create a new application group and a new web application, and add the web application to the specified application group.

If the application group does exist, add the web application to the specified application group. If the web application exists in another group, remove the web application from that group.

If you omit the **app-group** command and the application group name, the web application is added to the default application group named Applications.

access-portal app-group *(application group name)* **application** *(application name)* **up down**

Use the commands *up* and *down* to move an application up or down in the list.

no access-portal app-group *(application group name)*

Remove an application group.

no access-portal app-group *(application group name)* **application** *(application name)*

Remove an application from an application group.

access-portal app-group *(application group name)* **rdp** *(application name)* **host** *(host name) (port) (security type) (credential method) (username) (password)* **trusted enable description** *[description]*

Add an RDP application and configure the general settings.

The security type must be one of these options:

any — Firebox negotiates the security protocol with the remote host

rdp — Remote Desktop Protocol native security

tls — Transport Layer Security

nla — Network Level Authentication

The credential method must be one of these options:

credentials — Specify a user name and password. This option applies only to RDP app configurations that specify the **any** or **nla** security types.

specify-credentials — Require the user to specify a user name and password on the remote host login window

If you trust the remote server certificate, use **trusted enable**.

access-portal rdp *(application name)* **client-name** *(client name)* **color** *(bit)* **console enable language** *(language)* **program** *(file path)* **resize-method** *(resize method)*

Configure the optional session and display settings for an RDP app that already exists.

client-name is used by the RDP host to identify the RDP client.

color must be **8bit**, **16bit**, or **24bit**.

To connect to the console session, specify **console enable**.

language must one of these options: **English**, **German**, **French**, **Swiss-French**, **Italian**, **Japanese**, **Swedish**, **Other**

To automatically launch a program when Windows starts, specify **program** and a file path to the program.

resize-method must be **reconnect**. The reconnect option automatically disconnects if the client display size changes and reconnect with the new display size.

access-portal app-group *(application group name)* **ssh** *(application name)* **host** *(host name) (port) (credential method)* **description** *[description]*

Add an SSH application and configure the general settings.

The credential method must be one of these options:

specify-credentials — Require the user to specify a user name and password on the remote host login window

user — Specify a user name and password or private key

If you specify **user**, you must specify **password** or **private-key**.

If you specify **private-key** you must specify **from** and an FTP or TFTP file path in this format:

ftp://[user[:passwd]@]host[:port]/url-path

tftp://host/url-path

After you specify the FTP or TFTP path, type a decryption password.

(Optional) Use the **description** command to specify a description of the SSH app.

access-portal app-group *(application group name)* **ssh** *(application name)* **color** *(color)* **font monospace** *(font size)*

Configure the optional display settings for an RDP app that already exists.

color must be one of these options: **black-white**, **gray-black**, **green-black**, **white-black**

If you specify **font**, you must specify **monospace**

To configure the font size, specify **size** and a font size in points between 8 and 24.

access-portal max-session *(maximum number of sessions)*

max-session is the option to specify maximum number of active RDP or SSH sessions for each host. The default value is 20.

access-portal application *(application name)* **custom-icon from FTP** *(ftp://[user[:passwd]@]host[:port]/url-path)* **TFTP** *(tftp://host/url-path)*

After you add a web, SSH, or RDP application, you can use **custom-icon** to upload a custom icon for an application. The file must be a .JPG or .PNG file that is 64 x 64 pixels maximum.

[no] **access-portal user-access restrict enable**

Configure the user connection settings. By default, all applications are available to all users and groups authenticated with the Access Portal.

Use **access-portal user-access restrict enable** to enable the restrict option. If you enable the restrict option, you must specify which applications or application groups users or user groups have permission for:

Use **access-portal user-access user** *(user name) (authentication server) (application or group name)* to configure access to applications and application groups for a user.

Use **access-portaluser-access group** *(group name) (authentication server) (application name or group name)*to configure access to applications and application groups for a user group.

To disable the restrict option, use **no access-portal user-access restrict enable**.

[no] **access-portal portal interface** *(interface)*

The **interface** command appears in Fireware v12.1.3 or lower only. Specify interfaces on which the Access Portal is available for user connections. Specify a physical interface, VLAN, link-aggregation interface, or bridge interface. In Fireware v12.1.3 or lower, interfaces you specify are added to the *WG-VPN-Portal* alias in the *WatchGuard SSLVPN* policy.

In Fireware v12.2 or higher, to add or remove interfaces for the Access Portal, edit the WatchGuard SSLVPN policy.

access-portal portal auth-server*(server)*

The authentication server. Specify Firebox-DB, LDAP, RADIUS, SecurID, or the domain name of your Active Directory server.

access-portal portal session-timeout *(timeout value)*

Indicates the maximum amount of time, in hours, that a user can remain connected to the Access Portal.

access-portal portal idle-timeout *(timeout value)*

Indicates the maximum amount of time a user can be idle while connected to the Access Portal.

access-portal portal title *(page title)*

Specify the page title for the Access Portal.

access-portal portal port *(port)*

Specify a port number for user connections to the Access Portal and for Mobile VPN with SSL.

[no] **access-portal portal saml-ssoenable** *(host name)*

Enable SAML single sign-on authentication for the Access Portal.

For the *host name*, specify a FQDN that resolves to the Firebox external interface.

access-portal portal saml-sso hostname *(host name)*

For the *host name*, specify a FQDN that resolves to the Firebox external interface.

access-portal portal saml-sso metadata-url *(metadata-url)*

Specify the metadata URL provided by the administrator of your identity provider account.

[no] **access-portal portal login-logo from** *(FTP or TFTP server)* **enable**

Enable the custom login logo feature. Get a .JPG or .PNG file from an FTP or TFTP server and upload it to the Firebox.

[no] **access-portal portal background-image enable**

Enable the background image feature.

[no] **access-portal portal background-image from** *(FTP or TFTP server)* **enable**

Enable the custom background image feature. Get a .JPG or .PNG file from an FTP or TFTP server and upload it to the Firebox.

[no] **access-portal portal header-logo from** *(FTP or TFTP server)* **enable**

Enable the custom header logo feature. Get a .JPG or .PNG file from an FTP or TFTP server and upload it to the Firebox.

[no] **access-portal portal idp** *(identity provider)* **ident** *(name)*

Specify the name of a third-party identity provider (IdP).

(Optional) Use **ident** to specify a group attribute name. By default, the group attribute name is *memberOf*.

[no] **access-portal portal css-file from** *(FTP or TFTP server)* **enable**

Enable the custom CSS feature. Get a .CSS file from an FTP or TFTP server and upload it to the Firebox.

show access-portal app-group

Show a list of all application groups configured in the Access Portal.

Use **show access-portal app-group** *(app group name)* to see the name, description, and host location for all applications in the application group.

Use **show access-portal app-group** *(app group name)* **application** *(application name)* to see the name, description, and host location for an application in the application group.

show access-portal app-group portal

Show a summary of the Access Portal settings. The summary includes authentication, port, timeout, customization, and SSL settings.

show access-portal users

Show a list of all application groups configured in the Access Portal.

show access-portal user-access

Show a list of all Access Portal users.

Use **show access-portal user-access user** *(user name) (authentication server)* to see applications this user can connect to.

Use **show access-portal user-access group** *(user group name) (authentication server)* to see applications that users in this user group can connect to.

[no] **access-portal url-mappings enable**

enable is the option to enable reverse proxy functionality for the Access Portal.

access-portal url-mappings name *(reverse proxy action name)* **url-mapping ext-url** *(external URL)* **int-url** *(internal URL)* **path-mapping from** *(external URI path)* **to** *(internal URI path)* **authentication** *(access-portal | http-basic)*

Add a reverse proxy action and configure the general settings.

Use **authentication** to select whether to authenticate users with the Access Portal or HTTP Basic. By default, the authentication type is *access-portal* and credentials are not forwarded. If you select access-portal, you can use **forward-credentials** *(yes | no)* to specify whether to forward credentials from the Access Portal to the URL.

access-portal url-mappings name *(reverse proxy action name)* **url-mapping ext-url** *(external URL)* **int-url** *(internal URL)* **description** *(description)*

Use the **description** command to specify a description of the reverse proxy action.

access-portal url-mappings name *(reverse proxy action name)* **url-mapping ext-url** *(external URL)* **int-url** *(internal URL)* **trust***(yes | no)*

Use the **trust** command to specify if the service uses a self-signed certificate and you trust the connection and server.

access-portal url-mappings name *(reverse proxy action name)* **url-mapping ext-url** *(external URL)* **int-url** *(internal URL)* **ports-protocols** *(port or protocol)*

Use the **ports-protocol** command to set the external port, internal port, and the internal protocol.

ext-port — Use **ports-protocolsext-port***(external port)* to set the external port. The default external port is 443.

int-port — Use **ports-protocolsint-port***(internal port)* to set the internal port. The default internal port is 443.

int-protocol — Use **ports-protocolsint-protocol***(http | https)* to set the external port. The default protocol is https.

no **access-portal url-mappings name** *(reverse proxy action name)*

Remove the reverse proxy action.

no **access-portal url-mappings name** *(reverse proxy action name)* **from** *(external URI path)*

Remove the URL path action with the specified *(external URI path)* from the reverse proxy action.

no **access-portal url-mappings name** *(reverse proxy action name)* **trust-cert**

Set the **trust** value for the reverse proxy action to false.

show access-portal url-mappings

Show the reverse proxy actions configured on the Access Portal and if proxy buffering is enabled.

show access-portal url-mappings name *(reverse proxy action name)*

Show the specified reverse proxy action and the URL path actions that have been configured.

[no] **access-portal url-mappings proxy-buffering enable**

enable is the option to enable buffering for reverse proxies for the Access Portal.

Example

```
access-portal app-group Accounting web AccountingApp www.example.com

access-portal application AccountingApp custom-icon from
ftp://user1:P@swRd*39405@www.example.com:443/files

access-portal app-group rdpservers rdp rdpserver1 host server1.example.com
3389 any credentials user1 P@swRd*39405 description sandbox

access-portal app-group rdpservers rdp rdpserver2 host server2.example.com
3389 rdp specify-credentials trusted enable

access-portal app-group rdpservers rdp rdpserver2 host server2.example.com
3389 rdp specify-credentials description "sandbox server"

access-portal app-group sshservers ssh sshserver1 host server3.example.com
22 user user1 password P@swRd*39405 description "sandbox server"
```

```
access-portal app-group sshservers ssh sshserver1 host server3.example.com
22 specify-credentials description "sandbox server"

access-portal user-access user test Firebox-DB Applications

access-portal portal auth-server Firebox-DB

access-portal portal title "Example Company Portal"

access-portal portal login-logo from
ftp://user1:P@swRd*39405@www.example.com:443/files

show access-portal user-access user user1 Firebox-DB

access-portal portal saml-sso enable portal.example.com

access-portal portal idp Okta memberOf

access-portal portal saml-sso metadata-url https://host/url-path

show access-portal url-mappings name Example

access-portal url-mappings name Example url-mapping ext-url example.com int-
url example.com path-mapping from "/" to "/"
```

app-control

Description

Configure the Application Control service.

Syntax

app-control (*app-control-name*) (*action*) (*category*) ["*app-name*" *behavior*]

Create or edit an Application Control action. If the Application Control action does not exist, this command creates it and adds the action for the specified application or application category. If the Application Control action already exists, this command adds the action for the specified application or application category to the existing Application Control action.

app-control-name is the name of the Application Control action. The name is case sensitive. Use Global to configure the global Application Control action.

action is the name of the action to take for the controlled application category, application, or application behavior. It must be one of these options:

allow — Allow the connection

drop — Drop the connection

traffic-mgmt *tm-action* — Use the specified Traffic Management action. The parameter *tm-action* is the name of an existing Traffic Management action. It is case sensitive.

category is the application category to control. You must specify a category. To see a list of application categories, use the question mark on the command line after the action. For example, type `app-control Global drop ?`.

app-name is the name of an application within the specified application category. the app-name must be enclosed in double-quotes. If you do not specify an application name, the specified action applies to the all applications in the category.

behavior is the name of an application behavior. This allows you to control usage of some applications on a granular level. If you do not specify a behavior, the action applies to all behaviors of the application. The behaviors you can control depend on which application you specify. You can specify one of these behaviors, if the behavior is available for the selected application:

Authority — Log in
Access — Known command to access a server or peer
Communicate — Communicate with server or peer (chat)
Connect — Unknown command (p2p connect to peer)
Games — Games
Media — Audio and video
Transfer — File transfer

Use **no app-control** (*app-control-name*) to delete the entire Application Control action. You cannot delete an application control action if it is in use by a policy.

Use **no app-control** (*app-control-name*) (*category*) ["*app-name*" *behavior*] to delete an application category, an application, or an application behavior from the Application Control action.

Use **show categories** (*category*) to see a list of applications and application behaviors in a specified category.

app-control (*app-control-name*) (**default-action** *action*)

Set the default action to take if traffic does not match the applications controlled by an Application Control action.

app-control-name is the name of the Application Control action. The name is case sensitive.

action must be one of these options:

allow — allow the connection
drop — drop the connection
traffic-mgmt *tm-action* — Use the specified Traffic Management action. *tm-action* is the name of an existing Traffic Management action. It is case sensitive.
global — use the Global Application Control action

app-control (*app-control-name*) (**used-by** *policy-name* ...)

Enable an Application Control action for a policy.

app-control-name is the name of the Application Control action. The name is case sensitive.

policy-name is the name of the policy. The policy name is case sensitive. To apply an action to more than one policy, type the name of each policy, separated by a space.

Use **no app-control** *app-control-name* (**used-by** *policy-name*) to remove the Application

Control action from the policy configuration.

Example

```
app-control Global drop streaming-media
app-control Global default-action allow
app-control Global used-by http
app-control App-Control.1 allow network-management
app-control Global traffic-mgmt TM-1 streaming-media
no app-control App-Control.1
```

auth-portal

Description

Configure settings for the Authentication Portal page.

Syntax

[no] **auth-portal enable** [**font-name** *name*] [**font-size** *size*] [**form-background-color** *color*] [**logo** *from*] [**page-background-color** *color*] [**panel-background-color** *color*] [**registration-url** *url*] [**text-color** *color*] [**title** *title text*]

Configure the logo, text, font, and colors for the Authentication Portal page. The color settings and logo will also be used for the SSL VPN download page and the Certificate Portal.

enable is the option to enable the Authentication Portal.

[font-name] is the option to set the name of the font to use for the text on the Authentication Portal page. You can choose one of these fonts:

- Arial
- Comic Sans
- Courier New
- Georgia
- Lucida Console
- Microsoft-Sans-Serif
- Tahoma
- Times-New-Roman
- Trebuchet
- Verdana

[font-size] is the option to set the size of the font to use for the text on the Authentication Portal page. You can choose one of these options:

- xx-small
- x-small
- small
- medium
- large
- x-large
- xx-large

[form-background-color] is the option to set the color to use for the background of the login form in the Authentication Portal. You must use a hex code to specify the color. Use the format *#RRGGBB*. *RR* is red, *GG* is green, and *BB* is blue. The default value is #FFFFFF (white).

[logo] is the option to specify the image file to use for the logo in the Authentication Portal. Specify the directory location of the logo file. The logo must be a JPG or PNG file with a maximum size of 100 x 40 pixels.

[page-background-color] is the option to set the color to use for the background of the Authentication Portal page. You must use a hex code to specify the color. Use the format *#RRGGBB*. *RR* is red, *GG* is green, and *BB* is blue. The default value is #FFFFFF (white).

[panel-background-color] is the option to set the color to use for the borders of the login form in the Authentication Portal. You must use a hex code to specify the color. Use the format *#RRGGBB*. *RR* is red, *GG* is green, and *BB* is blue. The default value is #FFFFFF (white).

[registration-url] the URL of the page where users can create a user account before they authenticate. Type the URL in the format *https://host/url-path*.

[text-color] is the color to use for the text on the Authentication Portal page. You must use a hex code to specify the color. Use the format *#RRGGBB*. *RR* is red, *GG* is green, and *BB* is blue. The default value is #000000 (black).

[title] is the text for the title that appears on the Authentication Portal page. The title must be between no more than 255 characters in length.

[no] **auth-portal welcome-disclaimer** *enable* [**disclaimer** *enable*] [*message*]

Specify the Welcome or Disclaimer message that appears on the Authentication Portal page and enable the option to force users to accept the message before they can authenticate.

welcome-disclaimer is the option to enable or disable the Welcome or Disclaimer message that appears in the Authentication Portal.

[disclaimer] is the option to force users to accept the Welcome or Disclaimer message before they can authenticate.

[message] is the text to include in the Welcome or Disclaimer message in the Authentication Portal.

Example

auth-portal enable [**font-name** *Verdana*] [**font-size** *medium*] [**form-background-color** *#FFFFFF*] [**logo** *http://myserver.com/c/images/logo.jpg*] [**page-background-color** *#2aedb3*] [**panel-background-color** *#FFFFFF*] [**registration-url** *https://example.com/registration-url*] [**text-color** *#000000*] [**title** *Example Company Authentication Portal*]

auth-portalwelcome-disclaimer*enable* [**disclaimer***enable*] [*You must accept this message to proceed.*]

auth-setting

Description

Configure the authentication settings on the Firebox.

Syntax

auth-setting account-lockout enable

Enable the Account Lockout feature for users who use Firebox-DB for authentication. This feature prevents brute force attempts to guess user account passwords. To unlock a locked user account, use the **unlock** command.

auth-setting account-lockout (**attempts** *login-attempts*)

Configure the number of consecutive failed login attempts that can occur before a user account is temporarily locked.

auth-setting account-lockout (**duration** *lockout-duration*)

Configure the number of minutes that a temporarily locked account remains locked.

auth-setting account-lockout (**lockouts** *temp-lockouts*)

Configure the number of temporary lockouts that can occur before an account is permanently locked.

auth-setting (*timeout-type*) [**day** *days*] [**hour** *hours*] [**minute** *minutes*] [**second** *seconds*]

Configure the timeout setting options for authentication.

timeout-type is the authentication option that must be set for timeout. It must be one of these options:

auth-user-idle-timeout — The maximum length of time the user can stay authenticated when idle (not passing any traffic to the external network). If you set this field to zero (0) seconds, minutes, hours, or days, the session does not time out when idle, and the user can stay idle for any length of time.

auth-user-session-timeout — The maximum length of time the user can send traffic to the external network. If you set this field to zero (0) seconds, minutes, hours, or days, the session does not expire and the user can stay connected for any length of time.

mgmt-user-idle-timeout — The maximum length of time the user can stay authenticated when idle (not passing any traffic to the external network). If you select zero (0) seconds, minutes, hours, or days, the session does not expire when the user is idle, and the user can stay idle for any length of time.

mgmt-user-session-timeout — The maximum length of time the user can send traffic to the external network. If you select zero (0) seconds, minutes, hours, or days, the session does not expire and the user can stay connected for any length of time.

days is the duration in days. It must be an integer from 0 to 365.

hours is the duration in hours. It must be an integer from 0 to 23.

minutes is the duration in minutes. It must be an integer from 0 to 59.

seconds is the duration in seconds. It must be an integer from 0 to 59.

If you do not specify a timeout, the specified authentication type is set to never time out.

auth-setting case-sensitivity enable

Set the case-sensitivity option for user credentials. When enabled, users must use the correct capitalization when they log in.

auth-setting (**default-auth-server** *auth-svr*)

Set the default authentication server to use on the Firebox user authentication page.

auth-svr is the authentication server used by default. It must be one of these options: **Firebox-DB**, **RADIUS**, **LDAP**, or **SecurID**. Or, to use Active Directory, specify the domain name of a configured Active Directory server.

auth-setting auto-redirect enable

Automatically redirect the user to the authentication portal for authentication.

auth-setting auto-redirect (**url** *url-path*)

Send a redirect to a specified web site to the browser after successful authentication.

url-path is the web site to redirect after authentication.

auth-setting auto-redirect (**hostname** *host-name*)

Specify a host name for the page where your users are redirected, when you choose to automatically redirect users to the authentication portal for authentication.

host-name is the name of the host to redirect traffic to.

The host name must match the Common Name (CN) from the web server certificate. Make sure that this host name is specified in the DNS settings for your organization, and that the value of the host name in the DNS settings is the IP address of the Firebox.

auth-setting login-setting (*unlimited* | *number*) (*reject* | *logoff*)

Specify the number of login connections that each user can make to the Firebox.

unlimited — Set the option to *unlimited* to allow the same user credentials to be used to authenticate to the Firebox an unlimited number of times.

number — To limit the number of times a user account can authenticate, set the option to an integer (1 or higher).

reject — Specify *reject* to reject all additional connection attempts when the specified number of allowed connections is reached.

logoff — Specify *logoff* to log off the first connected user when the specified number of allowed connections is reached, and another user logs in with the same credentials.

auth-setting mgmt-user-lockout (*attempts*)

Set the number of consecutive failed login attempts for the **status** management account before the account is locked.

attempts is the maximum number of failed login attempts by the status user before the account is locked. It must be an integer from 0 to 1000. The default value is 0, which means no lockout occurs.

After the status account is locked, the admin user can use the **mgmt-user-unlock** command to unlock it.

To configure account lockout settings that apply to all Device Management user accounts, use the **device-mgmt-user account-lockout** command.

auth-setting min-password-length *(length)*

(Fireware v12.2.1 or higher) Specify the minimum password length for accounts that use Firebox Authentication (Firebox-DB).

length is a value between 8 and 32 characters.

auth-setting same-user-multi-login (0|1|2)

Set authentication to allow or deny more than one authenticated sessions from a user at the same time.

You must specify one of these options:

0 — Log off the first session when the user logs in a second time
1 — Allow multiple sessions for a user
2 — Reject subsequent log in attempts when a user is already logged in

Set to 1 by default.

auth-setting single-sign-on enable

Enable Active Directory Single Sign-On (SSO) on the Firebox.

Use **no auth-setting single-sign-on enable** to disable SSO.

auth-setting single-sign-on agent (*address*) **description** (description) **down position up**

Specify an Active Directory Single Sign-On (SSO) agent on the network. In Fireware v12.2 or higher, you can specify up to four SSO Agents.

address is the IPv4 address of an SSO Agent. In Fireware v12.3 or higher, you can specify an IPv6 address.

description is an optional text string you specify that helps to identify the SSO Agent.

(Fireware v12.1.3 or lower) *cache-timeout* is the amount of time in seconds the SSO information is stored.

To disable an agent, specify no **auth-settingsingle-sign-on agent**.

auth-setting single-sign-on agent (*address*) **down up position** (position number)

Use **down** or **up** to move the specified SSO Agent down or up in the list.

Use **position** to specify a number between 0 and 3 that correlates with the list position.

auth-setting single-sign-on except-ip (**host**| **range** | **subnet**) (*ip-address*)

Add addresses to the Active Directory SSO exception list. Addresses on the exception list are exempt from SSO.

ip-address must be one of these options: **host***ip*, **range***startipendip* , or **subnet***net*.

ip, *startip*, and *endip* must be an IPv4 address in the format of A.B.C.D. In Fireware v12.3 or higher, you can specify an IPv6 address in the format of A:B:C:D:E:F:G:H, A::G:H, or ::H.

net must be an IPv4 subnet in the format of A.B.C.D/# where # must be in the range of 0 to 32. In Fireware v12.3 or higher, you can specify an IPv6 subnet in the format of A:B:C:D:E:F:G:H/I, A::G:H/I, or ::H/I.

auth-setting single-sign-on sso-through-bovpn

Enable Active Directory Single Sign-On through the BOVPN tunnels on this Firebox.

enable — Enable this feature on the Firebox.

Use **no auth-setting single-sign-on sso-through-bovpn** to disable this feature.

auth-setting single-sign-on radius enable [*address*]

Enable RADIUS single-sign-on on the Firebox.

address is the IP address of the RADIUS server.

auth-setting single-sign-on radius (**exception** *ip-address*)

Add addresses to the RADIUS SSO exception list. Addresses on the exception list are exempt from SSO.

ip-address must be one of these options: **host***ip*, **range***startipendip* , or **subnet***net*.

ip, *startip*, and *endip* must be an IPv4 address in the format of A.B.C.D.

net must be an IPv4 subnet in the format of A.B.C.D/# where # must be in the range of 0 to 32.

You can specify more than one IP address in the command.

auth-setting single-sign-on radius (**group-attr** *attribute*)

Specify the RADIUS group attribute number used to get group names from RADIUS accounting messages.

attribute must be a number in the range 0 - 255.

auth-setting single-sign-on radius ((**idle-timeout**|**session-timeout**)*timeout*)

Configure the idle timeouts for RADIUS SSO authentication.

The **idle-timeout** specifies the maximum length of time the user can stay authenticated when idle (not passing any traffic to the external network). If you set this value to zero (0) seconds, minutes, hours, or days, the session does not time out when idle and the user can stay idle for any length of time.

The **session-timeout** specifies the maximum length of time the user can send traffic to the external network. If you set this field to zero (0) seconds, minutes, hours, or days, the session does not expire and the user can stay connected for any length of time.

timeout must be one of these options:

day *days* is the duration in days. It must be an integer from 0 to 365.
hour *hours* is the duration in hours. It must be an integer from 0 to 23.
minute *minutes* is the duration in minutes. It must be an integer from 0 to 59.
second *seconds* is the duration in seconds. It must be an integer from 0 to 59.

auth-setting single-sign-on radius (**secret** *sharedsecret*)

Configure the RADIUS server shared secret. This shared secret is used to verify RADIUS messages between the RADIUS server and the Firebox.

sharedsecret is the shared secret. It must be the same secret used by the RADIUS server. It must be between 8 and 128 characters.

auth-setting single-sign-on radius server-ip [*address*]

Configure the RADIUS server IP address.

address is the IP address of the RADIUS server.

auth-setting terminal-service (*option*)

Configure authentication settings for terminal services.

option must be one of these values

enable — Enable users to authenticate to your Firebox over a Terminal Server or Citrix server.

session-timeout— This is the length of time in seconds that the user can send traffic to the external network. If you specify 0, the session does not expire.

agent-ip-address — This must be the IP address of a terminal server. It must be in the form A.B.C.D.

Example

```
auth-setting account-lockout enable
auth-setting auth-user-idle-timeout minute 15
auth-setting mgmt-user-idle-timeout day 1 hour 6 minute 30
auth-setting auto-redirect enable
auth-setting auto-redirect url http://authsuccess.company.com/welcome/
auth-setting same-user-multi-login 2
auth-setting single-sign-on enable
auth-setting single-sign-on agent 10.0.1.253
auth-setting single-sign-on agent 2001:db8::1
auth-setting single-sign-on except-ip 10.0.1.33
auth-setting mgmt-user-lockout 5
auth-setting min-password-length 9
auth-setting single-sign-on sso-through-bovpn enable
auth-setting single-sign-on radius enable 203.0.113.100 RSSOsecrit
auth-setting terminal-service enable
auth-setting terminal-service 10.0.1.74
```

botnet

Description

Configure the Botnet Detection subscription service.

Syntax

botnet enable *allowed site*

enable — Enable the Botnet Detection service.

allowed site — Defines exceptions that will not be blocked by Botnet Detection.

fqdn — FQDN domain name.
host — Host IP address.
range — IP address range.
subnet — IP address and subnet prefix.

Use **no botnet enable** to disable Botnet Detection.

bridge

Description

Create or edit a bridge virtual interface on the Firebox. The bridge command starts a separate command mode with commands you can use to configure the bridge.

In bridge command mode, the command prompt changes to "WG(config/bridge-<bridge-name>)#" where <bridge-name> is the name of the bridge interface.

Use the **Exit** command to exit this mode.

Syntax

bridge (*bridgename*)

bridgename is a string that uniquely identifies the bridge you want to create or configure.

Use **no bridge** *bridgename* to delete the bridge virtual interface. You cannot delete a bridge that is used in the configuration.

After you type the command **bridge** *bridgename* the configuration continues to the bridge details command. The prompt changes to "`WG(config/bridge-bridgename)#`". Use the **Exit** command to exit this mode.

dhcp relay (*serverip*) [*serverip*] [*serverip]*

Configure the bridge interface to relay DHCP requests to up to three DHCP servers.

serverip is the IP address of a DHCP server that is used for computers on the interface. You can specify the IP addresses up to three DHCP servers. The Firebox sends DHCP requests to the IP addresses of all DHCP servers you specify.

Use **no dhcp enable** to disable DHCP relay on the interface.

dhcpserver (**start-addr** *startip endip leasetime*) [**dns-server** *dns*...] [**domain** *domainname*] [**reservation** *resvname macaddress ipaddress*] [**wins** *wins*...]

Configure the bridge interface as a DHCP server for computers on the member interfaces.

start-addr defines a DHCP address pool. In the same line, you can use the start-addr command multiple times with these parameters:

startip is the first IP address in the DHCP address pool.

endip is the last IP address in the DHCP address pool.

leasetime is the duration in hours that addresses are leased to devices on the network. The value must be an integer.

dns is the IP address of one or more valid DNS servers.

domainname is the domain name used by devices on the network.

reservation defines a pair of MAC address and IP address that are reserved within the DHCP address pool. In the same line, you can use the reservation command multiple times with these parameters:

resvname is a string to identify a reserved address.

macaddress is the MAC address of the Firebox with a reserved address.

ipaddress is the IP address assigned to the reserved address.

wins is the IP address of one or more valid WINS servers.

Use **no dhcp enable** to disable DHCP server on the interface.

dhcp *option*

Configure a predefined DHCP option. DHCP options are used by many VoIP phones.

option must be one of these predefined options:

capwap-ac-v4 *ipaddress* specifies the IP address of a CAPWAP access controllers. You can specify multiple IP addresses, separated by spaces. This corresponds to DHCP option 138 (CAPWAP access controller).

dhcp-state *state* specifies the DHCP state. This is used by ShoreTel phones for an FTP boot option. This corresponds to DHCP option 156 (DHCP state).

sip-server *ipaddress* specifies the IP address of a Session Initiation Protocol (SIP) server. You can specify multiple IP addresses, separated by spaces. This corresponds to DHCP option 120 (SIP servers).

[**tftp-server***address*] specifies the IP address or domain name of the TFTP server where a DHCP client can download the boot configuration. *address* can be a domain name or an IP address. This corresponds to DHCP option 66 (TFTP server name) and option 150 (TFTP server IP address).

[**tftp-boot-file***bootfile*] specifies the name of the boot file. This corresponds to DHCP option 67 (boot file name).

time-offset *seconds* specifies the time offset in seconds from Coordinated Universal Time (UTC). This corresponds to DHCP option 2 (time offset).

vendor-spec *option* specifies vendor-specific information. This corresponds to DHCP option 43 (vendor specific information).

dhcp custom-option *option-code option-name option-type value*

Configure a custom DHCP option, as described in RFC 2132. If you configure more than one interface to use the same DHCP option code, the *option-type* must be the same on each interface.

option-code is the DHCP option code. It must be an integer from 1 - 255. DHCP options 1, 3, and 28 are not supported.

name is a name to describe this DHCP option

option-type is the type of value required by this option. It must be one of these types:

boolean — Specify a Boolean DHCP option value (true or false)

four-byte-integer — Specify a DHCP option value as a four bytes integer

hexadecimal — Specify the DHCP option value as a hexadecimal number

ip-address-list — Specify the DHCP option value as a list of IP addresses, separated by spaces

one-byte-integer — Specify the DHCP option value as a one byte integer

text — Specify the DHCP option value as a text string

two-byte-integer — Specify the DHCP option value as a two bytes integer

unsigned-four-byte-integer — Specify the DHCP option value as an unsigned four bytes integer

unsigned-one-byte-integer — Specify the DHCP option value as an unsigned one byte integer

unsigned-two-byte-integer — Specify the DHCP option value as an unsigned two bytes integer

value is the value to assign to the option. The value must match the type specified in *type*.

interface (*if-number*| **name** *if-name*)

Add an interface member to the bridge.

if-number is the interface number to add as a member of the bridge.

if-name is the name of a physical or link aggregation interface to add to the bridge.

You can specify more than one member interface for the bridge.

Use **interface** (*if-number*|**name***if-name*) to remove an interface from the bridge.

ip address (*address*)

Change the IP address for the bridge.

address is the IP address assigned to the virtual interface.

It must be either an address with mask in the format of A.B.C.D A.B.C.D. or a net in the format of A.B.C.D/# where # must be in the range of 8 to 30.

ip ip-node-type (*option*)

Configure whether to enable IPv6 addressing on the bridge interface.

option must be one of these options:

ip4-only — use the configured IPv4 address only.

ip4-6 — enable an IPv6 address for this interface in addition to the configured IPv4 address. When you select this option, Fireware assigns a link-local IPv6 address to that interface, when the interface is active. Use the show interface command to see the assigned IPv6 address.

secondary (*address*)

address must be one of these options: *addr mask* or *net*

addr is an IP address, and must be in the format of A.B.C.D.

mask is an IP subnet mask, and must be in the format of A.B.C.D.

net is the IP address and subnet prefix in the format of A.B.C.D/# where # must be in the range of 0 to 32.

This command can take multiple address entries.

Use **no secondary** to remove all secondary addresses from this interface.

security-zone (*zone*) (*ip-address*) (**interface** (*if-number*|**name** *if-name*) (*if-number*|**name** *if-name*) ...)

zone is the security zone. It must be **trusted**, **optional**, or **custom**.

ip-address is the IP address assigned to the virtual interface. It is either an address with a mask in the format of A.B.C.D A.B.C.D. or a net in the format of A.B.C.D/#, where # must be in the range of 8 to 30.

if-number is the interface number assigned as a member of the bridge

if-name is the name of a physical or link aggregation interface assigned as a member of the bridge.

You can specify more than two member interfaces of the bridge.

spanning-tree

Enable and configure Spanning Tree Protocol for a bridge.

Use (*enable*) to enable Spanning Tree Protocol on the Firebox.

(*bridgeprio*) is the bridge priority. To make sure that the Firebox is always selected as the root bridge, specify a bridge priority number that is lower than all other bridges on your network. The default value is 32768. You can specify a value between 0 and 65535, in increments of 4096.

(**port**)

port number is the number of the Firebox port.

pathcost is the path cost. The default value is 0. You can specify a value between 0 and 65535.

portpri is the port priority. In an election, if all ports have the same path cost and Bridge ID, the port with the lowest port priority becomes the root port. The default value is 128. You can specify a value between 1 and 254, in increments of 16.

Timers:

[*fd*] is the forward delay timer. It specifies how long the Firebox ports remain in the Listening and Learning states. The default value is 15 seconds. You can specify a value between 4 and 30 seconds.

(*hello*) specifies how often a root bridge generates a BPDU. You can configure this value only for a Firebox that is the root bridge. The default is 2 seconds. You can specify a value between 1 and 10 seconds.

(*maxage*) specifies how often a bridge port saves its configuration BPDU information. The default is 20 seconds. You can specify a value between 6 and 40 seconds.

v6

Configure IPv6 settings for the bridge interface.

The available v6 command options are the same as for a physical trusted, optional, or custom interface. For more information, see the Command Mode section *v6* on page 228.

Example

```
bridge Bridge-10

security-zone trusted 10.10.1.1/24 interface 3 4 5

bridge BR3-4 spanning-tree bridgeprio 0
```

cluster

Description

Configure the FireCluster settings. This command applies only to devices that support FireCluster, and requires Fireware Pro.

FireCluster is not compatible with all features of Fireware OS. You cannot enable FireCluster if incompatible features are already enabled. For more information about FireCluster requirements and restrictions, see the FireCluster section of Fireware Help.

Syntax

cluster enable

Enable FireCluster on a Firebox.

cluster hardware-monitor enable

Enable monitoring of hardware health status as a criteria for cluster failover. When enabled, the FireCluster uses the Hardware Health Index (HHI) as part of the calculation of the Weighted Average Index (WAI) which is used as a criteria for FireCluster failover. This feature is disabled by default.

Use **no cluster hardware-monitor enable** to disable failover based on hardware status.

cluster hb-threshold (*threshold*)

Set the lost heartbeat threshold to trigger a FireCluster failover. The cluster master sends a VRRP heartbeat packet through the primary and backup cluster interfaces once per second. The lost heartbeat threshold determines the number of consecutive heartbeats not received by the backup master to trigger a failover.

threshold is the number of lost heartbeats to trigger a failover. It must be a number between 1 and 10. The default is 3.

cluster id (*c-id*)

Set the identification number of a FireCluster.
c-id is an identification number from 1 to 255.

cluster interface management (*if-number*|**name***if-name*)

Configure the interface for FireCluster management. You can specify either an interface number or an interface name.

if-number is the interface number of a physical interface.

if-name is the name of the interface. For a management interface, *if-name* can be the name of a physical interface, or a bridge, VLAN, or Link Aggregation interface.

cluster interface (**primary**|**secondary**) (*if-number*)

Configure the primary and secondary cluster interfaces. A cluster interface is a dedicated interface the cluster members use to communicate with each other about system status. You must configure a primary cluster interface.

The cluster interface type must be one of these options:

primary — Configure the interface as the primary cluster interface.

secondary — Configure the interface as the secondary cluster interface.

if-number is the interface number.

Use a crossover Ethernet cable (red) to connect the primary cluster interface on one Firebox to the primary cluster interface on the other Firebox. If you want to enable a secondary cluster interface, use a second crossover Ethernet cable to connect the backup cluster interfaces.

cluster mode (**active-active**|**active-passive**)

Selects the FireCluster mode. The mode must be one of these options:

active-active — Configure the cluster as active/active. Active/active mode is not supported for XTMv devices.

active-passive — Configure the cluster as active/passive.

cluster load-balance (**least-connections**|**round-robin**)

Specify the load balancing algorithm of an active/active FireCluster. The algorithm must be one of these options:

least-connections — Each new connection is assigned to the active cluster member with the lowest number of open connections. This is the default setting.

round-robin — New connections are distributed among the active cluster members in round robin order. The first connection goes to one cluster member. The next connection goes to the other cluster member, and so on.

cluster member (**add**|**edit**) (*member-name*) [**serial** *serial-no*] [**primary-ip** primary-ip] [**management-ip** *mgmt-ip*] [**secondary-ip** *secondary-ip*] (**from** *source*)

Add or edit a FireCluster member.

member-name is the name of the FireCluster member. It is case sensitive.

serial-no is the serial number of the Firebox.

primary-ip is the IP address of the primary cluster interface. It must be an IPv4 address in the form A.B.C.D.

mgmt-ip is the management IP address of the FireCluster. For an IPv4 address, it must be in the form A.B.C.D. For an IPv6 address, it must be in the form A.B.C.D.E.F.G.H. You can specify an IPv6 management IP address only if the management interface supports IPv6.

secondary-ip is the IP address of the secondary cluster interface. It must be an IPv4 address in the form A.B.C.D.

source FireCluster member license file from one of these options: *FTP*, *TFTP* or **console**.

If you change the **primary-ip** or **secondary-ip** to an IP address on a different subnet, you must specify the new IP addresses for both cluster members in the same command, as shown in the subsequent **Example**.

If you update the **primary-ip** or **secondary-ip** for an existing cluster, all cluster members must reboot at the same time after you save the configuration.

cluster notification snmp-trap enable

Activate and send SNMP traps for FireCluster.

cluster notification notification (**enable**) [**action-type** (**email**|**pop-window**)] [**launch-interval** *launchinterval*] [**repeat-count** *repeat-count*]

Configure FireCluster exception notification settings.

You must set the notification action-type to one of these settings:

email — the Log Server sends an email to the configured email address when an event occurs.

pop-window — the Log Server opens a dialog box when an event occurs.

launchinterval is the minimum time (in minutes) between different notifications, default is 15.

repeat-count is the number of events to include in a repeat log notification, default is 10.

no cluster member (*member-name*) [**license** *featurekey-id*]

Remove a cluster member or remove the feature key for a cluster member.

If **license** is not specified, this command removes the specified member from the cluster.

If **license** is specified, this command removes the specified feature key for the specified member.

member-name is the name of the FireCluster member device. It is case sensitive.

featurekey-id is the feature key ID to remove.

use **show feature-key** to see the feature key IDs for the cluster.

cluster monitor (*interface-name*)

For an active/passive FireCluster, enable the cluster to monitor the link status for an interface, as criteria for cluster failover. The link status of all interfaces is monitored by default.

interface-name is the name of a physical interface. It is case sensitive.

To disable monitoring of an interface, use the **no cluster monitor** *interface-name* command.

Example

```
cluster enable
cluster encryption encrypt-key
```

```
cluster id 3

cluster interface management 1

cluster member add Master 9085046373F7B 10.0.1.10/24 10.0.1.2/24
10.0.1.20/24 from ftp://ftp.company.com/licenses/9085046373F7B-license.txt

cluster member edit Member1 primary-ip 50.51.50.1/24 Member2 50.51.50.2/20

cluster member edit Member1 secondary-ip 40.41.40.1/24 Member2 40.41.40.2/24

cluster mode active-active

cluster load-balance least-Connections

cluster notification snmp-trap enable

cluster notification notification enable action-type email launch-interval
20 repeat-count 5

cluster monitor Optional-5
```

data-loss-prevention

Description

Configure the Data Loss Prevention (DLP) service.

Syntax

data-loss-prevention enable

Enable the Data Loss Prevention service.

Use **no data-loss-prevention enable** to disable the service.

Example

```
data-loss-prevention enable
```

ddns

Description

Configure the Firebox to use a dynamic domain name service provider.

Syntax

In Fireware 12.1.1, multiple dynamic DNS service providers are supported. Use this syntax:

ddns *(service provider type) (interface) (password) (user name) (domain name)* [**update-interval**] (*interval*) [**determine-ip**] [**service-option**] (*options*)

service provider type is the name of your dynamic DNS service provider. It must be one of these options:

dyndns
noip
dynu
dnsdynamic
freedns
duckdns

interface is the interface name of the interface for which you want to configure dynamic DNS. It must be an external interface. The external interface can be a physical interface, a VLAN interface, or a link aggregation interface.

username is the user name for your dynamic DNS account.

password is the password for your dynamic DNS account. A password is required for all dynamic DNS providers except DuckDNS.

domainname is a string that is the domain name for your dynamic DNS account.

update-interval *interval* is the time interval, in days, to force an update of the IP address. This must be an integer from 0 to 28.

(Fireware 11.12.1 and lower) *type* is the DynDNS service type. It must be one of these options: **dyndns**, or **custom**.

determine-ip is the optional to allow DynDNS to determine which IP address to use.

options is a string composed of one or more DynDNS options:

- You must type the “&” character before and after each option you add.
- If you add more than one option, you must separate the options with the “&” character.
- Available options are: mx=mailexchanger, backmx=YES|NO, wildcard=ON|OFF|NOCHG, and offline=YES|NO

In Fireware 12.1 and lower, DynDNS is the only supported dynamic DNS provider.

In Fireware v11.12.1 – 12.1, use this syntax:

ddns DynDNS (*interface*) (*username*) (*password*) (*domainname*) [**update-interval**] (*interval*) [**determine-ip**] [**service-option**] (*options*)

Example

Fireware 11.12.2 and higher:

```
ddns dyn External watchguard strongpass2 watchguard.com update-interval 28
determine-ip service-option "&backmx=NO&wildcard=ON&"
```

Fireware v11.12.1 and lower:

```
ddns DynDNS interface 0 watchguard strongpass2 watchguard.com 28 dyndns
"&backmx=NO&wildcard=ON&"
```

default-packet-handling

Description

Configure default packet handling settings.

Syntax

default-packet-handling (**logging** *log-msg-type*) (*log-action*) (**action** *notify-method*) (*log-rate*) [**launch-interval** *int*] [**repeat-count** *count*]

Configure log settings for default packet handling options.

log-msg-type is the type of log message to configure. It must be one of these options:

address — address space probes
arp — ARP spoofing attacks
ddos-des — DDOS attack destination
ddos-src - DDOS attack source
external — Unhandled external packet
icmp — ICMP flood attack
ike — IKE flood attack
incoming — Incoming broadcasts
internal — Unhandled internal packet

ip-spoofing — IP spoofing attacks
ip-src — IP source route
ipsec — IPSEC flood attack
outgoing — Outgoing broadcasts
ping — Ping of death
port — Port probes
syn — SYN flood attack
tcp-synproxy — TCP/real SYN flood attack
udp — UDP flood attack

Use **no default-packet-handling logging** *log-msg-type* to disable the logging of packets of the specified type.

log-action is the form of notification or the log rate. It must be one of these options:

1 — Send log message
2 — Send SNMP trap
3 — Send notification
4 — Log rate per minute

If the **log-action** selected is **3**, these notification options are also available:

action *notify-method* specifies the notification method. *notify-method* must be one of these options:
1 — Email
3 — Pop up window

If the **log-action** selected is **4**, you must include this option:

log-rate specifies the maximum number of log messages the Firebox generates in a minute for the log message type. It must be an integer from 1 to 2000000000.

launch-interval *int* is the minimum time in minutes between notifications. It must be an integer from 1 to 65525.

repeat-count *count* is the number of times an event must occur before a repeat notification is sent. It must be an integer from 1 to 256.

default-packet-handling unhandled (**auto-block**|**send-message**) **enable**

Set action taken for packets that do not match any default packet handling rule.

The action must be one of these options:

auto-block — Automatically block the source of unhandled packets. The Firebox adds the IP address that sent the packet to the temporary Blocked Sites list.
send-message — Send a TCP reset or ICMP error to the client when the Firebox receives an unhandled packet.

Use **no default-packet-handling unhandled** (**auto-block**|**send-message**) **enable**to disable actions for unhandled packets.

default-packet-handling dangerous-active (*activity*) (**enable**) [*threshold*]

Enable default packet handling rules for certain types of dangerous activity.

activity is the form of dangerous activity. It must be one of these options:

arp-spoof — Drop arp spoofing attack (this option is supported only in drop-in or bridge network modes and only in the CLI)

icmp-flood — Drop ICMP flood attack

ike-flood — Drop IKE flood attack

ip-scan — Block address space probes

ipsec-flood — Drop IPSEC flood attack

port-scan — Block port space probes

source-route — Drop IP source route

spoofing-attack — Drop spoofing attack

syn-flood — Drop SYN flood attack

synproxy-flood — Drop SYN proxy flood attack

udp-flood — Drop UDP flood attack

threshold is the threshold value. It is an integer as follows:

Ports 10 to 65535 for icmp-flood or syn-flood.

Packets per second 1 to 65535 for udp-flood, ipsec-flood, ike-flood, ip-scan, or port-scan.

threshold does not apply to spoofing-attack or source-route.

default-packet-handling ddos (**server-ddos**|**client-ddos**) **enable** (*quota*)

Configure evaluation of traffic for distributed denial of service (DDoS).

You must specify one of these options:

client-ddos — Set a maximum allowed connections per second from any source protected by the Firebox to any one destination.

server-ddos — Set a maximum allowed connections per second from any external source to the Firebox external interface. This includes connections to internal servers allowed by a static NAT policy.

quota is the maximum number of connections per second. It must be an integer from 10 to 65535.

Example

```
default-packet-handling logging ike 3 action 3 launch-interval 50
repeatcount 10

default-packet-handling logging ike 4 5

default-packet-handling unhandled auto-block enable

default-packet-handling dangerous-activity ike-flood enable 1000

default-packet-handling ddos server-ddos enable 1500
```

device-mgmt-user

Description

Configure global authentication settings that apply to Device Management user accounts.

Syntax

device-mgmt-user account-lockout enable

Enable the Account Lockout feature for Device Management users who use Firebox-DB for authentication. This feature prevents brute force attempts to guess user account passwords. To unlock a locked user account, use the **unlock** command.

The "admin" Device Management account can never be permanently locked out.

device-mgmt-user account-lockout (**attempts** *login-attempts*)

Configure the number of consecutive failed login attempts that can occur before a Device Management user account is temporarily locked.

device-mgmt-user account-lockout (**duration** *lockout-duration*)

Configure the number of minutes that a temporarily locked Device Management account remains locked.

device-mgmt-user account-lockout (**lockouts** *temp-lockouts*)

Configure the number of temporary lockouts that can occur before a Device Management account is permanently locked.

Example

```
device-mgmt-user account-lockout enable
device-mgmt-user account-lockout attempts 3
device-mgmt-user account-lockout duration 5
```

dnswatch

Description

Enable and configure the DNSWatch service. The DNSWatch security subscription is supported in Fireware 12.1.1 and higher.

Syntax

dnswatch enable

Enable the DNSWatch service on the Firebox.

dnswatch enforcement [*enforcement-option*]

Configure the usage enforcement option for Firebox trusted, optional, and custom interfaces.

enforcement-option must be one of these options:

all — Enable usage enforcement on all trusted, optional, and custom interfaces.
none — Disable usage enforcement on all interfaces.

select — enable usage enforcement for selected interfaces. By default, this option enables usage enforcement on all interfaces.

dnswatch require interface [*interface-name*]

Enable or disable DNSWatch usage enforcement on an interface when DNSWatch is configured to enable usage enforcement on selected interfaces.

interface-name must be the name of an interface.

To see the list of interface names, use the **show interface** command.

To disable enforcement for an interface, use the command **no dnswatch require interface** [*interface-name*].

Example

```
dnswatch enable

dnswatch enforcement all

dnswatch enforcement select

dnswatch require interface Trusted
```

external-auth-hotspot

Description

When you enable a hotspot for your wired or wireless guest network, you can configure it as the *External Guest Authentication* hotspot type. With this hotspot type, the Firebox sends new hotspot users to an external web server for authentication.

Use this hotspot type if you want to automatically connect new hotspot users to an external web server that collects and verifies authentication credentials or other information for the hotspot user. Based on the information the user provides, the external web server sends an access decision to the Firebox. The Firebox then either allows or denies the user access to the hotspot.

To use this option, you must configure the authentication and failure web pages on an external web server, and you must configure the web server to exchange the necessary query strings with the Firebox. For more information about the hotspot external guest authentication process and requirements, see *Fireware Help*.

Syntax

external-auth-hotspot [**authentication-url** "*auth-url*"] [**failure-url** "*fail-url*"] [**secret** *sharedsecret*]

auth-url the URL of the authentication page on the external web server. The authentication URL must begin with *https://* or *http://* and must specify the IP address or domain name of the web server. It must be enclosed in quotation marks.

failure-url is the URL of the authentication failure page on the external web server. The failure URL must begin with *https://* or *http://* and must specify the IP address or domain name of the web server. It must be enclosed in quotation marks.

sharedsecret is the shared secret. It must be the same secret used by the external web server to generate the checksum that is used to validate the hotspot access decision. It must be between 1 and 32 characters.

external-auth-hotspot [**enable**]

Enable the wireless Firebox hotspot to use hotspot external guest authentication.

To disable the external guest authentication hotspot, run this command: **no wireless guest external-auth-hotspot enable**.

external-auth-hotspot [**failure-url** "*fail-url*"] [**authentication-url** "*auth-url*"] [**secret** *sharedsecret*]

failure-url is the URL of the failure page on the external web server. The failure URL must begin with *https://* or *http://* and must specify the IP address or domain name of the web server. It must be enclosed in quotation marks.

auth-url the URL of the authentication page on the external web server. The authentication URL must begin with *https://* or *http://* and must specify the IP address or domain name of the web server. It must be enclosed in quotation marks.

sharedsecret is the shared secret. It must be the same secret used by the external web server to generate the checksum that is used to validate the hotspot access decision. It must be between 1 and 32 characters.

external-auth-hotspot idle-timeout [**day** *days*] [**hour** *hours*] [**minute** *minutes*] [**second** *seconds*]

Configure the idle timeout settings for hotspot connections to a hotspot that uses external guest authentication.

days — The duration in days. It must be an integer from 0 to 365.

hours — The duration in hours. It must be an integer from 0 to 23.

minutes — The duration in minutes. It must be an integer from 0 to 59.

seconds — The duration in seconds. It must be an integer from 0 to 59.

If **idle-timeout** is set to 0, user sessions never time out based on inactivity. The default idle timeout is 2 hours.

external-auth-hotspot secret *sharedsecret* [**authentication-url** "*auth-url*"] [**failure-url** "*fail-url*"]

Configure the shared secret for the hotspot connections to the external web server.

sharedsecret is the shared secret. It must be the same secret used by the external web server to generate the checksum that is used to validate the hotspot access decision. It must be between 1 and 32 characters.

auth-url the URL of the authentication page on the external web server. The authentication URL must begin with *https://* or *http://* and must specify the IP address or domain name of the web server. It must be enclosed in quotation marks.

failure-url is the URL of the failure page on the external web server. The failure URL must begin with *https://* or *http://* and must specify the IP address or domain name of the web server. It must be enclosed in quotation marks.

external-auth-hotspot session-timeout [**day** *days*] [**hour** *hours*] [**minute** *minutes*] [**second** *seconds*]

Configure the session timeout settings for hotspot connections to a hotspot that uses external guest authentication.

days — The duration in days. It must be an integer from 0 to 365.
hours — The duration in hours. It must be an integer from 0 to 23.
minutes — The duration in minutes. It must be an integer from 0 to 59.
seconds — The duration in seconds. It must be an integer from 0 to 59.

If **session-timeout** is set to 0 (the default value), user sessions never time out based on total time connected.

Example

```
external-auth-hotspot enable
external-auth-hotspot authentication-url "https://10.0.2.80:8080/auth.html"
failure-url "http://10.0.2.80:8080" secret ***************
external-auth-hotspot idle-timeout minute 30
external-auth-hotspot session-timeout hour 23
```

feature-key

Description

Configure automatic feature key synchronization and expiration alarm notification.

Syntax

[*no*] **feature-key automatic-synchronization enable**

Enable or disable automatic feature key synchronization. Automatic feature key synchronization enables the Firebox to automatically download the latest feature key from your account on the WatchGuard web site when a feature is expired or about to expire. It is not enabled by default.

Use **no feature-key automatic-synchronization enable** to disable automatic feature key synchronization.

[*no*] **feature-key notification snmp-trap enable**

Activate and send SNMP traps when a feature is expired or about to expire.

Use **no feature-key automatic-synchronization enable** to disable automatic feature key synchronization.

[*no*] **feature-keynotificationnotification** (**enable**) [**action-type** (**email**|**pop-window**)] [**launch-interval** *launchinterval*] [**repeat-count** *repeat-count*]

Configure feature key expiration alarm notification settings.

You must set the notification **action-type** to one of these settings:

email — the Log Server sends an email to the configured email address when an event occurs.

pop-window — the Log Server opens a dialog box when an event occurs.

launchinterval is the minimum time (in minutes) between different notifications, default is 15.

repeat-count is the number of events to include in a repeat log notification, default is 10.

Use **no feature-key notification notification enable** to disable alarm notification.

Example

```
feature-key automatic-synchronization enable
feature-key notification snmp-trap enable
feature-key notification notification enable action-type email
```

garp

Description

Enable or disable gratuitous ARP (GARP) on Ethernet-like interfaces in Mixed Routing Mode.

Syntax

garpenable

By default, GARP is enabled for Ethernet-like interfaces in Mixed Routing Mode. In Fireware v12.8 or higher, to disable GARP for the interface, use **no garp enable**. If you disable GARP, the Firebox no longer sends GARP broadcasts. The GARP setting is added to the Firebox XML configuration and remains after a reboot.

You cannot suppress GARP for 1-to-1 NAT or for FireCluster failover. Even if you disable GARP for interfaces included in 1-to-1 NAT or FireCluster failover configurations, GARP broadcasts required for these features are not suppressed.

To re-enable GARP, use **garpenable**.

geolocation

Description

Configure the geolocation settings of the Firebox.

Syntax

geolocation action (*action-name*)

Add a new geolocation action with the specified name.

Use **no geolocation action** (*action-name*) to delete the specified geolocation action. Only actions that are not used by any policies can be deleted.

geolocation action (*action-name*) (**continent** *continent-name*)

Configure the geolocation action to block connections to or from all countries in the specified continent. You can specify more than one continent, separated by spaces.

continent-name is case-sensitive, and must be one of these options: Europe, Asia, "North America", "South America", Oceania. Africa, Antarctica

geolocation action (*action-name*) (**country** *country-name*)

Configure the geolocation action to block connections to or from the specified country. You can specify more than one country, separated by spaces.

country-name is case-sensitive, and must match the country name at it appears in the Geolocation configuration in Fireware Web UI and Policy Manager. If a country name contains a space, you must enclose the country name in quotation marks.

geolocation action(*action-name*) (**used-by** *policy-name*)

Configure the specified policy to use the specified geolocation action.

geolocation enable

Enable the Geolocation service on the Firebox.

Use **no geolocation enable** to disable geolocation.

geolocation (**exception [fqdn|host|range|subnet]** *address*)

Add the specified address to the exception list for geolocation. Geolocation does not block connections to or from addresses on the exception list.

address can be an IPv4 or IPv6 host IP address, network IP address, host range, or fully qualified domain name (FQDN).

In Fireware 12.3.1 and lower, you cannot add a geolocation exception that overlaps an existing exception.

Example

```
geolocation enable
geolocation action newaction
geolocation action Global country "Hong Kong"
geolocation action Global continent Antarctica
geolocation exception fqdn watchguard.com
geolocation exception host 203.0.113.100
geolocation exception range 203.0.113.10 203.0.113.50
no geolocation exception range 203.0.113.10 203.0.113.50
geolocation exception subnet 203.0.113.0/24
```

global-setting

Description

Configure the global settings of the Firebox.

Syntax

global-setting auto-reboot enable

Enable the auto-reboot feature for the Firebox.

Use **no global-setting auto-reboot enable** to disable auto-reboot.

global-setting auto-reboot ([**day** *day*]|[**hour** *hr min*]|[**minute** *min*])

Defines the auto-reboot timer for the Firebox.

day is the day of the week. It must be one of these options:

0 — Sunday
1 — Monday
2 — Tuesday
3 — Wednesday
4 — Thursday
5 — Friday
6 — Saturday
7 — Every day

hr is the number of hours from 0 to 23.

min is the optional number of minutes from 0 to 59.

global-setting device-admin-connections enable

Enable more than one user with Device Administrator credentials to log in to the Firebox at the same time.

Use **no global-setting device-admin enable** to disable this option.

When this option is enabled, if one Device Administrator has unlocked the configuration file to make changes, another Device Administrator cannot make changes to the configuration file until the first Device Administrator has either locked the configuration file again or has logged out of the Firebox.

global-setting fault-report enable

Enable the Firebox to send fault reports to WatchGuard.

Use **no global-setting fault-report enable** to disable the Fault Reports feature.

global-setting hostout-traffic-control enable

Enable control of traffic generated by the Firebox in Fireware v12.2 or higher.

Use **no global-setting hostout-traffic-control enable** to disable this option.

global-setting icmp-message (*message*)

Define the ICMP error message for the Firebox.

Use **no global-setting icmp-message message** to disable icmp-message function.

message is the ICMP message returned to the source. It must be one of these options:

allow-all — Allow all ICMP messages.
fragmentation-required — Allow ICMP Fragmentation Req messages.
host-unreachable — Allow ICMP Host Unreachable messages
network-unreachable — Allow ICMP Network Unreachable messages.
port-unreachable — Allow ICMP Port Unreachable messages.
protocol-unreachable — Allow IMCP Protocol Unreachable messages.
time-exceeded — Allow ICMP Time Exceeded messages.

If the message selected is **fragmentation-required**, then the DF bit is set to 1.

global-setting quota enable

Enable the bandwidth and time quotas feature.

Use **no global-setting quota enable** to disable the bandwidth and time quotas feature.

global-setting report-data enable

Enable the Firebox to send detailed device feedback to WatchGuard.

Use **no global-setting report-data enable** to disable the Device Feedback feature.

global-setting tcp-close-timeout (*unit*) (*timeout-value*) ...

Set the TCP close timeout value. This value determines how long a connection remains in the connection table after the TCP connection is closed with RST.

unit is the time unit for the timeout-value. It must be one of these options: **day**, **hour**, **minute**, or **second**. You can specify more than one unit, followed by the timeout-value for that unit.

timeout-value is the connection timeout. value associated with the timeout unit. Default is 10 seconds. Maximum is 180 seconds.

global-setting tcp-connection-timeout (*unit timeout-value*) ...

Set the TCP connection idle timeout value.

unit is the time unit for the timeout-value. It must be one of these options: **day**, **hour**, **minute**, or **second**. You can specify more than one unit, followed by the timeout-value for that unit.

timeout-value is the connection timeout. value associated with the timeout unit. Default ide timeout is 1 hour. Maximum idle timeout is 30 days.

global-setting tcp-mss-adjustment (**automatic**|[**limit-to** *size*])

Set the TCP maximum segment size adjustment.

You must select one of these options:

automatic — automatic adjustment

limit-to *size* — limit to a specified size. *size* is the specified size in bytes. It must be an integer from 40 to 1460.

global-setting tcp-mtu-probing (**dynamic-enable** | **enable**)

Set the option for TCP MTU Probing. When TCP MTU Probing is enabled, clients on your network can get access to the Internet through a zero-route BOVPN tunnel configured on this Firebox, even when your Firebox has received an ICMP unreachable packet for the traffic sent through the BOVPN tunnel (an ICMP black hole was detected).

dynamic-enable — TCP MTU probing is disabled until an ICMP network issue is detected. When an ICMP network issue is detected, TCP MTU probing is automatically enabled and remains enabled.

enable — TCP MTU probing is always enabled

Use **no global-settingtcp-mtu-probing enable** to disable TCP MTU Probing.

global-setting tcp-syn-checking enable

Enable the TCP/syn check for the Firebox.

Use **no global-setting tcp-syn-checking enable** to disable TCP/syn checking.

global-setting tcp-time-wait-timeout (*unit*) (*timeout-value*) ...

Set the interval to remove closed connections from the connection table. When a TCP connection is closed with a FIN, the connection entry is removed from connection table after the tcp-time-wait-timeout interval. If you set this value too high, terminated connections will remain in the connection table longer, which affects the connection rate. If you set this value too low, it can cause some out-of-order TCP packets to not be received.

unit is the time unit for the timeout-value. It must be one of these options: **minute**, or **second**. You can specify more than one unit, followed by the timeout-value for that unit.

timeout-value is the connection timeout. value associated with the timeout unit. Default value is 60 seconds. Maximum value is 740 seconds.

global-setting tcp-window-scale (*option*)

Specify the TCP window scale option as described in RFC 1323. This global setting is available only in Fireware CLI.

option must be a value between 0 and 14. The default value is 14.

global-setting traffic-flow flush-connections (*option*)

Specify whether to clear existing connections when the static NAT configuration changes.

option must be one of these options:

none — do not clear existing connections when you modify an SNAT action used by a policy.

related — close active connections through a policy that uses an SNAT action that you modify.

global-setting traffic-management enable

Enable traffic management for the Firebox.

Use **no global-setting traffic-management enable** to disable traffic management for the Firebox.

global-setting udp-stream-timeout (*unit*) (*timeout-value*) ...

Set the UDP stream timeout value. The udp-stream-timeout specifies the timeout value of UDP streams after enough packets have been sent and received for the connection to reach the assured state. If you set this value too high, UDP connections stay in the connection table longer. This affects the connection rate. You might want to increase this value if you have a problems where connections time out.

unit is the time unit for the timeout-value. It must be one of these options: **minute**, or **second**. You can specify more than one unit, followed by the timeout-value for that unit.

timeout-value is the connection timeout. value associated with the timeout unit. Default is 3 minutes. Maximum is 30 minutes.

global-setting udp-timeout (*unit*) (*timeout-value*) ...

Set the UDP timeout value. The udp-timeout specifies the timeout for initial UDP packets in a connection. The udp-timeout value determines the length of time the Firebox waits to see enough packets sent and received for the connection to become assured, at which point it is considered a stream. If you use UDP protocols that send very little data over a long time frame, you might want to increase this value to help the Firebox more accurately track your udp connections.

unit is the time unit for the timeout-value. It must be one of these options: **minute**, or **second**. You can specify more than one unit, followed by the timeout-value for that unit.

timeout-value is the connection timeout. value associated with the timeout unit. Default is 30 seconds. Maximum is 10 minutes.

global-setting webui-port (*port*)

Set the Web User Interface port for the Firebox.

port is the port number from 1 to 65535.

Example

```
global-setting auto-reboot enable
global-setting auto-reboot hour 2 30
global-setting tcp-close-timeout seconds 20
global-setting icmp-message deny-all
global-setting tcp-mtu-probing enable
global-setting tcp-syn-checking enable
global-setting tcp-mss-adjustment limit-to 100
global-setting tcp-connection-timeout hour 5 minute 30 seconds 10
global-setting webui-port 8585
```

gwc

Description

Configure the Gateway Wireless Controller.

Syntax

gwc enable

Enable the Gateway Wireless Controller.

Use **no gwc enable** to disable the Gateway Wireless Controller.

gwc passphrase *passphrase*

Configure the Gateway Wireless Controller AP management passphrase.

gwc manual-passphrase enable

(Fireware v12.0.2 and lower)

Use manual global passphrase instead of auto-generated dynamic passphrases.

Use **no gwc manual-passphrase enable** to disable the manual passphrase and enable auto-generated dynamic passphrases.

gwc firmware-auto-update enable

Automatically update WatchGuard AP device firmware when a new version is available on the Firebox.

Use **no gwc firmware-auto-update enable**to disable automatic updates.

gwc syslog-server enable *server-ip*

Send WatchGuard AP device log messages to a syslog server.

server-ip — Specify the syslog server IP address.

Use **no gwc syslog-server enable** to disable logging to a syslog server.

gwcair-deploy enable

(Fireware v12.0.2 and lower)

Enable over-the-air wireless deployment of AP300 devices.

Use **no gwc air-deploy enable** to disable over-the-air wireless deployment.

gwc auto-deploy enable

Enable automatic deployment of unpaired AP devices.

Use **no gwc auto-deploy enable** to disable automatic deployment.

gwc bridge-lans enable

(Fireware v12.2.1 and higher)

Enable bridging of LAN interfaces on APs with two LAN ports.

Use **no bridge-lans enable** to disable bridging of the LAN interfaces.

gwc discovery *ip address broadcast-all*

Configure AP discovery broadcast address.

ip address — A broadcast address for a network. For example, 10.0.0.255 for a 10.0.0.1/24 network.

broadcast-all — Broadcast on all networks. (Default)

gwc disable-discovery

Disable automatic AP discovery broadcasts.

Use **gwc disable-discovery enable** to enable automatic discovery broadcasts.

gwc mgmt-vlan enable *[vlan-id]*

Configure management communications VLAN ID tagging.

mgmt-vlan — Management communications VLAN tagging.

vlan-id — The management communications VLAN ID. 1 to 4094. Default is 4094.

Use **no gwc mgmt-vlan enable** to disable communications VLAN tagging.

gwc reports *enable*

Enable logging of wireless events for reports.

reports — Logging of wireless events for reports.

enable — Enable logging for reports.

Use **no gwc reports enable** to disable the feature.

gwcscan-interval *(hours)*

Configure intervals for automatic wireless scans for wireless maps and rogue AP devices.

scan-interval — Hours between automatic wireless scans for wireless maps and rogue AP devices.

hours — Number of hours between automatic wireless scans.

gwcschedule-reboot *enable*

Configure scheduled reboots for your WatchGuard AP devices.

schedule-reboot — Scheduled reboot of AP devices.

enable — Enable scheduled reboots.

Use **no gwc schedule-reboot enable** to disable the feature.

gwcschedule-reboot *reboot-time*(*day*) (*hour*) (*minute*)

Configure the day and time for scheduled reboots.

schedule-restart — Scheduled reboot of AP devices.

restart-time — Set the reboot time.

day — Set the reboot day.

hour — Must be an integer from 0-23.

minute — Must be an integer from 0-59.

gwc ssh enable

Enable SSH access to all WatchGuard AP devices. Secure SSH access to wireless AP devices is used by WatchGuard Technical Support to help troubleshoot issues with the AP device. Enable this option only if requested by technical support.

Use **no gwc ssh enable** to disable SSH access.

gwc (**mac-acl allowed**|**denied**) *mac-addr name*

Manage the MAC address access control lists.

allowed — Add the address to the allowed MAC addresses.

denied — Add the address to the denied MAC addresses.

mac-addr — Specify the client MAC address.

name — Specify a name for the client with this MAC address.

Use **no gwc** (**allowed**|**denied**) **mac-addr [name]** to disable MAC address access control for the specified MAC address.

gwc [alarm-ap-offline|alarm-rogue-ap] *enable*

Enable Gateway Wireless Controller alarms.

alarm-ap-offline — Alarm notification if AP device goes offline.

alarm-rogue-ap — Alarm notification if rogue AP device detected.

enable — Enable alarm.

gwc notification (**snmp-trap** enable | **notification** enable **action-type** action-type enable [**launch-interval** launch-interval] [**repeat-count** repeat-count])

Configure Gateway Wireless Controller notifications.

notification — Enable a notification.

snmp-trap — Enable an SNMP trap notification.

action-type — You can set the type of notification as **email** or **pop-window**. The default is **email**.

launch-interval — Set the launch interval in minutes. The default is 15 minutes.

repeat-count — Set the repeat count for the notification. The default is 10.

gwc ssid *name*

Add an SSID to the Gateway Wireless Controller.

Use **no gwc ssid *name*** to remove the SSID from the Gateway Wireless Controller.

gwc ssid *name* **broadcast enable**

Enable broadcast for the specified SSID.

ssid — Configure an SSID.

name — Specify the SSID name.

broadcast — Broadcast the SSID on the wireless network.

Use **no gwc ssid** *name* **broadcast enable** to disable broadcast for the specified SSID.

gwcssid *name***auto-deployenable**

Enable automatic deployment for the specified SSID.

ssid — Configure an SSID.

name — Specify the SSID name.

auto-deploy — Enable automatic deployment on this SSID.

Use **no gwcssid** *name* **auto-deploy enable** to disable automatic deployment for the specified SSID.

gwc ssid *name* **isolation enable**

Enable client isolation for the specified SSID.

ssid — Configure an SSID.

name — Specify the SSID name.

isolation — Control whether wireless clients can communicate directly to each other through the AP device.

Use **no gwc ssid** *name* **isolation enable** to disable client isolation for the specified SSID.

gwc ssid *name* **mac-acl enable** (**allowed**|**denied**)

Use the MAC address access control list defined in the Gateway Wireless controller settings.

ssid — Configure an SSID.
name — Specify the SSID name.
mac-acl — MAC address access control list.
allowed — Allowed MAC addresses.
denied — Denied MAC addresses.

Use **no gwc ssid** *name* **mac-acl enable** to disable MAC address access control.

gwc ssid *name* **vlan-tagging enable** *vlan-id*

Configure the VLAN ID for an SSID.

ssid — Configure an SSID.
name — Specify the SSID name.
vlan-tagging — Enable VLAN tagging.
vlan-id — Specify the VLAN ID.

Use **no gwc ssid name vlan-tagging enable** to disable VLAN tagging.

gwc ssid *name***rogue-detect enable bssid**

Configure rogue AP detection for an SSID.

enabled — Enable rogue AP detection on this SSID.
bssid — Specify rogue AP exceptions by MAC address.

Use **no gwc ssid name rogue-detect enable** to disable rogue AP detection.

gwc ssid *name* **security** (**wpa-only**|**wpa2-only**|**wpa-wpa2**) **encryption** *passphrase* [**interval** interval]

Enable encryption security for an SSID.

ssid — Configure an SSID.
name — Specify the SSID name.
security — Select the security mode: wpa-only, wpa2-only, or wpa-wpa2.
encryption — Select the type of encryption: AES, AES or TKIP.
passphrase — Type the encryption passphrase.
interval — Type the group key update interval. 30 to 3600 seconds.

Use **no gwc ssid name security enable** to disable encryption security.

gwc ssid *name* **security** (**wpa-e**|**wpa2-e**|**wpa-wpa2-e**) *encryption radius-server radius-secret* [**interval** *interval*][**port** *port*][**accounting enable** *accounting-server accounting-secret* [**accounting-port** *accounting-port*] [**accounting-interval** *accounting-interval*]]

Enable enterprise encryption security with a RADIUS server.

ssid — Configure an SSID.
name — Specify the SSID name.
security — Select the security mode: wpa-e, wpa2-e, or wpa-wpa2-e.
encryption — Select the type of encryption: AES, AES or TKIP.
radius-server — Type the RADIUS server address.
radius-secret — Type the RADIUS secret.

interval — Type the group key update interval. 30 to 3600 seconds.
port — Type the RADIUS port.1 to 65535.
accounting — Enable RADIUS accounting server.
accounting-server — Type the address of the RADIUS accounting server.
accounting-secret — Type the RADIUS secret for the accounting server.
accounting-port — Type the port for the RADIUS accounting server.
accounting-interval — Type the group key update interval for the RADIUS accounting server. 30 to 3600 seconds.

Use **no gwc ssid** *name* **security** (**wpa-e**|**wpa2-e**|**wpa-wpa2-e**) *encryption radius-server radius-secret* **accounting enable** to disable enterprise encryption security.

gwc ssid *name* **access-point** *ap-name* [**access-point** *ap-name*]

Add a WatchGuard AP device to an SSID.

ssid — Configure an SSID.
name — Specify the SSID name.
access-point — Configure a WatchGuard AP device.
ap-name — Name of the WatchGuard AP device.

Use **no gwc ssid** *name* **access-point** *ap-name* [**access-point** *ap-name*] to remove the WatchGuard AP device from an SSID.

gwc ssid *name* **station-rate-shaping** *enable*

Activate traffic rate-shaping per user for an SSID.

ssid — Configure an SSID.
name — Specify the SSID name.
station-rate-shaping — Configure traffic rate-shaping per user for this SSID.
enable — Enable traffic rate-shaping per user for this SSID.

gwc ssid *name* **max-download-rate|max-station-download-rate|max-station-upload-rate|max-upload-rate** *rate*

Specify the rate shaping options for the SSID

ssid — Configure an SSID.
name — Specify the SSID name.
max-download-rate — Restrict download bandwidth on the SSID.
max-station-download-rate — Restrict download rate per user on the SSID.
max-station-upload-rate — Restrict upload rate per user on the SSID.
max-upload-rate — Restrict upload bandwidth on the SSID.

gwcssid *name***fast-roaming***enable*

Enable fast roaming on an SSID. Requires WPA2 security.

ssid — Configure an SSID.
name — Specify the SSID name.
fast roaming — Configure fast roaming for this SSID.
enable — Enable fast roaming for this SSID.

gwcssid *name***band-steering***enable*

Enable band steering on an SSID.

ssid — Configure an SSID.
name — Specify the SSID name.
band-steering — Configure band steering for this SSID.
enable — Enable band steering for this SSID.

gwcssid *name***min-assn-rssi***enable*

Enable minimum association RSSI on an SSID.

ssid — Configure an SSID.
name — Specify the SSID name.
min-assn-rssi — Configure minimum association RSSI for this SSID.
enable — Enable minimum association RSSI for this SSID.

gwcssid *name***smart-steering***enable*

Enable smart steering on an SSID.

ssid — Configure an SSID.
name — Specify the SSID name.
min-assn-rssi — Configure smart steering for this SSID.
enable — Enable smart steering for this SSID.

gwc ssid *name* **time-based-activation** *enable*

Enable time-based activation for an SSID.

ssid — Configure an SSID.
name — Specify the SSID name.
time-based-activation — Configure time-based activation for an SSID.
enable — Enable time-based activation for this SSID.

gwc ssid *name* **time-based-interval** *start-hour start-min end-hour end-min*

Set the interval for time-based activation for an SSID.

ssid — Configure an SSID.
name — Specify the SSID name.
time-based-interval — Configure the activation time period for this SSID.
start-hour — Must be an integer from 0-23.
start-min — Must be an integer from 0-59.
end-hour — Must be an integer from 0-23.
end-min — Must be an integer from 0-59.

gwc ssid *name* **vulnerability-mitigation**

Enable WPA/WPA2 vulnerability mitigation for an SSID.

ssid — Configure an SSID.

name — Specify the SSID name.

vulnerability-mitigation — Enable WPA/WPA2 KRACK vulnerability mitigation that blocks handshake messages that can potentially exploit clients and forces clients to reauthenticate.

no gwc access-point *name* [*automatic*]

Remove a WatchGuard AP device from the Gateway Wireless Controller.

access-point — Configure a WatchGuard AP device.

name — WatchGuard AP device name.

automatic — Remove the WatchGuard AP device without confirmation.

gwc access-point *name model serial-num passphrase*

Add or edit a WatchGuard AP device.

access-point — WatchGuard AP device.

name — WatchGuard AP device name.

model — Select the AP device model.

serial-num — Type the WatchGuard AP device serial number. Must be 13 characters in length.

passphrase — Type the pairing passphrase.

gwc access-point *name* **location** *location*

Edit the location of a WatchGuard AP device.

access-point — WatchGuard AP device.

name — WatchGuard AP device name.

location — Location of the WatchGuard AP device.

Use **no gwc access-point** *name* **location** *location* to remove the location of a WatchGuard AP device.

gwc access-point *name* **syslog-server enable** *server-ip*

Configure a syslog server for the WatchGuard AP device.

access-point — WatchGuard AP device.

name — WatchGuard AP device name.

syslog-server — Send log messages to a syslog server.

server-ip — Type the syslog server IP address.

Use **no gwc access-point** *name* **syslog-server enable** to disable logging to a syslog server.

gwc access-point *name* **mgmt-vlan enable** *vlan-id*

Configure a management communications VLAN ID for a WatchGuard AP device.

access-point — WatchGuard AP device.

name — WatchGuard AP device name.

mgmt-vlan — Use management communications VLAN tagging.

vlan-id — Type the management communications VLAN ID.

Use **no gwc access-point** *name* **mgmt-vlan enable** to disable management communications VLAN tagging.

gwcaccess-point*name* [**roam-interval**|**roam-packets**|**steer-attempts-thresh**|**steer-blackout-period**|**steer-rssi-thresh** *value*

Configure steering parameters for a WatchGuard AP.

access-point — WatchGuard AP.
name — WatchGuard AP name.
roam-interval — Roam Initiation Threshold Interval (seconds).
roam-packets— Roam Initiation Threshold Packets.
steer-attempts-thresh — Steering Attempts Threshold.
steer-blackout-period — Steering Blackout Period (minutes).
steer-rssi-thresh — Steering RSSI Threshold (dBm).

gwc access-point *name* [**band-steering**|**fast-handover**|**disable-leds enable** *rssi_threshold*

Enable options of a WatchGuard AP device.

access-point — WatchGuard AP device.
name — WatchGuard AP device name.
band-steering — Enable band steering on this AP device. (Fireware v12.0.2 and lower)
fast-handover — Enable fast handover on this AP device. (Fireware v12.0.2 and lower)
rssi_threshold — The RSSI threshold for Fast Handover in dBm. For example, *-85*. (Fireware v12.0.2 and lower)
disable-leds — Disable LEDs on the WatchGuard AP device to hide its activity.

Use **no gwc access-point** *name* [**disable-leds**| **enable** to disable these options.

gwc access-point *name* **network dhcp**

Configure the WatchGuard AP device to use DHCP.

access-point — WatchGuard AP device.
name — WatchGuard AP device name.
network — Configure network settings.
dhcp — Obtain an IP address from DHCP.

gwc access-point *name* **network** (*ip netmask*|*net*) *default-gw*

Configure the WatchGuard AP device with a static IP address.

access-point — WatchGuard AP device.
name — WatchGuard AP device name.
network — Configure network settings.
ip — Type an IP address.
netmask — Type a subnet mask.
net — Type an IP address with slash network notation.
default-fw — Specify the default gateway.

gwc access-point *name* (**radio1**|**radio2**) [**band** *band*][**wireless-mode** *wireless-mode*] **[preferred-channel** *preferred-channel*] [**channel-width** *channel-width*]] [**client-limit**] [**transmit-power** *transmit-power*]

Configure the radio settings for a WatchGuard AP device.

access-point — WatchGuard AP device.

name — WatchGuard AP device name.

radio — Specify radio1 or radio2.

band — Select the radio frequency band: 2.4 GHz or 5 GHz.

wireless-mode — Set the wireless mode. When the band is 2.4 GHz, the value can be: 802.11 B/G/N Mixed, 802.11 B/G Mixed, 802.11 G, 802.11 G/N, or 802.11 N only. When the band is 5 GHz. The value can be: 802.11 A/N Mixed, 802.11 A, 802.11 N only, or 802.11 AC.

preferred-channel — Set the preferred channel. This is based on your country information.

channel-width — Set the channel width: 20MHz, 40MHz, 80MHz, or 20/40 MHz.

client-limit — Set the client limit for this radio (0-127). 0 means unlimited.

transmit-power — Set the transmit power.

gwc use-trust-mechanism enable

Enable the Trust Store to identify trusted AP devices in your deployment.

Use **no gwc use-trust-mechanism enable** to disable the Trust Store and trust all AP devices.

Example

```
gwc enable
gwc ssid mywireless
gwc ssid mywireless broadcast enable
gwc ssid mywireless mac-acl enable denied
gwc access-point ap1 disable-leds enable
gwc access-point ap1 network dhcp
gwc access-point ap1 mgmt-vlan enable 10
gwc access-point ap1 ap100 123456789abcd mypassphrase
```

hotspot

Description

Create or modify a custom hotspot, or configure the hotspot guest administrator and hotspot global settings that apply to all enabled hotspots.

Syntax

hotspot guest-admin (*name*) **auth-server** (**Firebox-DB** | **auth-server** *auth-server*) (**password** *password*)

Add Guest Administrator account to the hotspot configuration. A Guest Administrator can connect to the Guest Administration portal on the Firebox to configure the settings for the guest user accounts and customize the vouchers guest users receive with their user account information. The Guest Administrator can also delete guest user accounts before they expire.

name specifies the name of the Guest Administrator. You can use these characters for the Guest Administrator user name: (A–Z, a–z), (0-9), or (-,space,_,.,*).

auth-server is the authentication server where the Guest Administrator credentials are stored.

Specify **Firebox-DB** for a local user account defined on the Firebox.

Specify **auth-server** for a user account on an external authentication server, and specify the name of the *authentication server*: LDAP, RADIUS, SecurID, or the Active Directory domain name.

password specifies the password for the user account in Firebox-DB.

hotspot *timeout-type* [**day** *days*] [**hour** *hours*] [**minute** *minutes*] [**second** *seconds*]

Configure global timeout settings to limit the amount of time that users can continuously use any hotspot.

timeout-type is the timeout option for hotspot sessions. It must be one of these options:

idle-timeout — The maximum length of time the user can stay connected to the hotspot when they do not send or receive traffic. . If you set this value to 0, users are not disconnected if they do not send or receive traffic.

session-timeout — The maximum length of time the user can remain connected to the hotspot. If you set this value to 0, the hotspot session does not expire and the user can stay connected for any length of time.

Specify the hotspot timeout durations in days, hours, minutes and seconds.

days — The number of days as an integer from 0 to 365.

hours — The number of hours as an integer from 0 to 23.

minutes — The number of minutes as an integer from 0 to 59.

seconds — The number of seconds as an integer from 0 to 59.

hotspot maximum-accounts *limit*

Set a limit on the number of guest user accounts that Guest Administrators can add. This setting limits the combined total number of users that Guest Administrators can add for all hotspots.

limit is the maximum number of accounts. It must be an integer between 1 and 6000.

hotspotname (*hotspot-name*)

Add or edit a hotspot with the specified name.

hotspot-name is a string that uniquely identifies the hotspot in the configuration.

After you type the command **hotspot name** *hotspot-name*, additional commands are available for you to configure the hotspot details.

The prompt changes to: `WG(config/hotspot-hotspot-name`

Use **no hotspot name** *hotspot-name* to remove a configured hotspot.

Custom Hotspot Settings

Use the remaining hotspot commands to configure settings for a hotspot and enable the hotspot for one or more Firebox interfaces. These commands are available only after you use the **hotspot name** command to configure a hotspot.

Use the **Exit** command to exit this mode.

auto-redirect ("*url*")

Specifies the url that users are redirected to after they accept the terms on the hotspot splash screen.

url is the URL of the web site users are redirected to. It must be enclosed in double quotes.

background-color ("*background-color*")

Sets the color of the hotspot splash screen background. The default color is #FFFFFF (white).

background-color must be a hex color code in the format “#RRGGBB” where RR is Red, GG is Green, and BB is Blue. Each character must be a hex value <[-](alpha|0-9)(alpha|0-9|-|_|.)*>. You must use quotes around these color codes.

connectionscredentials (**name-and-passphrase** *maximum-accounts*| **only-passphrase** *maximum-accounts*)

Enables the *Custom Page* hotspot to require users to specify credentials when they connect to the hotspot.

Specify *name-and-passphrase* to require users to specify a user name and a passphrase to connect.

Specify *only-passphrase* to require users to specify only a passphrase to connect.

maximum-accounts is the maximum number of user accounts that can be included in the hotspot configuration at any time.

connections no-credentials lock-time [**day** *days*] [**hour** *hours*] [**minute** *minutes*] [**second** *seconds*]

Enables the *Custom Page* users to connect to the hotspot without user names and passphrases.

lock-time is the amount of time users are locked out of the hotspot after their session times out. If you specify 0 for the lockout value, users are not locked out and can log in again immediately after their sessions expire.

days — The number of days as an integer from 0 to 365.

hours — The number of hours as an integer from 0 to 23.

minutes — The number of minutes as an integer from 0 to 59.

seconds — The number of seconds as an integer from 0 to 59.

enable *interface*

Enable the hotspot on the specified interface.

interface is the name of an interface. It can be any enabled trusted, optional, or custom interface. The interface name is case-sensitive.

You can specify more than one interface, separated by spaces.

Use **no enable** *interface* to disable the hotspot on the specified interface.

font-color ("*font-color*")

Sets the color of the text on the hotspot splash screen. The default color is #000000 (black).

background-color must be a hex color code in the format “#RRGGBB” where RR is Red, GG is Green, and BB is Blue. Each character must be a hex value <[-](alpha|0-9)(alpha|0-9|-|_|.)*>. You must use quotes around color codes.

font-name (*font-name*)

Sets the font for the text on the hotspot splash screen.

font-name must be one of these values: arial, comic-sans-ms, courier-new, georgia, lucida-console, microsoft-sans-serif, tahoma, times-new-roman, trebuchet-ms, verdana.

hotspot font-size (*font-size*)

Sets the font size for the text on the hotspot splash screen.

font-size must be one of these values: xx-small, small, medium, large, x-large, xx-large.

logo [**from** *from*]

Sets the logo for the hotspot splash page.

from — Specify the file name and location of the hotspot splash screen page logo.

terms-text (**input** *input* | **from** *from*)

Import a text file with the terms and conditions that users must agree to before they can connect to your network. The terms and conditions text must be less than 20000 characters.

input — Type the terms and conditions text.

from — Specify the file name and location of the text file with the terms and conditions text. The location must be an FTP or TFTP server.

title ("*title*")

Configures the title on the splash screen for the *Custom Page* hotspot type.

title is the title text on the splash screen page. The title text must be enclosed in quotation marks.

use-logo (**custom** *custom* | **default** *default*)

Configures the logo that appears on the splash screen for a *Custom Page* hotspot type.

custom is the URL to the file name for the custom logo to use on the hotspot splash screen.

default selects the default WatchGuard logo.

welcome-message (**input** *input* | **from** *from*)

Configures the *Welcome* message that appears on the splash screen for the *Custom Page* hotspot type. The maximum allowed number of characters is 2048.

input — Type the *Welcome* message text.

from — Specifies the file name and location of the *Welcome* message text file. The location must be an FTP or TFTP server.

Example

```
hotspot name myhotspot

enable Trusted

background-color "CCFFFF"

font-color "99CCCC" font-name verdana font-size medium

connections no-credentials lock-time 1 day

welcome-message input Welcome to the Successful Company Hotspot!

terms-text from tftp://myserver/terms.txt

use-logo custom tftp://myserver/customlogo.jpg

authentication-url "https://10.0.2.80:8080/auth.html" failure-url
"http://10.0.2.80:8080" secret myhotspotsecret

hotspot guest-admin Example-Co_Admin auth-server Firebox-DB

hotspot idle-timeout hour 2 minute 30

hotspot session-timeout hour 23
```

interface

Description

Configure the specified interface. This command starts interface mode to enable commands to configure the specified interface. After you use the interface command, the configuration continues to the interface details commands.

In Interface mode, the command prompt changes to "WG(config/if-fe*n*)#", where *n* is the interface number you specified.

For information about the commands available in this mode, see *Interface Commands*.

Use the **Exit** command to exit this mode.

Syntax

interface FastEthernet (*number*)

number must be an integer from 0 to the max number of ports minus one, depending on the platform and model.

Example

```
interface FastEthernet 0
```

intrusion-prevention

Description

Enable and configure the Intrusion Prevention Service (IPS).

Syntax

intrusion-prevention enable

Enable the Intrusion Prevention Service.

Use **no intrusion-prevention enable** to disable the Intrusion Prevention Service.

intrusion-prevention exception (*signature-ID*) (*action*) (*record-method*)

Create an IPS exception for a signature.

signature-ID is the IPS signature ID number.

action is the action to take when the IPS signature is matched. It must be one of these options:

block — denies the request, drops the connection, and adds the IP address of the sender to the Blocked Sites list.

drop — denies the request, and drops the connection. No information is sent to the source of the message.

allow — allows the connection

record-method is the method to record the event when the exception has been matched. It must be one of these options:

log — send a message to the log file.

alarm — trigger an alarm.

all — send a message to the log file and trigger an alarm.

intrusion-prevention notification notification enable [**action-type** *action-type*] [**launch-interval** *launch-interval*] [**repeat-count** *repeat-count*]

Configure IPS exception notification settings.

You must set the notification action-type to one of these settings:

email — the Log Server sends an email to the configured email address when an event occurs.

pop-window — the Log Server opens a dialog box when an event occurs.

launch-interval is the minimum time (in minutes) between different notifications, default is 15.

repeat-count is the number of events to include in a repeat log notification, default is 10.

intrusion-prevention notification snmp enable

Enable the device to send event notifications to the configured SNMP management system.

intrusion-prevention (*threat-level*) (*action*) (*record-method*)

Configure the action for each IPS threat level

threat-level is the IPS threat level associated with the signature. It must be one of these options: **critical**, **high**, **medium**, **low**, or **information**.

action is the action to take when the IPS signature at this threat level is matched. It must be one of these options:

block — denies the request, drops the connection, and adds the IP address of the sender to the Blocked Sites list.

drop — denies the request, and drops the connection. No information is sent to the source of the message.

allow — allows the connection

record-method is the method to record the event when an IPS action occurs for the specified threat level. It must be one of these options:

log — send a message to the log file.

alarm — trigger an alarm.

all — send a message to the log file and trigger an alarm.

intrusion-prevention mode (**full-scan|fast-scan**)

Select the IPS scan mode. There are two scan modes.

full-scan — Scan all packets for policies that have IPS enabled.

fast-scan — Scans fewer packets to improve performance. This option greatly improves the throughput for scanned traffic, but does not provide the comprehensive coverage of full-scan mode.

intrusion-prevention (**used-by** *policy-name*)

Enable IPS for a policy.

policy-name must match the name of an existing policy in the device configuration. The policy name is case-sensitive.

Use **no intrusion-prevention used-by policy-name** to disable the IPS for a policy.

Example

```
intrusion-prevention enable

intrusion-prevention threat-level critical block alarm
```

```
intrusion-prevention notification notification enable action-type email
intrusion-prevention used-by http-proxy
intrusion-prevention exception 1052692 allow log
intrusion-prevention mode fast-scan
```

ip

Description

Configure Internet Protocol settings for firewall features, for example, blocked sites and ports.

Syntax

ip allowed-site (*address*)

Add or remove an IP address from the allowed IP address list. This is also known as the blocked sites exceptions list.

address must be one of these options: **host** *ip*, **range** *startip endip* , **subnet** *net*, or **FQDN** *fqdn-site*.

ip, *startip*, and *endip* must be an IPv4 address in the format of A.B.C.D or an IPv6 address in the format A:B:C:D:E:F:G:H.

net must be an IPv4 subnet in the format of A.B.C.D/# where # must be in the range of 0 to 32 or an IPv6 subnet in the format A:B:C:D:E:F:G:H/I.

fqdn-site is a Fully Qualified Domain Name. This includes wildcard domains. For example, *host.example.com*, or *"*.example.com"*.

Use **no ip allowed-site** to clear all entries on the allowed IP address list.

ip blocked-port *port* [**log** *logstate*] [**auto-blocked** *autostate*] [**alarm** *alarmsetting alarmoption*]

Block all traffic to the specified port or ports.

port is an integer from 1 to 65535. You can configure more than one port.

logstate enables or disables log messages when packets are addressed to the specified port. The value must be: **enable** or **disable**.

autostate enables automatic addition of the source IP address to the list of blocked sites when packets are addressed to the specified port. The value must be: **enable** or **disable**.

alarmsetting selects the notification alarm parameter. *alarmoption* configures the parameter. The values must be one of these options:

action-type (**email**|**popup**)— The alarm notification method. The value must be **email** or **popup**

blocked-ip-enable (**enable**|**disable**) — enable or disable blocking

launch-interval *interval* — an integer from 60 to 3932100. The minimum time (in minutes) between different notifications.

remote-enable (**enable**|**disable**)

repeat-count — an integer from 1 to 256

trap-enable(**enable**|**disable**) — enable or disable the Firebox to send SNMP notifications.

You can configure more than one alarm setting.

ip blocked-port notification *(notification_action)* **enable** [**log-rate** *int*] [**action-type email|pop-window**] [**launch-interval** *int*] [**repeat-count** *count*]

Enable notifications for blocked ports.

notification_action is the form of notification. It must be one of these options:

log-message — Send log message

notification — Send notification

snmp-trap — Send SNMP trap

If *notification_action* is **log-message**, these notification options are also available:

log-rate *int* specifies the maximum number of log messages the Firebox generates for blocked ports in a minute. It must be an integer from 1 to 2000000000.

If *notification_action* is **notification**, these notification options are also available:

action-type specifies the notification action. It can be one of these options:

email — Sends an email

pop-window — Opens a pop-up window

launch-interval *int* is the minimum time in minutes between notifications. It must be an integer from 1 to 65525.

repeat-count *count* is the number of times an event must occur before a repeat notification is sent. It must be an integer from 1 to 256.

ip blocked-site (*domain*) [**alarm** *alarmsetting alarmoption*] ...

Block all traffic from the specified domain name.

domain is a domain name, for DNS lookups.

alarmsetting selects the notification alarm parameter. *alarmoption* configures the parameter. The values must be one of these options:

action-type (**email**|**popup**)— The alarm notification method. The value must be **email** or **popup**

blocked-ip-enable (**enable**|**disable**) — enable or disable blocking

launch-interval*interval* — an integer from 60 to 3932100. The minimum time (in minutes) between different notifications.

remote-enable (**enable**|**disable**)

repeat-count — an integer from 1 to 256

trap-enable(**enable**|**disable**) — enable or disable the Firebox to send SNMP notifications.

You can configure more than one alarm setting.

ip blocked-site (**duration** (*minutes*)

Configure the duration that a site remains on the blocked sites list after being automatically added because of packet handling rules.

minutes is an integer from 1 to 99999.

ip blocked-site (**dynamic** *ip-address*) **expire-after** [**day** *dd*] [**hour** *hh*] [**minute** *min*] [**second** *sec*]

Block all traffic from specified IP addresses for the specified time.

ip-address is the address of the host to be temporarily blocked. It must be an IPv4 address in the format of A.B.C.D or an IPv6 address in the format A:B:C:D:E:F:G:H.

dd is the number of days from 0 to 365.

hh is the number of hours from 0 to 23.

min is the number of minutes from 0 to 59.

sec is the number of seconds from 0 to 59.

Use **no ip blocked-site** (**dynamic** *ip-address*) to remove a site from the temporary blocked sites list.

ip blocked-site dynamic flush

Flush the status of all dynamically blocked sites.

ip blocked-site (*address*) [**alarm** *alarmsetting alarmoption*]

Block all traffic from specified host, subnet or range of IP addresses.

address must be one of these options: **host** *ip*, **range** *startip endip* , **subnet** *net*, or **FQDN** *fqdn-site*.

ip, *startip*, and *endip* must be an IPv4 address in the format of A.B.C.D or an IPv6 address in the format A:B:C:D:E:F:G:H.

net must be an IPv4 subnet in the format of A.B.C.D/# where # must be in the range of 0 to 32 or an IPv6 subnet in the format A:B:C:D:E:F:G:H/I.

fqdn-site is a Fully Qualified Domain Name. This includes wildcard domains. For example, *host.example.com*, or *"*.example.com"*.

alarmsetting selects the notification alarm parameter. *alarmoption* configures the parameter. The values must be one of these options:

action-type (**email**|**popup**)— The alarm notification method. The value must be **email** or **popup**

blocked-ip-enable (**enable**|**disable**) — enable or disable blocking

launch-interval*interval* — an integer from 60 to 3932100. The minimum time (in minutes) between different notifications.

remote-enable (**enable**|**disable**)

repeat-count — an integer from 1 to 256

trap-enable(**enable**|**disable**) — enable or disable the Firebox to send SNMP notifications.

You can configure more than one alarm setting.

Use **no blocked-site** (*address*) to remove an address from the blocked sites list.

ip blocked-site notification *(notification_action)* **enable** [**action-type email|pop-window**] [**launch-interval** *int*] [**repeat-count** *count*]

Enable notifications for blocked sites.

notification_action is the form of notification. It must be one of these options:

notification — Send notification

snmp-trap — Send SNMP trap

If *notification_action* is **notification**, these notification options are also available:

action-type specifies the notification action. It can be one of these options:

email — Sends an email

pop-window — Opens a pop-up window

launch-interval *int* is the minimum time in minutes between notifications. It must be an integer from 1 to 65525.

repeat-count *count* is the number of times an event must occur before a repeat notification is sent. It must be an integer from 1 to 256.

ip blocked-site notification log-message (**log-rate** *int)*

Enables log messages and specifies the maximum number of log messages the Firebox generates for blocked sites.

log-rate *int* is the maximum number of log messages to generate in a minute. It must be an integer from 1 to 2000000000.

ip dns cache enable

By default, the DNS cache is enabled if you enable DNS forwarding or DNSWatch. When the DNS cache is enabled, the Firebox caches the results of DNS queries (up to 10,000 entries).

Use **no ip dns cache enable** to disable the DNS cache.

ip dns domain-name (*domain*)

Provide a default domain name to complete unqualified host names.

domain is the provided domain name.

Use **no ip dns domain-name** to remove the DNS domain name.

ip dns forwarding

Enable and configure DNS forwarding.

Use **ip dns forwarding enable** enable to enable DNS forwarding.

Use **no ip dns forwarding enable** to disable DNS forwarding.

ip dns forwarding [*domain*] (*domain name*) [*server*] (*server IP address*)

Add a conditional DNS forwarding rule. DNS queries for the domain you specify are forwarded to the DNS server that you specify.

ip dns forwarding interface (*interface name*)

Specify the Trusted, Optional, or Custom interface on which DNS forwarding is enabled.

ip dns forwarding log enable

Enable log messages for DNS forwarding.

ip dns server *address*

Add or remove a DNS server(s).

address is the IPv4 or IPv6 address of a DNS server. You can configure a maximum of three DNS server IP addresses.

If *destination* is an IPv4 host, the IPv4 address must be in the format A.B.C.D

If *destination* is an IPv6 host, the IPv6 address must be in the format A:B:C:D:E:F:G:H.

Use **no ip dns servers** to remove all DNS server entries.

ip dynamic-routing [*protocol*] **enable**

Enable dynamic routing for the specified dynamic routing protocol. You must import a valid dynamic routing configuration file before you can enable a dynamic routing protocol.

protocol must be one of these options: **bgp**, **ospf**, or **rip**.

If *protocol* is not specified, dynamic routing is enabled but not configured for any protocol.

When you enable a dynamic routing protocol, Fireware automatically adds the necessary dynamic routing policy for that protocol. The automatically created policies are called DR-RIP-Any, DR-OSPF-Any, and DR-BGP-Any.

ip multicast

Enable multicast routing and configure settings.

enable — Enable the PIM-SM multicast routing protocol globally. You must also enable multicast routing on Firebox interfaces.

interface *(interface name)* — Enable multicast routing for an interface

setinterface*(interface name)***rp-candidate** — Specify an interface as a Rendezvous Point (RP) candidate

ip route (*destination*) (*fwdaddr*) [**metric** *metricvalue*]

Create an IPv4 static network route.

destination must be one of these options: *ipaddress* or *net*.

ipaddress is the IP address for the destination in the format of A.B.C.D.

net is the IP subnet for the destination in the format of A.B.C.D/# where # must be in the range of 0 to 32.

fwdaddr is the IP address of the forwarding router, in the format of A.B.C.D.

Use **no ip route** (*destination*) to remove a static route.

ip route vpn-route (vif-name) (*destination*) [**metric** *metricvalue*]

Create a BOVPN virtual interface route.

vif-name must be the name of a configured BOVPN virtual interface.

destination must be one of these options: *ipaddress* or *net*.

ipaddress is the IP address for the destination in the format of A.B.C.D.

net is the IP subnet for the destination in the format of A.B.C.D/# where # must be in the range of 0 to 32.

metricvalue is the route metric. It must be an integer from 1 to 254. The default metric is 1.

Use **no ip route vpn-route** (*destination*) to remove a static route.

ip wins (*address*)

Configure WINS servers used by the Firebox for services such as Mobile VPN and DHCP.

address must be an IPv4 address in the format of A.B.C.D.

You can configure a maximum of three IP addresses.

Use **no ip wins** to clear all WINS server addresses out of the configuration.

Example

```
ip allowed-site host 200.23.101.3

ip blocked-port 2000 log enable auto-blocked enable alarm blocked-ip-enable
enable launch-interval 60 repeat 3 action-type email

ip blocked-site www.example.com

ip blocked-site 200.23.103.0/24

ip blocked-site duration 15

ip blocked-site notification log-message log-rate 5

ip dns domain-name example.com

ip dns server 192.168.1.1 192.168.1.2

ip dns server 2561:1900:4545:0003:0200:F8FF:FE21:67CF

ip dynamic-routing bgp

ip multicast enable

ip multicast interface External

ip multicast set interface External rp-candidate

ip route 100.100.101.3 200

ip route vpn-route BovpnVif.1 10.10.10.0/24
```

```
ip wins 192.168.1.1 192.168.1.2
```

link-aggregation

Description

Create or edit a link aggregation interface on the Firebox. This command starts link aggregation mode to enable commands to configure the specified link aggregation interface. After you use the link-aggregation command, the configuration continues to the link-aggregation details commands.

In link aggregation mode, the command prompt changes to "WG(config/link-aggregation-<la-name>)#" where <la-name> is the selected link aggregation interface.

For more information about commands available in this mode, see *Link Aggregation Commands*.

Use the **Exit** command to exit this mode.

Syntax

link-aggregation (*la-name*)

la-name is a name that uniquely identifies the link aggregation interface.

Use **no link-aggregation** (*la-name*) to delete the link aggregation interface.

Example

```
link-aggregation LA-1
```

link-monitor

(Fireware v12.3 or higher) Configure link monitor targets for interfaces. In Fireware v12.4 or higher, you can add internal interfaces (Trusted, Optional, and Custom) and BOVPN virtual interfaces to Link Monitor.

In Fireware v12.2.1 or lower, the **link-monitor** command is part of the **multi-wan** command.

link-monitor *(interface name)*

Use **link-monitor** *(interface name)* **enable** to enable link monitor for an interface. The interface must already exist.

Use **no link-monitor** *(interface name)* **enable** to disable link monitor for an interface.

no **link-monitor** (*interface*) **interval** (*frequency*)

interface is the name of the external interface. *Frequency* must be a number between 1 and 1200.

no **link-monitor** (*interface*) **next hop** *(IP address)*

(Fireware v12.4 or higher) *(IP address)* is the IP address of the next hop.

no **link-monitor** (*interface*) [**deactivate-count***dcount*]

dcount is the number of failures that must occur for the Firebox to deactivate the interface. The default value is 3. You must specify a number between 1 and 10.

no **link-monitor** (*interface*) [**reactivate-count***rcount*]

rcount is the number of successes that must occur for the Firebox to reactivate the interface. The default value is 3. You must specify a number between 1 and 10.

no **link-monitor** (*interface*) [**operation***operation*]

operation sets whether the probe uses both TCP and PING to check the status, or only one. It must be either: AND or OR. The default value is OR.

no **link-monitor** (*interface*) (**ping***icmptarget*)

Enable a ping link monitor for an interface.

icmptarget is the destination host that the Firebox can ping to check the status. It must be either a domain name or an IP address in the format A.B.C.D.

One target in the link monitor configuration must be configured to measure loss, latency, and jitter with the **measured** command. To measure loss, latency, and jitter for this target, use **link-monitor** (*interface*) **ping***(IP address or domain name)* **measured**

Use **no link-monitor** *(interface)***ping** *(IP address)* to disable a ping target for an interface.

link-monitor (*interface*) (**tcp***tcpaddress*)

Enable a TCP link monitor for an interface.

tcpaddress is the IP address and port of a destination host that the Firebox can use to negotiate a TCP handshake to check status. It must be an address in the format A.B.C.D #, where # is an integer from 1 to 65535.

One target in the link monitor configuration must be configured to measure loss, latency, and jitter with the **measured** command. To measure loss, latency, and jitter for this target, use **link-monitor** (*interface*) **tcp***(IP address)* **measured**

Use **no link-monitor** *(interface)***tcp** *(IP address)* to disable a ping target for an interface.

link-monitor (*interface*) (**dns***IP address*) *(domain name)*

Enable a DNS link monitor for an interface.

IP address is the IP address of the destination host that the Firebox can ping to check the status. It must be an IP address in the format A.B.C.D.

Domain name is the domain name of the destination host that the Firebox can ping to check the status.

One target in the link monitor configuration must be configured to measure loss, latency, and jitter with the **measured** command. To measure loss, latency, and jitter for this target, use **link-monitor** (*interface*) **dns***(IP address)* (domain name) **measured**

Use **no link-monitor** *(interface)***dns** *(IP address)* to disable a ping target for an interface.

Example

```
link-monitor External-1 ping 203.0.113.50 measured

link-monitor Trusted ping 10.0.50.1 measured

link-monitor External-2 dns 203.0.113.50 example.com measured

no link-monitor External-2 dns 203.0.113.50
```

log-setting

Description

Enable message logging facilities.

Syntax

log-setting debug-level (*type*) (*level*)

Control debug log messages of the type and level specified.

type must be one of these options:

Access-Portal-52 — diagnostic log level for Access Portal

Authentication — debug log level for authentication and access authorization

Daas-53 — diagnostic log level for the component that enables the Firebox to communicate with WatchGuard Cloud

FireCluster-2 — debug log level for all FireCluster components

Cluster-Management-3 — debug log level for cluster configuration and management tasks

Cluster-Event-Monitoring-4 — debug log level for the process that monitors FireCluster resources

Cluster-Transport-5 — debug log level for FireCluster member communication channels

Cluster-Operation-6 — debug log level for cluster member roles and operations

Firewall-7 — debug log level for all firewall activities, including packet filtering and default threat protection

FQDN-49 — debug log level for the FQDN (fully-qualified domain name) component

Management-8 — debug log level for Firebox management

Mobile-Security-46 — debug log level for Mobile Security

EPM-48 — debug log level for the End-Point Manager component

Networking-9 — debug log level for all networking components

DHCP-client-10 — debug log level for the component that enables the Firebox to receive IP address assignments from a DHCP server

DHCP-server-11 — debug log level for the component that enables the Firebox to assign IP address information to DHCP clients

PPP-12 — debug log level for PPP support component for PPPoE

PPPoE-13 — debug log level for PPPoE

Dynamic-Routing-36 — debug log level for dynamic routing

RADVD-37 — debug log level for IPv6 router advertisements

GWC-39 — debug log level for the Gateway Wireless Controller

Static Interface-40 — debug log level for the component that specifies the static IP address for an interface

Link Monitor-41 — debug log level for the Link Monitor

Network-Diagnostics-43 — debug log level for the component that runs network diagnostics

DIM-47 — debug log level for the Device Info Manager component

DHCP-Fingerprinting-49 — debug log level for the DHCP Fingerprinting component

Proxy-14 — debug log level for all proxy components

Connection-Framework-Manager-15 — debug log level for the component that manages proxy policy connections

Session-Manager-16 — debug log level for the component that converts network packet streams into TCP and UDP connections

DNS-17 — debug log level for the DNS connection analysis component

FTP-18 — debug log level for the FTP connection analysis component

H323-19 — debug log level for the H.323 connection analysis component

HTTP-20 — debug log level for the HTTP connection analysis component

HTTPS-21 —debug log level for the HTTPS connection analysis component

POP3-22 — debug log level for the POP3 connection analysis component

SMTP-23 — debug log level for the SMTP connection analysis component

SIP-24 — debug log level for the SIP connection analysis component

TCP-UDP-25 — debug log level for the TCP-UDP connection analysis component

Security-Subscriptions-27 — debug log level for all security subscription services

Gateway-Antivirus-28 — debug log level for Gateway AntiVirus

spamBlocker-29 — debug log level for SpamBlocker

WebBlocker-30 — debug log level for WebBlocker

Reputation-Authority-35 — debug log level for Reputation Enabled Defense

VPN-31 — debug log level for all VPN components

IKE-32 — debug log level for the IPSec VPN tunnel key exchange component

SSLVPN-34 — debug log level for Mobile VPN with SSL

L2TP-38 — debug log level for Mobile VPN with L2TP

GRE-42 — debug log level for the GRE tunnel

level must be one of these options: **Off**, **Low**, **Medium**, or **High**.

log-setting log-level (*type*) (*level*)

Control diagnostic log messages of the type and level specified.

type must be one of these options:

Access-Portal-52 — diagnostic log level for Access Portal

Authentication — diagnostic log level for authentication and access authorization

Daas-53 — diagnostic log level for the component that enables the Firebox to communicate with WatchGuard Cloud

FireCluster-2 — diagnostic log level for all FireCluster components

Cluster-Management-3 — diagnostic log level for cluster configuration and management tasks

Cluster-Event-Monitoring-4 — diagnostic log level for the process that monitors FireCluster resources

Cluster-Transport-5 — diagnostic log level for FireCluster member communication channels

Cluster-Operation-6 — diagnostic log level for cluster member roles and operations

Firewall-7 — diagnostic log level for all firewall activities, including packet filtering and default threat protection

FQDN-49 — diagnostic log level for the FQDN (fully-qualified domain name) component

Management-8 — diagnostic log level for device management

Mobile-Security-46 — diagnostic log level for Mobile Security

EPM-48 — diagnostic log level for the End-Point Manager component

Networking-9 — diagnostic log level for all networking components

DHCP-client-10 — diagnostic log level for the component that enables the Firebox to receive IP address assignments from a DHCP server

DHCP-server-11 — diagnostic log level for the component that enables the Firebox to assign IP address information to DHCP clients.

PPP-12 — diagnostic log level for PPP support component for PPPoE

PPPoE-13 — diagnostic log level for PPPoE

Dynamic-Routing-36 — diagnostic log level for dynamic routing

RADVD-37 — diagnostic log level for IPv6 router advertisements

GWC-39 — diagnostic log level for the Gateway Wireless Controller

Static Interface-40 — diagnostic log level for the component that specifies the static IP address for an interface

Link Monitor-41 — diagnostic log level for the Link Monitor

Network-Diagnostics-43 — diagnostic log level for the component that runs network diagnostics

DIM-47 — diagnostic log level for the Device Info Manager component

DHCP-Fingerprinting-49 — diagnostic log level for the DHCP Fingerprinting component

Network-Discovery-45 — diagnostic log level for the Network Discovery component

Proxy-14 — diagnostic log level for all proxy components

Connection-Framework-Manager-15 — diagnostic log level for the component that manages proxy policy connections

Session-Manager-16 — diagnostic log level for the component that converts network packet streams into TCP and UDP connections

DNS-17 — diagnostic log level for the DNS connection analysis component

FTP-18 — diagnostic log level for the FTP connection analysis component

H323-19 — diagnostic log level for the H.323 connection analysis component

HTTP-20 — diagnostic log level for the HTTP connection analysis component

HTTPS-21 —diagnostic log level for the HTTPS connection analysis component

POP3-22 — diagnostic log level for the POP3 connection analysis component

SMTP-23 — diagnostic log level for the SMTP connection analysis component

SIP-24 — diagnostic log level for the SIP connection analysis component

TCP-UDP-25 — diagnostic log level for the TCP-UDP connection analysis component

Security-Subscriptions-27 — diagnostic log level for all security subscription services

Gateway-Antivirus-28 — diagnostic log level for Gateway AntiVirus

spamBlocker-29 — diagnostic log level for SpamBlocker

WebBlocker-30 — diagnostic log level for WebBlocker

Reputation-Authority-35 — diagnostic log level for Reputation Enabled Defense

VPN-31 — diagnostic log level for all VPN components

IKE-32 — diagnostic log level for the IPSec VPN tunnel key exchange component

SSLVPN-34 — diagnostic log level for Mobile VPN with SSL

L2TP-38 — diagnostic log level for Mobile VPN with L2TP

GRE-42 — diagnostic log level for the GRE tunnel

level must be one of these options: **Off**, **Error**, **Warning**, **Information**, or **Debug**.

log-setting syslog-server (*number*) (*option*)

Configure the Firebox to send log messages to a remote syslog server or QRadar server. In Fireware v12.4 or higher you can configure up to three syslog servers.

number specifies the syslog server number. It must be **1**, **2**, or **3**.

For each syslog server, *option* must be one of these options:

syslog (*timestamp* | *serial-number*) **enable** — Specify the IP address for a remote syslog server. It must be in the format of A.B.C.D. To include the time stamp or Firebox serial number in the log messages, include the *timestamp* or *serial-number* options.

ibm-leef (*serial-number* | *header*) **enable** — Specify the IP address for a QRadar server. To include the Firebox serial number or message header details in the log messages, include the *serial-number* or *header* options.

enable (*address*) — *address* is the IP address of a remote syslog server.

default — Restore default syslog settings

serial-number enable — Include the Firebox serial number in syslog messages.

timestamp enable — Include timestamp in syslog messages.

facility (*type*) (*setting1*)— Select the syslog facility for each type of log message.

type must be one of these options: **alarm**, **traffic**, **event**, **diagnostic**, **performance**.

setting1 is the syslog facility. It must be one of these options: **none**, **auth**, **priv-auth**, **cron**, **daemon**, **ftp**, **kern**, **lpr**, **mail**, **news**, **syslog**, **user**, **uucp**, **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, or **local7**.

log-setting (*type*) **enable**

Enable the collection of a specified category of log messages.

type must be one of these options:

- **debug-level**
- **firebox-itself-logging**

- **ike-packet-trace**
- **internal-storage**
- **log-level**
- **performance-statistics**
- **security-service-statistics**
- **syslog-server**
- **watchguard-log-server**

Log message type options with additional settings are described in the related sections.

Use **no log-settings** (*type*) to disable the category of log messages.

log-setting internal-storage enable

Send log messages to Firebox internal storage.

log-settingwatchguard-log-serverenable (*ip-address* | *fqdn*) (*key*) **log-server** (*ip-address* | *fqdn*) (*key*)

Specify one or more sets of WatchGuard Log Servers to which the Firebox sends log messages. You can send log messages to an instance of WatchGuard Dimension and to WatchGuard WSM Log Servers.

watchguard-log-server*enable* is the option to enable the Firebox to send log messages to the first set of Dimension or WSM Log Servers.

ip-address is the list of IP addresses for the first set of Log Servers. The first IP address in the list is the Primary Log Server. Additional IP addresses in the list are the secondary Log Servers used for failover if the Primary server in this list is unavailable. You must specify at least one Log Server IP address.

fqdn is the fully qualified domain name addresses for the first set of Log Servers. The first address in the list is the Primary Log Server. Additional addresses in the list are the secondary Log Servers used for failover if the Primary server in this list is unavailable. You must specify at least one Log Server address. DNS must be enabled to use FQDN.

key is the encryption key used to send information between the Firebox and each Log Server.

log-server is the option to send log messages from the Firebox to a second set of Dimension or WSM Log Servers.

ip-address is the list of IP addresses for the second set of Log Servers. The first IP address in the list is the Primary Log Server. Additional IP addresses in the list are the secondary Log Servers used for failover if the Primary server in this list is unavailable.

fqdn is the list of fully qualified domain name addresses for the second set of Log Servers. The first address in the list is the Primary Log Server. Additional addresses in the list are the secondary Log Servers used for failover if the Primary server in this list is unavailable. DNS must be enabled to use FQDN.

key is the encryption key used to send information between the Firebox and each Log Server.

Example

```
log-setting log-level authentication debug

log-setting syslog-server 192.168.111.15 traffic ftp debug

log-setting ike-packet-trace enable
```

```
log-setting watchguard-log-server enable 10.0.1.50 s3cur!+y 10.0.1.20
se@ur!ty log-server 10.20.1.50 l0gg!ng 10.20.1.20 lo@@in@
```

logon-disclaimer

Description

Enable and configure the settings for the Logon Disclaimer dialog box that appears when users log in to the Firebox. You must configure the Logon Disclaimer settings before you can enable the feature.

Syntax

logon-disclaimer [**page-title** *page-title*] [**disclaimer** (**from** *url* | **input** *disclaimer*)] [**logo** *url*]

Specify the page title text, disclaimer message text, and logo for the Logon Disclaimer message and dialog box.

page-title — Specify the text of the page title for the Logon Disclaimer.
page-title — The text of the page title.

disclaimer — Specify the text of the disclaimer message included in the Logon Disclaimer. Select to upload a file with the disclaimer message text from a URL or manually input the disclaimer message text.
from *url* — Select to upload the disclaimer message text from a file on an FTP or TFTP server and specify the location of the file.

input *disclaimer* — Select to manually type the logon disclaimer message text and specify the message text.

logo — Upload a logo to use with the Logon Disclaimer from a URL.
url — Specify the URL where the logo file is located. The image file you select must be a JPG, GIF, or PNG file, no larger than 200 x 65 pixels.

Use **no logon-disclaimer logo enable** to disable the logo used in the Logon Disclaimer.

logon-disclaimer enable

Enable the Logon Disclaimer feature.

Use **no logon-disclaimer enable** to disable the Logon Disclaimer feature.

Example

```
logon-disclaimer page-title Important Information disclaimer input You must
read and accept the terms and conditions before you can log in. logo
ftp://example-co.com\network-server\images\logon-disclaimer_logo.jpg

logon-disclaimer enable
```

loopback

Description

Enable a loopback interface, which is a virtual interface assigned to the Firebox that is not associated with a specific physical interface. You can use the loopback interface for dynamic routing to multiple ISPs when your Firebox is configured with multi-WAN. The loopback interface name is automatically set to **WG-Loopback** and you cannot change it.

Syntax

loopback enable [*address*]

Enable the loopback interface. You can optionally set the IP address if it is not already configured.

address must be one of these options:

ip-address mask
ip-addr is an IP address, and must be in the format of A.B.C.D.
mask is an IP subnet mask, and must be in the format of A.B.C.D.

net is an IP address and subnet mask, and must be in the format of A.B.C.D/#, where # must be in the range of 0 to 32.

Use **no loopback enable** to disable the loopback interface.

loopback *address*

Set the primary IP address of the loopback interface.

address must be one of these options:

ip-address mask
ip-addr is an IP address, and must be in the format of A.B.C.D.
mask is an IP subnet mask, and must be in the format of A.B.C.D.

net is an IP address and subnet mask, and must be in the format of A.B.C.D/#, where # must be in the range of 0 to 32.

loopback description "*description*"

Add a description for the loopback interface.

description is the text description of the interface in the configuration. If it contains spaces, it must be enclosed in quotation marks.

loopback secondary

loopback secondary *address*

Add a secondary IP address to the loopback interface.

address must be one of these options:

ip-address mask
ip-addr is an IP address, and must be in the format of A.B.C.D.

mask is an IP subnet mask, and must be in the format of A.B.C.D.

net is an IP address and subnet mask, and must be in the format of A.B.C.D/#, where # must be in the range of 0 to 32.

You can specify more than one address, separated by spaces.

Example

```
loopback enable 203.0.113.86/24
loopback description "multiwan loopback interface"
loopback secondary 203.0.113.88/24
```

managed-client

Description

Configure the Firebox as a managed client. You can configure your Firebox to be managed by an instance of Dimension or by a WSM Management Server. The settings you specify for an instance of Dimension are different than those you specify for a WSM Management Server.

Syntax

managed-client dimension-command dimension-command-addresses [(*ident*) | (*ipaddr*)]

Specify the domain name or IP address of your instance of Dimension.

ident is the domain name.

ipaddr is the IP address.

managed-client dimension-command enable

Enable the Firebox as a managed client of your instance of Dimension.

No options available.

Use **no managed-client dimension-command** to disable the administration of the Firebox as a managed client of Dimension.

managed-client dimension-command port *(number)*

Specify the port to use to connect to your instance of Dimension.

number is the port number specified in your Dimension configuration.

managed-client management-server device-name (*name*)

Add the name used to identify the managed client on the Management Server and in reports.

name is a unique alphanumeric name that identifies the Firebox.

managed-client management-server enable

Enable the Firebox as a managed client.

No options available.

Use **no managed-client** to disable the administration of the Firebox as a managed client.

managed-client management-server certificate from (*location*)

Import a Management Server CA certificate.

location must be either a valid FTP or TFTP address or the string console.

managed-client management-server primary (*address*) (*password*)

Set the primary Management Server.

address is the IP address of the primary Management Server. It must be in the form of A.B.C.D.

password is the unencrypted client shared secret.

managed-client management-server secondary (*address*) (*password*)

Set one or more secondary WSM Management Servers.

address is the IP address of a secondary Management Server. It must be in the form of A.B.C.D.

password is the unencrypted client shared secret.

You can configure up to three secondary Management Servers.

managed-client management-server tunnel (*enable*) (*ssl-server*) (*username*)

Configure the settings for a Management Tunnel over SSL for this Firebox.

enable is the option to enable the Management Tunnel. To disable the Management Tunnel for the Firebox, use **no enable**.

ssl-server is the IP address of Management Server for the Management Tunnel over SSL. It must be in the form of A.B.C.D.

username is the device name of the Firebox to use for the Management Tunnel.

Example

```
managed-client certificate from tftp://myftpsite/files/upload/client.ca
managed-client enable
managed-client device-name FB001
managed-client primary 192.168.111.3 strongpass
managed-client secondary 192.168.140.4 strongpass 192.168.140.5 strongerpass
managed-client tunnel enable 192.168.111.3 FB001
```

mobile-security

Description

Configure settings for Mobile Security for connections from Android and iOS mobile devices.

Mobile Security requires a feature key on the Firebox.

Syntax

mobile-security enable

Enable the Mobile Security feature.

To see Mobile Security configuration settings, use **show mobile-security**.

mobile-security (**compliance-android**|**compliance-ios**)**keep-alive** (*interval*)

Configure the Mobile Security keep-alive interval for FireClient. This controls how often FireClient contacts the Firebox after the initial connection. The default is 30 seconds.

compliance-android — set the keep-alive interval for FireClient on Android devices.
compliance-ios — set the keep-alive interval for FireClient on iOS devices.
interval is the keep-alive interval, in seconds.

mobile-security compliance-android deny (*requirement*) **enable**

Configure Mobile Security compliance requirements for Android devices. When mobile devices use FireClient to connect, FireClient for Android downloads these settings and uses them to assess whether the mobile device is compliant.

requirement must be one of these options:

ad-risk-ware — Do not allow devices with adware or riskware applications installed

malware — Do not allow devices with malware applications installed

rooted — Do not allow devices that are rooted

unknown-source — Do not allow devices that allow application installation from unknown sources.

usb-debugging — Do not allow devices that have USB debugging enabled

These compliance requirements are all enabled by default.

mobile-security compliance-android os-version (*version*) (*version*)

Set allowed versions of Android OS. You can specify more than one version, separated by spaces.

version is the allowed Android OS version. It can be any number in the format *major.minor.subminor*. You can use * as a wildcard. For example you can specify 6.*, or 6.0.* as the OS version.

mobile-security compliance-android sdk-update (*interval*)

Configure how frequently FireClient for Android checks for updates to the Kaspersky SDK used for application scans.

interval is the frequency, in hours, that FireClient checks for updates to the Kaspersky SDK. It must be a value between 4 and 240.

mobile-security compliance-ios jailbroken enable

Configure Mobile security to deny connections from iOS devices that are jailbroken.

mobile-security compliance-ios os-version (*version*) (*version*)

Set the compliant versions of iOS. You can specify more than one version. The version must be in the format

version is the allowed iOS version. It must be a number in the format *major.minor.subminor*. You can use * as a wildcard. For example you can specify 9.*, or 9.2.* as the OS version.

mobile-security compliance-check-always

Set the mobile device compliance status to **Unknown** until the compliance check has been completed when a mobile device reconnects.

mobile-security compliance-grace-period (*grace-period*)

Keep the previous compliance status if the mobile client reconnects within the specified grace period.

grace-period is the length of the grace period, in seconds.

mobile-security device-authorization-agreement enable (*source*)

Add or change the Device Authorization Agreement that users must accept in the FireClient app before FireClient can connect to the Firebox. The maximum length of the agreement is 65535 characters.

source is the location of the text to use in the agreement. It must be either a valid FTP or TFTP address or **console**.

If you specify console as the source, you can past or type the text into the CLI. Press **Control-D** to add the text, or **Control-C** to cancel.

mobile-security enforcement (**interface** *interface-alias*

Enable Mobile Security enforcement for connections to the specified interfaces. By default, Mobile Security is enabled for the aliases Any-Trusted and Any-Optional.

interface-alias must be the name (alias) of an enabled trusted, optional, or custom interface, or an alias that contains trusted, optional or custom interfaces.

mobile-security enforcement (**exception** *address*)

Add a Mobile Security exception. Mobile Security is not enforced on traffic from mobile devices to addresses on the exceptions list.

address must be one of these options: **host***ip*, **range***startipendip* , **subnet** *net*, or **FQDN***fqdn-site*.

ip, *startip*, and *endip* must be an IPv4 address in the format of A.B.C.D or an IPv6 address in the format A:B:C:D:E:F:G:H.

net must be an IPv4 subnet in the format of A.B.C.D/# where # must be in the range of 0 to 32 or an IPv6 subnet in the format A:B:C:D:E:F:G:H/I.

fqdn-site is a Fully Qualified Domain Name. This includes wildcard domains. For example, *host.example.com*, or *"*.example.com"*.

mobile-security protection-android (*protection-type*) **enable**

Configure whether FireClient monitors installation of applications and files on an Android device after the initial compliance scan.

protection-type must be one of these options:

app-install Monitor installation of new applications

folder-monitor Monitor installation of new APK (Android application package) files.

mobile-security vpn-compliance-enforcement enable

Enable Mobile Security enforcement for Android and iOS devices that use a VPN client to connect to the network.

Example

```
mobile-security enable

mobile-security compliance-ios os-version 9.0 9.1

mobile-security enforcement interface WG-Wireless-Access-Point1
```

modem

Description

Configure modem settings. In Fireware v12.1 and higher, modems are configured as external interfaces with modem failover enabled. In Fireware v12.1 to v12.2.1, link monitor settings appear in the multi-WAN configuration.

In Fireware v12.0.2 and lower, modems can be configured for failover but do not appear as external interfaces in the Firebox configuration. Link monitor settings appear in the modem configuration.

For a list of which Firebox models support modem failover, and the list of supported modems, see the *Fireware Help*.

Syntax

modem [*param*] **enable**

Enable a modem parameter (*param*). Where *param* is one of these options:

<null> — Enable modem for dial-up failover when all external interfaces are down.

3g4gmodem — Enable 3G/4G modem support.

builtin — Enable support for Firebox models with a built-in 4G LTE modem or the 4G LTE interface module.

manually-dns — Manually configure the DNS IP address.

debug-trace — Enables the modem and Point-to-Point Protocol (PPP) debug trace.

Use **no modem** *param* **enable** to disable the above modem commands options.

Use **no modem enable** to disable the modem.

modem telephone (*tel-no*) (*name*) (*domain-name*) (*passwd*) (*dns1*) (*dns2*)

Configure the dial-up account settings for modem failover. The *name*, *domain-name*, and *passwd* settings are not required for all 3G/4G modems.

tel-no is the telephone number.

For a serial modem, this is the remote access dial-in phone number of the Internet Service Provider.

For a 3G/4G modem, this is the access number specified by your wireless service provider.

name is the user name for PPP authent

domain-name is the domain name for PPP authentication.

passwd is the password.

dns1 is the primary DNS IP address.

dns2 is the secondary DNS IP address.

modem account-name (*name*) (*passwd*)

Configure or change the account name and password in the settings for modem failover.

name is the user name for PPP authentication.

passwd is the password.

modem account-domain (*domain-name*)

Configure or change the account domain in the account settings for modem failover.

domain-name is the domain name for PPP authentication.

modem alternate-telephone (*tel-no*)

Add an alternate phone number in the account settings for modem failover.

tel-no is the remote access dial-in alternate phone number of the Internet Service Provider.

modem apn (*ap-name*)

Configure an Access Point Name (APN), if required for connections to your wireless service provider. This applies to both 3G/4G modems and the 4G LTE modem.

ap-name is the Access Point Name.

modem (*param*) (*value*)

Configure modem options in the account settings for modem failover.

param is one of these options:

dial-timeout (*value*) — set the dial-up timeout of the PPP negotiation if the modem does not connect.

value is time in seconds from 60 to 300; default is 120.

redial-attempts (*value*) — set the number of dial-up attempts before it gives up the PPP negotiation.

value is the number of redials from 0 to 5 default is 3.

inactive-timeout (*value*) — set the inactive session timeout of the PPP connection.

value is time in minutes from 0 to 30; default is 0.

mtu (value) — set the Maximum Transmission Unit of the PPP connection.

value is in bytes is from 256 to 1500; default is 1500.

primary-dns (*value*) — specifies the primary DNS in the DNS settings.

value is the IP address of the primary DNS.

secondary-dns (*value*) — specifies the secondary DNS in the DNS settings.

value is the IP address of the secondary DNS.

volume (*value*) specifies the loudness of the modem's volume.

value must be one of these options: **Off**, **Low**, **Medium**, or **High**.

modem pppd-option (*option*) ...

Configure ppp options.

option is a ppp option that is required to make a connection. To specify more than one ppp option, separate the options with a comma and use double quotes around the list of options.

modem link-monitor (*ext-if*) (*lm-param*)

(Fireware v12.0.2 and lower) Define the Link Monitor configuration for devices that use a modem for failover.

In Fireware v12.1 to v12.2.1, Link Monitor settings appear in the multi-WAN configuration.

ext-if is the interface number of the External Interface that is monitored to trigger a failover.

lm-param is the Link Monitor parameter. *lm-param* must be one of these options:

ping (*host*) — Enable Ping to probe the remote side of the external link. *host* is the remote host to ping. This can be an IP address or a host name. Use **no modem link-monitor ext-if ping enable** to disable ping probes.

tcp(*host*) [*port*] — Enable TCP to probe the remote side of the external link. *host* is host port where: host is the remote host to negotiate TCP session. This can be an IP address or a host name. *port* is the port number to use for TCP negotiation, which is port 80 by default. If you do not specify a port number, the default value is used. Use **no modem link-monitor ext-if tcp enable** to disable TCP probes.

both enable — A conditional state, which if enabled, requires the link monitor to satisfy both the ping and a TCP probe before the external interface is marked as active again. Use **no modem link-monitor ext-if both enable** to require either ping or TCP probe only.

probe-interval [*sec*] — The time space between each link monitoring probe. *sec* is the time in seconds from 1 to 1200 and is 15 seconds by default.

deactivate-count [*number*] — The number of consecutive link monitoring failures before it deactivates the external interface. *number* is the number of probes from 1 to 10 and is 3 by default.

reactivate-count [*number*] - The number of consecutive link monitoring successes before it reactivates the external interface. *number* is the number of probes from 1 to 10 ; default is 3.

Example

```
modem enable

modem 3g4gmodem enable

modem account-name user1 domain.com mypa55w0rd 202.50.129.53 202.50.130.53

modem telephone 2061234 user1 example.com mypa55w0rd 202.50.129.53
202.50.129.54

modem alternate-telephone 2064321

modem dial-timeout 90

modem primary-dns 202.50.129.53

modem option receive-all

modem link-monitor 0 ping 196.24.1.1

modem pppd-option receive-all
```

multi-wan

Description

Configure the external interfaces to use multi-WAN features.

In Fireware v12.3 or higher, link monitor commands are separate from multi-WAN commands.

Syntax

multi-wan failback-option (**gradual**|**immediate**)

Set the action to take when the original address becomes available again.

The action must be **gradual** or **immediate**.

multi-wan load-balance failover (*interface1*) [*interface2*] ...

Set the failover sequence for interfaces in a multi-WAN failover configuration.

interface1 is the name of the first interface to which traffic fails over.

interface2 is the name of the second interface to which traffic fails over.

You can enter as many interface names as you have interfaces configured for multi-WAN failover. There must be a minimum of two.

multi-wan load-balance interface-overflow (*interface1 threshhold1*) (*interface2 threshhold2*) ...

Set the load balance overflow sequence in a multi-WAN interface overflow configuration.

interface1 is the name of the first interface to which traffic is distributed.

threshhold1 is the threshold value in 100 Kbps increments. It must be an integer from 0 to 10000.

interface2 is the name of the second interface to which traffic is distributed.

threshhold2 is the threshold value in 100 Kbps increments. It must be an integer from 0 to 10000.

You can enter as many interface names as you have interfaces configured for multi-WAN interface overflow. There must be a minimum of two.

multi-wan load-balance round-robin (*interface1 weight1*) (*interface2 weight2*) ...

Set the round-robin sequence in a multi-WAN round-robin configuration.

interface1 is the name of the first interface to which traffic is distributed.

weight1 is the round-robin weight. It must be an integer from 0 to 65535.

interface2 is the identifying name of the second interface to which traffic is distributed.

weight2 is the round-robin weight. It must be an integer from 0 to 65535.

You can enter as many interface names as you have interfaces configured for multi-WAN round-robin. There must be a minimum of two.

multi-wan load-balance routing-table (*interface1*) (*interface2*) ...

Set the interface sequence in a multi-WAN routing table configuration.

interface1 is the name of the first interface to which traffic is distributed.

interface2 is the name of the second interface to which traffic is distributed.

You can enter as many interface names as you have interfaces configured for multi-WAN routing table. There must be a minimum of two.

no **multi-wan link-monitor** (*interface*) **enable**

(Fireware v12.2.1 or lower) Use **multi-wan link-monitor** *(interface)* **enable** to enable link monitor for an interface. By default, link monitor is enabled for all interfaces configured for multi-WAN except modem interfaces.

In Fireware v12.3 or higher, link monitor settings are separate from the multi-WAN configuration.

Use **no multi-wan link-monitor** *(interface)* **enable** to disable link monitor for an interface.

no **multi-wan link-monitor** (*interface*) **enable ping** *(IP address or domain name)*

(Fireware v12.2.1 or lower) Enable a ping link monitor for an interface.

Use **no multi-wan link-monitor** *(interface)***ping** to disable ping link monitoring for an interface.

no **multi-wan link-monitor** (*interface*) **enable tcp** *(IP address or domain name)*

(Fireware v12.2.1 or lower) Enable a TCP link monitor for an interface.

Use **no multi-wan link-monitor** *(interface)***tcp** to disable tcp link monitoring for an interface.

no **multi-wan link-monitor** (*interface*) **interval** (*frequency*)

(Fireware v12.2.1 or lower) *interface* is the number of the external interface. It must be an integer from 0 to 7.

no **multi-wan link-monitor** (*interface*) [**deactivate-count** *dcount*]

(Fireware v12.2.1 or lower) *dcount* is the number of failures that must occur for the Firebox to deactivate the interface. The default value is 3.

no **multi-wan link-monitor** (*interface*) [**reactivate-count** *rcount*]

(Fireware v12.2.1 or lower) *rcount* is the number of successes that must occur for the Firebox to reactivate the interface. The default value is 3.

no **multi-wan link-monitor** (*interface*) [**operation** *operation*]

(Fireware v12.2.1 or lower) Set the method to use to check the status of an interface configured for multi-WAN.

operation sets whether the probe uses both TCP and PING to check the status, or only one. It must be either: AND or OR. The default value is OR.

no **multi-wan link-monitor** (*interface*) (**ping** *icmptarget*)

(Fireware v12.2.1 or lower) Set the method to use to check the status of an interface configured for multi-WAN.

icmptarget is the destination host that the Firebox can ping to check the status. It must be either a domain name or an IP address in the format A.B.C.D.

multi-wan link-monitor (*interface*) (**tcp** *tcpaddress*)

(Fireware v12.2.1 or lower) Set the method to use to check the status of an interface configured for multi-WAN.

tcpaddress is the IP address and port of a destination host, that the Firebox can use to negotiate a TCP handshake to check status. It must be an address in the format A.B.C.D #, where # is an integer from 1 to 65535.

multi-wan (**tcp-sticky-timer**|**udp-sticky-timer**|**others-sticky-timer**) (*interface*)

Configure the global sticky connection duration for TCP connections, UDP connections, and connections that use other protocols. You can set sticky connection parameters only with the round-robin or interface-overflow multi-WAN methods.

Specify one of these options: **tcp-sticky-timer**, **udp-sticky-time**, **others-sticky-timer**

interface is the interface number. It must be an integer from 0 to the maximum interface value on the Firebox.

Example

```
multi-wan tcp-sticky-timer 0

multi-wan load-balance failover sequence 0 2 5 6

multi-wan load-balance round-robin weights 0 10

multi-wan 2 interval 30 deactivate-count 5 reactivate-count 2 operation and
icmp 192.168.32.2 tcp 192.168.33.2 28
```

netflow

Enable the Firebox as a NetFlow exporter. NetFlow is a protocol that is used to collect and analyze IP network traffic.

netflow enable

Enable NetFlow on your Firebox.

netflow version *(version)*

Specify which version number of the NetFlow protocol to use.

version must be **v5** or **v9**. To monitor IPv6 traffic, you must use V9.

netflow collector *(IP address) (port)*

Specify the IP address and port of the collector. A collector is a remote server that analyzes flow data from the Firebox. The Firebox must be able to communicate with the collector at the specified IP address and port with the UDP protocol.

IP address is the IPv4 or IPv6 address of a NetFlow collector.

Port is the port number configured on the collector.

netflow firebox-traffic hostin

(Fireware v12.5 or higher) Monitor traffic destined for the Firebox itself.

netflow firebox-traffic hostout

(Fireware v12.5 or higher) Monitor Firebox-generated (self-generated) traffic, which is traffic generated by the Firebox itself.

In Fireware v12.4.1 or lower, use **netflow interface Firebox**.

netflow timeout *(number)*

Specify an Active Flow Timeout value. The Active Flow Timeout is the amount of time an active connection should wait before it terminates. In the Firebox NetFlow configuration, we recommend that you specify an Active Flow Timeout value that is lower than the Active Flow Timeout value on the collector.

number must be between 0 and 60 minutes.

netflow sampling-rate *(rate)*

Enable Sampling mode and specify a sampling rate. In Sampling mode, the Firebox randomly selects 1 out of every n packets to sample. For example, if you specify a Sampling mode of 100, the Firebox samples 1 out of every 100 packets.

rate must be a value between 2 and 65535 packets.

To disable Sampling mode, use **no netflow sampling-rate**

netflow interface *(interface name)*

Specify the name of an interface you want to monitor with NetFlow. You can specify any interface configured on the Firebox. You can specify more than one interface.

In Fireware v12.5 or higher:

Use **ingress** to monitor inbound traffic on an interface.

Use **egress** to monitor outbound traffic on an interface.

In Fireware v12.4.1 or lower, to monitor Firebox-generated (self-generated) traffic, use **netflow interface Firebox**. In Fireware v12.5 or higher, use **netflow firebox-traffic**.

Example

```
netflow collector 203.0.113.40 2055
netflow version v9
netflow interface External
netflow interface "External 2"
netflow Firebox-traffic hostout
```

network-mode

Description

Set the network mode.

If you use bridge mode, your Firebox cannot complete some functions that require it to operate as a gateway. These functions include: multi-WAN, VLANs, network bridges, static routes, FireCluster, secondary networks, DHCP server or DHCP relay, serial modem failover, NAT, dynamic routing, any type of VPN for which the Firebox is an endpoint or gateway, and some proxy functions, including HTTP Web Cache Server.

Syntax

network-mode (*option*)

Set the network mode to Routed, Drop-in or Bridge mode.

option must be one of these options:

routed

drop-in (*address*) (*gateway*)

bridge (*address*) (*gateway*) [*vlan-tag-for-mgmt*] [**aging**]

address is the IP address used as the primary address for all interfaces on the Firebox. It is either an address with netmask in the format of A.B.C.D A.B.C.D. or a network in the format of A.B.C.D/#, where # is the netmask in the range of 8 to 30.

gateway is the IP address of default gateway. It must be in the form A.B.C.D.

vlan-tag-for-mgmt is the optional VLAN tag to allow for management connections to the Firebox from a VLAN.

aging is a timer for Spanning Tree Protocol that specifies the aging time of the MAC address table. The default value is 300 seconds. You can specify a value between 0 and 2147483647.

network-mode auto-host-mapping (*if-number* (**enable**|**disable**))

Specify the interface for automatic host mapping.

if-number is the interface index number.

For each interface, you must specify one of these options: **enable** or **disable**.

You can specify more than one interface with their respective settings.

network-mode bridge dhcp (*int*) (*ipaddr*) [**any**] [**force-renew**] [**host-id**] [**host-name**] [**management-address**] [**release**] [**renew**]

Configure a Firebox to get a system IP address from a DHCP server. You must specify a management IP address for management connections to the Firebox.

int is the amount of time in hours before the DHCP lease expires.

Use *any* to automatically get an IP address from the DHCP server.

Use *ipaddr* to manually specify an IP address.

force-renew specifies that the DHCP server sends requests to the DHCP client to renew the IP address.

host-id is a host ID that you specify.

host-name is a host name that you specify.

management-address is the IP address you specify for management connections to the Firebox.

Use *release* to release the IP address lease on the DHCP server.

Use *renew* to renew the IP address lease on the DHCP server.

network-mode bridge v6 ip

(Fireware v12.8 or higher) In Bridge mode, specify a static IPv6 system address and other IPv6 settings.

address*(IPv6 address)*is the IPv6 address and netmask.

To remove the address, use **no network-mode bridge v6 ip address enable**.

autoconf Stateless address auto configuration. If you specify this command, the Firebox automatically assigns an IPv6 link-local address to this interface. When you enable IP address autoconfiguration, the external interface is automatically enabled to receive IPv6 router advertisements, and you do not have to specify a default gateway.

dad-transmit *(number of transmits)*is the number of DAD (Duplication Address Detection) transmits. The default value is 1.

default-gw*(gateway address)* is the IPv6 default gateway address. You do not have to specify a default gateway if you specified **autoconf**.

dhcp enable Enable a DHCPv6 client on this interface to request an IP address from a DHCPv6 server. To get IPv6 addresses, the DHCPv6 client can use a rapid two-message exchange (solicit, reply) or a four-message exchange (solicit, advertise, request, reply). By default, the DHCPv6 client uses the four-message exchange. To use the two-message exchange, enable **dhcp6-client-rapid-commit**on this interface and on the DHCPv6 server.

hop-limit*(limit)* is the number of network segments a packet can travel over before it is discarded by a router. The default value is 64.

network-mode bridge spanning-tree

Enable and configure Spanning Tree Protocol for a Firebox in Bridge mode.

Use *enable*) to enable Spanning Tree Protocol on the Firebox.

(*bridgeprio*) is the bridge priority. To make sure that the Firebox is always selected as the root bridge, specify a bridge priority number that is lower than all other bridges on your network. The default value is 32768. You can specify a value between 0 and 65535, in increments of 4096.

port)

port number is the number of the Firebox port.

pathcost is the path cost. The default value is 0. You can specify a value between 0 and 65535.

portpri is the port priority. In an election, if all ports have the same path cost and Bridge ID, the port with the lowest port priority becomes the root port. The default value is 128. You can specify a value between 1 and 254, in increments of 16.

Timers:

[*fd*] is the forward delay timer. It specifies how long the Firebox ports remain in the Listening and Learning states. The default value is 15 seconds. You can specify a value between 4 and 30 seconds.

(*hello*) specifies how often a root bridge generates a BPDU. You can configure this value only for a Firebox that is the root bridge. The default is 2 seconds. You can specify a value between 1 and 10 seconds.

(*maxage*) specifies how often a bridge port saves its configuration BPDU information. The default is 20 seconds. You can specify a value between 6 and 40 seconds.

network-mode dhcp relay (*serverip*) [*serverip*] [*serverip]*

Configure a Firebox to relay DHCP requests to up to three DHCP servers. This command applies only to a Firebox configured in drop-in mode.

serverip is the IP address of a DHCP server that is used for computers on the trusted, optional and custom interfaces. You can specify the IP addresses up to three DHCP servers. The Firebox sends DHCP requests to the IP addresses of all DHCP servers you specify.

Use **no dhcp enable** to disable DHCP relay.

network-mode dhcp server (**start-addr** *startip endip*) (*leasetime*) (**dns-server** *dns*...) (**domain** *domainname*) [**reservation** *resvname macaddress ipaddress*] [**wins** *wins*...]

Configure as a DHCP server for computers connected to the Firebox. This command applies only to a Firebox configured in drop-in mode.

start-addr defines a DHCP address pool. In the same line, you can use the start-addr command multiple times with these parameters:

startip is the first IP address in the DHCP address pool.

endip is the last IP address in the DHCP address pool.

leasetime is the duration in hours that addresses are leased to devices on the network. The value must be an integer.

dns is the IP address of one or more valid DNS servers.

domainname is the domain name used by devices on the network.

reservation defines a pair of MAC address and IP address that are reserved within the DHCP address pool. In the same line, you can use the reservation command multiple times with these parameters:

resvname is a string to identify a reserved address.
macaddress is the MAC address of the Firebox with a reserved address.
ipaddress is the IP address assigned to the reserved address.

wins is the IP address of one or more valid WINS servers.

Use **no dhcp enable** to disable DHCP server.

network-mode related-host (*ip-address*) (*if-number*)

ip-address is the IP address that is related to the interface.

if-number is the interface index that is related to the IP address.

Example

```
network-mode routed

network-mode drop-in 200.100.100.0/24 200.200.200.3

network-mode auto-host-mapping 3 enable 4

network-mode bridge spanning-tree bridgeprio 0
```

network-scan

Description

Enable and configure network scanning for the Network Discovery feature.

Syntax

network-scan interface *(interface name)* **schedule**

interface — The name of the network interface to scan.

schedule — Enable and configure a network scan schedule.

enable — Enable a schedule for a network scan.
daily — Configure a daily scan schedule.
date — Configure a scan schedule for a specific date.
monthly — Configure a monthly scan schedule.
weekly — Configure a weekly scan schedule.

ntp

Description

Configure the Firebox to get timestamps from an NTP server, and enable the Firebox as an NTP server.

Syntax

ntpenable

Enable the Firebox to use an external NTP server to synchronize the system time.

No options available.

Use **no ntp enable** to disable use of an NTP server.

ntp server ip (*ip-address*)

Add the IP address of the NTP server the Firebox uses to synchronize the system time.

address is the IP address of an NTP server in the format A.B.C.D.

Use no **ntp server ip** (*address*) to remove an NTP server from the configuration.

ntp server domain (*hostname*)

Add an NTP server with a domain name.

hostname is the hostname (FQDN) of an NTP server.

Use **no ntp server domain** (*hostname*) to remove an NTP server from the configuration.

ntpdevice-as-server enable

Enable the Firebox as an NTP server. Before you enable this option, you must use the **ntp enable** command to enable the Firebox to use an NTP server.

When you enable your Firebox as an NTP server, the **NTP Server** policy is automatically created to allow NTP traffic from clients on your trusted and optional networks to the NTP server on the Firebox.

Use **no ntp sevice-as-server enable** to disable the NTP server on the Firebox.

Example

```
ntp server ip 200.220.100.12
ntp server domain ntp.foo.org
ntp device-as-server enable
no ntp server ip 203.201.39.1
```

policy

Description

Enter the Policy command mode. In policy mode, the command prompt changes to "WG (config/policy)#".

For information about policy mode commands, see *Policy Commands*.

Use the **Exit** command to exit this mode.

Syntax

policy

No options available.

Example

```
interface policy
WG(config/policy)#
```

pppoe

Description

Create or edit a secondary PPPoE interface. This command starts pppoe interface configuration mode to enable commands to configure the specified secondary PPPoE interface. After you use the pppoe command, the configuration continues to the pppoe secondary commands.

In pppoe command mode, the command prompt changes to "WG(config/pppoe-<name>)#" where <name> is the name of the secondary PPPoE interface.

Use the **Exit** command to exit this mode.

Syntax

pppoe (*name*)

Create or edit a secondary PPPoE interface on this Firebox.

name is the name of the secondary PPPoE interface.

associated-interface (*ext-interface-name*) (*username*) (*password*)

Associate the secondary PPPoE interface with an external interface that is configured to use PPPoE, and specify the PPPoE credentials for the secondary interface.

ext-interface-name is the name of the external interface to associate the secondary PPPoE interface with. It must the name of an external interface that is configured to use PPPoE.

username is the user name to use for PPPoE authentication for this secondary interface. It must be a string between 1 and 47 characters in length.

password is the password to use for PPPoE authentication for this secondary interface. It must be a string between 1 and 32 characters in length.

After you associate the secondary PPPoE interface to an external interface, other commands in this mode become available.

auth (*reauth*) (**ac-name** *acname*) (**auth-timeout** *timeout*) (**service-name** *serv*)

Configure PPPoE authentication settings.

reauth is the allowed number of authentication retries from 0 to 20.

acname is the Access Concentrator Name.

timeout is the number of seconds between each connection attempt from 0 to 60.

serv is the PPPoE Service Name.

Use **no auth** with any of the previous parameters to disable the setting.

auto-reboot enable (*day*) (*hour*) (*minute*)

Configure a scheduled automatic restart of the PPPoE session.

day is the day of the week to restart. It must be one of these options:

0 — Sunday
1 — Monday
2 — Tuesday
3 — Wednesday
4 — Thursday
5 — Friday
6 — Saturday
7 — Daily

hour is the hour of the day to restart. It must be an integer from 0 to 23.
minute is the minute of the hour to restart. It must be an integer from 0 to 59.

Use **no auto-reboot enable** to disable automatic restart.

connection (*type*) (*time*)

Configure PPPoE connection settings.

type must be either: **always-on** or **dial-on-demand**.

time must be one of these settings:

if *type* is **always-on**, *time* is the auto-reconnect time in seconds from 0 to 3600.
if *type* is **dial-on-demand**, *time* is the inactivity timeout in minutes from 0 to 60.

host-uniq enable

Enable the host-uniq tag in PPPoE discovery packets.

Use **no pppoe host-uniq enable** to disable the host-uniq tag.

lcp-echo enable (*retries*) (**lcp-timeout** *lcptimeout*)

Configure the use of LCP echo requests to detect lost PPPoE connections.

retries is the number of LCP retries in seconds from 1 to 60.

lcptimeout is the LCP echo timeout in seconds from 1 to 1200.

Use **no lcp-echo enable** to disable LCP echo requests.

mtu (*size*)

Set the Maximum Transmission Unit value for the secondary PPPoE interface.

size is the size in bytes of the maximum transmission unit. Must be an integer from 68 to 9000.

static-ip (*ipaddress*) [**send-ipenable**]

Configure a static IP address.

ipaddress is a static IP address used for PPPoE.

send-ip enable — enables the Firebox to send the static IP address to the PPPoE server during PPPoE negotiation. This is enabled by default when you configure a static IP address.

Use **no static-ip** to remove the static IP address and get an IP address automatically.

Use **no static-ip send-ip enable** if you do not want the Firebox to send the static IP address to the PPPoE server during PPPoE negotiation.

use-peer-dns enable

Enable the Firebox to negotiate DNS with the PPPoE server.

Use **no use-peer-dns enable** if you do not want the Firebox to negotiate DNS with the PPPoE server.

user-info (*username*) (*password*)

Configure the user login information.

username is the PPPoE user name.

password is the PPPoE password.

Example

```
pppoe pppoe2
associated-interface External myuser mypasswd
static-ip 100.100.100.10
connection always-on 30
auth 3 ac-name concentrator1 auth-timeout 10
```

```
auth service-name serviceA
connection dial-on-demand 60
auto-reboot enable day 3
lcp-echo enable 3 lcp-timeout 30
user-info myuser mypasswd
```

quota-action

Description

Configure bandwidth and time quota actions.

Syntax

quota-action (*name*) (*bandwidth*) (*time)*

Create a quota action.

name — Name of the quota action.

bandwidth — Bandwidth limit for this quota action in MB.

time — Time limit for this quota action in minutes.

Use **no quota-action [name]** to delete a quota action.

Example

```
quota-action action1 10000 60
```

quota-exception

Description

Configure bandwidth and time quota exceptions.

Syntax

quota-exception (***fqdn***|***host***|***range***|***subnet***) (*address)*

Define a quota exception.

fqdn — FQDN (Fully Qualified Domain Name). This includes wildcard domains. For example, *host.example.com*, or *"*.example.com"*.

host — A single IP address. It must be in the format A.B.C.D.

range — A range of IP addresses. The start and end range address must be in the format A.B.C.D.

subnet — A network subnet in slash network notation. It must be in the format A.B.C.D./#, where # is a number from 0 to 32.

Example

```
quota-exception fqdn "*.example.com"
quota-exception host 10.10.10.1
```

quota-rule

Description

Configure bandwidth and time quota rules.

Syntax

quota-rule (*name*) **enable**

Enable the quota rule.

name is the name of the quota rule.

Use **no quota-rule [name]** to delete the quota rule.

Use **no quota-rule [name] enable** to disable the quota rule.

quota-rule (*name*) **description** (*description)*

Provide a description for the quota rule.

name is the name of the quota rule.

description is the description of the quota rule.

quota-rule (*name*) **quota-action** (*name*)

The name of the corresponding quota action.

name is the name of the quota rule.

quota-action is the quota action to apply to this quota rule.

name is the name of the quota action to apply to this quota rule.

quota-rule (*name*) **user-group** (*user|group*) *auth server*

The user or group to which the rule applies.

name is the name of the quota rule.

user-group assigns a user or group to this quota rule.

user is the name of the user for this quota rule.

group is the name of the group for this quota rule.

auth server is the authentication server for the user or group (such as *Firebox-DB*). Use *any* for any domain.

Example

```
quota-rule rule1 enable
quota-rule rule1 quota-action action1
quota-rule rule1 user-group user user1 any
```

sd-wan

Description

(Fireware v12.3 or higher) Add or edit an SD-WAN action.

(Fireware v12.4 or higher) Add internal (Trusted, Optional, or Custom) interfaces to an SD-WAN action, add more than one BOVPN virtual interface to an SD-WAN action, and select metrics for BOVPN virtual interfaces.

Syntax

[no] **sd-wan***(SD-WAN action name)* **interface** (interface name) (interface name)

Add a new SD-WAN action, or add or remove interfaces from an existing SD-WAN action.

To add a new SD-WAN action, you must specify one or more existing external interfaces or one existing BOVPN virtual interface. If you add a BOVPN virtual interface, you cannot add external interfaces. If the interface name includes a space, enclose the interface name in quotation marks.

To remove an interface from the SD-WAN action, use **no sd-wan** *(SD-WAN action name)* **interface** *(interface name)*

sd-wan*(SD-WAN action name)***description** *(description)*

Add an optional description of the SD-WAN action.

sd-wan*(SD-WAN action name)***failback**

You can specify one of these failback types:

gradual — Allow active connections to use the failover interface
immediate — Stop all active connections immediately
none — Use failover interface for new connections

sd-wan*(SD-WAN action name)* **jitter** (number)

Jitter is the variance in packet delivery delay measured in milliseconds (ms).

To use jitter metrics to determine when an interface fails over or fails back, specify a number between 1 and 1000 ms.

In Fireware v12.4 or higher, you can select to monitor jitter for BOVPN virtual interfaces.

sd-wan*(SD-WAN action name)***interface** (interface name)

To add an interface to the SD-WAN action, specify the name of an interface that is already configured on the Firebox. The interface name is case-sensitive.

In Fireware v12.4 or higher, you can specify internal (Trusted, Optional, or Custom) interfaces and you can add more than one BOVPN virtual interface.

sd-wan*(SD-WAN action name)***latency** (number)

Latency is the packet delivery delay measured in milliseconds (ms).

To use latency metrics to determine when an interface fails over or fails back, specify a number between 1 and 2000 ms.

In Fireware v12.4 or higher, you can select to monitor latency for BOVPN virtual interfaces.

sd-wan*(SD-WAN action name)***loss** (number)

Loss is the percentage of packets lost.

To use loss metrics to determine when an interface fails over or fails back, specify a number between 1 and 100 percent.

In Fireware v12.4 or higher, you can select to monitor loss for BOVPN virtual interfaces.

sd-wan*(SD-WAN action name)***manual-failback force**

If you configured gradual or no failback with the **failback** command, you can use the **manual failback** command later to manually fail back connections. These options are available:

force — Available if you used the **failback gradual** command. The **manual failbackforce**command terminates active connections and forces new connections to use the failback interface.

gradual — Available if you used the **failback none** command. The **manual failback gradual** command keeps active connections on the failover interface and forces new connections to use the failback interface.

immediate — Available if you used the **failback none** command. The **manual failback immediate** command terminates active connections and forces new connections to use the failback interface.

sd-wan*(SD-WAN action name)***mode**

(Fireware v12.8 or higher) For an existing SD-WAN action, specify one of these modes:

failover — Configure an SD-WAN action that uses the Failover method.

round-robin — (Fireware v12.8 or higher) Configure an SD-WAN action that uses the Round-Robin method.

By default, the weight for interfaces in a Round-Robin SD-WAN action is 1. For an interface that already exists in the SD-WAN Round-Robin action, you can specify an interface weight between 0 and 65535. Example: **sd-wan** (SD-WAN action name) **mode round-robin interface** (interface name) (weight)

sd-wan*(SD-WAN action name)***operation**

Specify one of these operation types:

and — Fail over if values for all selected measurements are exceeded.

or — Fail over if values for any selected measurements are exceeded.

Example

```
sd-wan SDWAN.action1 interface External-1
sd-wan SDWAN.action1 interface "External 2"
sd-wan SDWAN.action1 loss 6
sd-wan SDWAN.action1 latency 25
sd-wan SDWAN.action1 operation and
sd-wan SDWAN.action1 failback gradual
sd-wan SDWAN.action1 manual-failback force
sd-wan SDWAN.action1 mode round-robin
sd-wan SDWAN.action1 mode round-robin interface eth1 15
```

signature-update

Description

Configure signature updates for Gateway AntiVirus, IntelligentAV, IPS, Application Control, and Data Loss Prevention.

Syntax

signature-update http-proxy-server enable

Enable the Firebox to contact the signature update server using an HTTP proxy server.

Use **no signature-update proxy-server-enable** to disable the HTTP proxy server settings.

signature-update http-proxy-server address (*server-address*)

Configure the address of the HTTP proxy server to use to contact the signature update server.

server-address is the IP address or host name of the HTTP proxy server.

signature-update http-proxy-server port (*server-port*)

Configure the server port of the HTTP proxy server to use to contact the signature update server.

server-port is the IP address or host name of the HTTP proxy server. The default port is 8080.

signature-update http-proxy-server authentication (**basic-auth**|**no-auth**|**ntlm-auth**) (*username*) (*domain*) (*password*)

Configure the authentication credentials to use for connections to the http proxy server.

You can specify one of these authentication types:

basic-auth — The HTTP proxy server uses basic authentication

no-auth — The HTTP proxy server does not require authentication
ntlm-auth — The HTTP proxy server uses NTLM authentication

username is the user name used for authentication to the HTTP proxy server.

domain is the domain name used for authentication to the HTTP proxy server.

password is the password used for authentication to the HTTP proxy server.

If you specify **no-auth**, *username*, *domain*, and *password* are not required.

signature-update server-url (*https-url*)

Configure the secure URL of the update server.

https-url is the URL of the update server. It must be in the format: https://host/url-path.

The default URL for the update server is https://services.watchguard.com.

signature-update update (**DLP**|**GAV**|**IAV**|**IPS**|**TOR**)

Force an immediate update for the specified signature type.

The signature type must be one of these options:

DLP — Update the signatures for Data Loss Prevention
GAV — Update the signatures for Gateway AntiVirus
IAV — Update the signatures for IntelligentAV
IPS — Update the signatures for Intrusion Prevention and Application Control
TOR — Update the signatures for Tor Exit Node Blocking

signature-update signature-type (**DLP**|**GAV**|**IAV**|**IPS**|**TOR**) (**enable**|**disable**)

Enable or disable automatic signature updates for the specified signature type.

The signature type must be one of these options:

DLP — Update the signatures for Data Loss Prevention
GAV — Update the signatures for Gateway AntiVirus
IAV — Update the signatures for IntelligentAV
IPS — Update the signatures for Intrusion Prevention and Application Control
TOR — Update the signatures for Tor Exit Node Blocking

Example

```
signature-update update IPS

signature-update signature-type GAV enable

signature-update http-proxy-server enable

signature-update http-proxy-server address 100.100.100.50

signature-update http-proxy-server authentication basic-auth user1
example.com s3cret-pswd
```

snat

Description

Configure a static NAT or server load balancing SNAT action. Server load balancing requires Fireware with a Pro upgrade, and is not supported on XTM 2 Series, 3 Series, and Firebox T10 devices.

Syntax

snat (*snat-name*) **server-load-balancing** [**description** *description*] (*address-type ext-address*) (**round-robin**|**least-connection**) [**source-ip** *source-addr*] [**sticky-connection** *sticky-time sticky-unit*] (*int-address*) [**port** *port-num*] [**weight** *weight*] (*int-address*) [**port** *port-num*] [**weight** *weight*])

Configure a server load balancing SNAT action.

snat-name is the name of the SNAT action. The maximum length is 47 characters.

description is an optional description for this SNAT action.

address-type is the type of interface address. It must be one of these options:

external-addr —Specify the external address as the alias name of an external or optional interface.

external-IP — Specify the external address as the IP address of an external or optional interface. In Fireware v12.2.1 or higher, you specify the IP address of a loopback interface.

ext-address is the alias name or IP address of the external or optional interface.

If *external-address-type* is **external-addr**, ext-address must be the alias of an external or optional interface. If *external-address-type* is **external-IP**, *ext-address* must be the IP address of an external or optional interface. It must be in the format A.B.C.D.

You must specify the load balancing method to use. It must be one of these options:

round-robin — distribute incoming sessions among the servers in round-robin order.

least-connection — send each new session to the server that has the lowest number of open connections.

source-ip — set a source IP address. If you set a source IP address, the Firebox changes the source IP address of traffic handled by policies that use this server load balancing action. The same source IP address is used for all servers in the server load balancing action.

source-addr — The source IP address to use. It must be in the format A.B.C.D.

sticky-connection — change these connection settings:

sticky-time — The amount of time (in seconds) that a connection continues to use the same internal server. The default sticky connection time is 28800 seconds (8 hours). If sticky-time is set to 0, sticky connections are disabled.

sticky-unit — The unit of time to use for the sticky connection time. It must be one of these options: hours, minutes, or seconds.

int-address is the IP address of an internal server. You must specify a minimum of two internal server IP addresses in a server load balancing SNAT action.

For each internal server, you can optionally specify these parameters in this order:

port — the internal port to use. This setting enables port address translation (PAT).

weight —the weight to use for server load balancing. The default is 1.

snat (*snat-name*) **static-nat** (*description*) (*external-address-type ext-address*) (*int-address* [**port** *port-num*] [**source-ip** *source-addr*])

Configure a static NAT action.

snat-name is the name of the static NAT action. The maximum length is 47 characters.

description is an optional description for this static NAT action.

external-address-type is the type of external interface address. It must be one of these options:

external-addr — Specify the external address as the alias name of an external or optional interface.

external-ip — Specify the external address as the IP address of an external or optional interface. In Fireware v12.2.1 or higher, you specify the IP address of a loopback interface.

ext-address is the alias name or IP address of the external or optional interface.

If *external-address-type* is **external-addr**, ext-address must be the alias of an external or optional interface. If *external-address-type* is **external-IP**, *ext-address* must be the IP address of an external or optional interface. It must be in the format A.B.C.D.

int-address is the IP address of an internal server.

port — For each internal address, you can optionally specify the port.

port-num — the internal port to use. This setting enables port address translation (PAT).

source-ip — For each internal IP Address, you can optionally specify a source IP address.

source-addr — the source IP address to use. It must be in the format A.B.C.D.

You can configure multiple static NAT mappings for the same SNAT action

Example

```
snat snat-slb server-load-balancing external-addr External round-robin
10.0.100.10 weight 2 10.0.100.11 weight 1

snat snat2 description corp-webserver server-load-balancing external-ip
100.100.100.50 round-robin 10.0.50.10 10.0.50.11 10.0.50.12

snat snat7 static-nat external-addr External 10.0.100.20

snat snat8 static-nat external-ip 50.50.50.10 10.10.10.50 port 8080
```

snmp

Description

Configure the Firebox to integrate with SNMP tools.

Syntax

snmp alg-nat

Use NAT for connections through the SNMP application layer gateway.

snmp server (*address*) ...

Configure SNMP management computers.

address is an IP address in the format A.B.C.D.

You can configure up to three SNMP management computers.

Use **no snmp server** (*address*) to remove an SNMP management computer from the configuration.

snmp version v1_2 community (*string*)

Configure the Firebox to use SNMP version 1 or 2 polling.

string is the value of the community string.

snmp version v3 (*username*) (**md5** (*authpassword*)|**sha1** (*authpassword*) |**none**) (**des** (despassword)|**none**)

Configure the Firebox to use SNMP version 3 polling.

username is a string for the SNMP user name.

You can set the authentication protocol to **md5**, **sha1**, or **none**.

authpassword is the user password on the SNMP management computer for MD5 or SHA1 authentication.

You can set the privacy protocol to **des** or **none**.

despassword is the password used to encrypt DES on the SNMP management computer.

snmp trap enable (*type*)

Enable SNMP traps for the Firebox.

type must be one of these options: **trap v1**, **trap v2c**, **trap v3**, **inform v2**, or **inform v3**.

Example

```
snmp servers 100.100.2.4 100.100.3.3
snmp version v3 watchguard MD5 strongpass des str0ngpa55.
snmp traps enable inform v3
```

static-arp

Description

Create an IP address to MAC address binding.

Syntax

static-arp (*name*) (*ip-address*) (*mac-address*)

name is the name of the interface.

ip-address is the IP address of the computer.

mac-address is the physical address of the computer.

Example

```
static-arp user1 10.0.1.56 00:1F:3C:C7:70:9A
```

system

Description

Set global device properties.

Syntax

system contact (*name*)

name is the name of the system administrator.

system location (*location*)

location is the geographic location of the Firebox.

system name (*device-name*)

device-name is the friendly name of the Firebox as it appears in reports and graphic displays.

system timezone (*zone*)

zone is the timezone of the Firebox. It must be a two digit integer from 00 to 74.

To get a list of zone values, type **system timezone ?**

threat-detection

Description

Enable the Threat Detection and Response (TDR) subscription service on the Firebox.

Syntax

threat-detection enable

Enable the Threat Detection and Response service on the Firebox.

threat-detection (**account-uuid** *uuid*)

Specify your Threat Detection and Account UUID. The account UUID is required for the Firebox to report network events to your TDR account.

uuid must match the Account UUID on the Firebox Configuration page in your TDR account

Example

```
threat-detection enable
threat-detection account-uuid d4372396-ff5e-4a75-8548-4807f0492855
```

tor-exit-node-blocking

Description

Configure the Tor Exit Node Blocking service (Fireware v12.8.1 and higher).

Syntax

tor-exit-node-blocking enable

Enable the Tor Exit Node Blocking service.

Use **no tor-exit-node-blocking enable** to disable the service.

trusted-ca-certificates

Description

Enable or disable automatic trusted CA certificate updates on the Firebox.

Syntax

trusted-ca-certificates automatic-update enable

Enable automatic CA certificate updates.

Use **no trusted-ca-certificates automatic-update enable** to disable automatic updates.

v6 ip route

Description

Configure IPv6 static routes and IPv6 BOVPN virtual interface routes.

Syntax

v6 ip route (*destination*) (*fwdaddr*) [**metric** *metricvalue*]

Create an IPv6 static network route.

destination must be one of these options: *address* or *net*.

ipv6-address is the IP address for the destination in the format of A:B:C:D:E:F:G:H.
ipv6-net is the IP subnet for the destination in the format of A:B:C:D:E:F:G:H/I.

fwdaddr is the forwarding router's address in the format of A.B.C.D.

metricvalue is the route metric. It must be an integer from 1 to 1024. Default value is 1.

v6 ip route vpn-route (*bovpn_vif*) (*destination*) [**metric** *metricvalue*]

Create an IPv6 static network route through a BOVPN virtual interface.

bovpn_vif is the name of an existing BOVPN virtual interface. It is case sensitive.

destination must be one of these options: *address* or *net*.

ipv6-address is the IP address for the destination in the format of A:B:C:D:E:F:G:H.
ipv6-net is the IP subnet for the destination in the format of A:B:C:D:E:F:G:H/I.

metricvalue is the route metric. It must be an integer from 1 to 1024. Default value is 1.

Example

```
v6 ip route 2561:1900:4545:3:200:F8FF:FE21:67CF
2260:F3A4:32CB::D837:FC76:12FC 2

v6 ip route vpn-route BovpnVif.1 2001::DB8:20 2
```

vlan

Description

Create or edit a VLAN virtual interface on the Firebox. The VLAN command starts a separate command mode with commands you can use to configure the VLAN. In VLAN command mode, the command prompt changes to "WG(config/vlan-<vlan-name>)#" where <vlan-name> is the name of the VLAN interface.

Use the **Exit** command to exit this mode.

Syntax

vlan (*vlanname*)

vlanname is a string that uniquely identifies the VLAN.

Use **no vlan** (*vlanname*) to delete the VLAN virtual interface.

vlan-id (*id*) (**security-zone** (**external**|**trusted**|**optional**)) (*address*) **member** (*if-number*|**name** *if-name*) (**tagged**|**untagged**)

Configure the settings for a new VLAN.

id is the VLAN unique identifier. It must be a number from 1 to 4094.

You must set the **security-zone** to one of these options: **external**, **trusted**, **optional**, or **custom**.

address is the IP address assigned to the virtual interface.

For **trusted** and **optional** zones it is either an address with mask in the format of A.B.C.D A.B.C.D. or a net in the format of A.B.C.D/# where # must be in the range of 8 to 30.

For the **external** zone it can be one of these options: **static-ip**, **dhcp** or **pppoe**.

If *address* is **static-ip** you must also specify the static *ipaddress*. It is either an address with mask in the format of A.B.C.D A.B.C.D. or a net in the format of A.B.C.D/# where # must be in the range of 8 to 30.

If *address* is **pppoe**, you must also specify the PPPoE *username* and *password*.

If *address* is **dhcp**, you must specify DHCP configuration options.

- *ipaddress* configures the DHCP server to lease a specific IP address.

- **Any** configures the external interface to get a DHCP-assigned IP address from the ISP.

- *leasetime* is the duration in hours that addresses are leased to devices on the network.

- **host-id** *hostid* is the Host ID to use to negotiate an IP address from the DHCP server.

- **host-name** *hostname* is the host name to use to negotiate an IP address from the DHCP server.

if-number is the interface number to add as a member of the VLAN.

if-name is the name of a physical or link aggregation interface to add to the VLAN.

You must specify whether packets sent by this vlan interface are **tagged**, or **untagged**.

You can specify more than one member interface for the VLAN.

After you configure a VLAN to use PPPoE, use the **pppoe** command to configure other PPPoE options. For information, see the **pppoe** command in *Interface Command Mode Reference*

vlan-id (*id*)

Change the ID for the VLAN.

id is the VLAN unique identifier. It must be a number from 1 to 4094.

aging

Configure the aging time (in seconds). The default value is 300 seconds. You can specify a value between 0 and 2147483647.

8021penable

Enable 802.1p priority marking (tagging) for Layer 2 frames.

To disable, use **no 8021p enable**.

dhcpserver (**start-addr** *startip endip leasetime*) [**dns-server** *dns*...] [**domain** *domainname*] [**reservation** *resvname macaddress ipaddress*] [**wins** *wins*...]

Configure the VLAN interface as a DHCP server for computers on that interface.

start-addr defines a DHCP address pool. In the same line, you can use the start-addr command multiple times with these parameters:

startip is the first IP address in the DHCP address pool.

endip is the last IP address in the DHCP address pool.

leasetime is the duration in hours that addresses are leased to devices on the network. The value must be an integer.

dns is the IP address of one or more valid DNS servers.

domainname is the domain name used by devices on the network.

reservation defines a pair of MAC address and IP address that are reserved within the DHCP address pool. In the same line, you can use the reservation command multiple times with these parameters:

resvname is a string to identify a reserved address.

macaddress is the MAC address of the Firebox with a reserved address.

ipaddress is the IP address assigned to the reserved address.

wins is the IP address of one or more valid WINS servers.

Use **no dhcp enable** to disable DHCP server on the interface.

dhcp *option*

Configure a predefined DHCP option. DHCP options are used by many VoIP phones.

option must be one of these predefined options:

capwap-ac-v4 *ipaddress* specifies the IP address of a CAPWAP access controllers. You can specify multiple IP addresses, separated by spaces. This corresponds to DHCP option 138 (CAPWAP access controller).

dhcp-state *state* specifies the DHCP state. This is used by ShoreTel phones for an FTP boot option. This corresponds to DHCP option 156 (DHCP state).

sip-server *ipaddress* specifies the IP address of a Session Initiation Protocol (SIP) server. You can specify multiple IP addresses, separated by spaces. This corresponds to DHCP option 120 (SIP servers).

[**tftp-server***address*] specifies the IP address or domain name of the TFTP server where a DHCP client can download the boot configuration. *address* can be a domain name or an IP address. This corresponds to DHCP option 66 (TFTP server name) and option 150 (TFTP server IP address).

[**tftp-boot-file***bootfile*] specifies the name of the boot file. This corresponds to DHCP option 67 (boot file name).

time-offset *seconds* specifies the time offset in seconds from Coordinated Universal Time (UTC). This corresponds to DHCP option 2 (time offset).

vendor-spec *option* specifies vendor-specific information. This corresponds to DHCP option 43 (vendor specific information).

dhcp custom-option *option-code option-name option-type value*

Configure a custom DHCP option, as described in RFC 2132. If you configure more than one interface to use the same DHCP option code, the *option-type* must be the same on each interface.

option-code is the DHCP option code. It must be an integer from 1 - 255. DHCP options 1, 3, and 28 are not supported.

name is a name to describe this DHCP option

option-type is the type of value required by this option. It must be one of these types:

boolean Specify a Boolean DHCP option value (true or false)

four-byte-integer Specify a DHCP option value as a four bytes integer

hexadecimal Specify the DHCP option value as a hexadecimal number

ip-address-list Specify the DHCP option value as a list of IP addresses, separated by spaces

one-byte-integer Specify the DHCP option value as a one byte integer

text Specify the DHCP option value as a text string

two-byte-integer Specify the DHCP option value as a two bytes integer

unsigned-four-byte-integer Specify the DHCP option value as an unsigned four bytes integer

unsigned-one-byte-integer Specify the DHCP option value as an unsigned one byte integer

unsigned-two-byte-integer Specify the DHCP option value as an unsigned two bytes integer

value is the value to assign to the option. The value must match the type specified in *type*.

intra-vlan-inspection (**enable**|**disable**)

Enable or disable the Firebox to apply firewall policies to traffic between interfaces that are members of the VLAN. In Fireware v12.1.1 and higher, this setting is enabled by default for new external VLAN interfaces.

ip address (*address*)

Change the IP address for the VLAN.

address is the IP address assigned to the virtual interface.

For trusted and optional zones it is either an address with mask in the format of A.B.C.D A.B.C.D. or a net in the format of A.B.C.D/# where # must be in the range of 8 to 30.

For the external zone it can be one of these options: static-ip, dhcp or pppoe.

ip ip-node-type (*option*)

Configure whether to enable IPv6 addressing on the VLAN interface.

option must be one of these options:

ip4-only — use the configured IPv4 address only.

ip4-6 — enable an IPv6 address for this interface in addition to the configured IPv4 address. When you select this option, Fireware assigns a link-local IPv6 address to that interface, when the interface is active. Use the show interface command to see the assigned IPv6 address.

member (*if-number*|**name** *if-name*) (**tagged**|**untagged**)

Add an interface member to the VLAN.

if-number is the interface number to add as a member of the VLAN.

if-name is the name of a physical or link aggregation interface to add to the VLAN.

You must specify whether packets sent by this VLAN interface are **tagged**, or **untagged**.

You can specify more than one member interface for the VLAN.

Use **no member** (*interface*) to remove an interface from the VLAN.

secondary (*address*)

address must be one of these options: *addr mask* or *net*

addr is an IP address, and must be in the format of A.B.C.D.

mask is an IP subnet mask, and must be in the format of A.B.C.D.

net is the IP address and subnet prefix in the format of A.B.C.D/# where # must be in the range of 0 to 32.

This command can take multiple address entries.

Use **no secondary** to remove all secondary addresses from this interface.

security-zone (**external**|**trusted**|**optional**|**custom**) (*address*)

Change the security zone for the VLAN. When you change the security zone, you must also change the VLAN IP address.

The security zone must be one of these options: external, trusted, optional, or custom.

address is the IP address assigned to the interface.

For trusted, optional and custom zones it is either an address with mask in the format of A.B.C.D A.B.C.D. or a net in the format of A.B.C.D/# where # must be in the range of 8 to 30.

For the external zone it can be one of these options: static-ip, dhcp or pppoe.

The dhcp address option is not supported for an external VLAN on a FireCluster.

spanning-tree

Enable and configure Spanning Tree Protocol for a VLAN on the Firebox.

Use *enable*) to enable Spanning Tree Protocol.

(*bridgeprio*) is the bridge priority. To make sure that the Firebox is always selected as the root bridge, specify a bridge priority number that is lower than all other bridges on your network. The default value is 32768. You can specify a value between 0 and 65535, in increments of 4096.

port)

port number is the number of the Firebox port.

pathcost is the path cost. The default value is 0. You can specify a value between 0 and 65535.

portpri is the port priority. In an election, if all ports have the same path cost and Bridge ID, the port with the lowest port priority becomes the root port. The default value is 128. You can specify a value between 1 and 254, in increments of 16.

Timers:

[*fd*] is the forward delay timer. It specifies how long the Firebox ports remain in the Listening and Learning states. The default value is 15 seconds. You can specify a value between 4 and 30 seconds.

(*hello*) specifies how often a root bridge generates a BPDU. You can configure this value only for a Firebox that is the root bridge. The default is 2 seconds. You can specify a value between 1 and 10 seconds.

(*maxage*) specifies how often a bridge port saves its configuration BPDU information. The default is 20 seconds. You can specify a value between 6 and 40 seconds.

v6

Configure IPv6 settings for the VLAN interface. You must use the **ip ip-node-type** command to enable IPv6 for the interface before you can configure IPv6 settings.

The available v6 command options are the same as for a physical trusted, optional, or custom interface. For more information, see the Command Mode section *v6* on page 228.

Example

```
vlan VLAN10
vlan-id 10 security-zone trusted 10.10.1.1/24 member 3 tagged 4 tagged
vlan-id 11
intra-vlan-inspection enable
ip address 10.10.1.2/24
member name LA-1 untagged
security zone optional 10.10.1.3/24
vlan VLAN10 spanning-tree bridgeprio 0
```

vpn-setting

Description

Enable and configure global VPN settings.

vpn-setting (*setting*) **enable**

setting must be one of these settings:

built-in-ipsec-policy — enable the use of the built-in IPSec policy that allows IPSec traffic from Any-External to Firebox. Enabled by default.

failover — automatically remove VPN routes with the tunnel for a BOVPN virtual interface is down. If you select this option, you must do one of two things to make sure that the VPN routes for a BOVPN virtual interface are added to the routes table when the tunnel is available. You can either enable policy-based routing for the BOVPN virtual interface, or, in the BOVPN virtual interface configuration, use the **auto-start enable** option.

ipsec-use-non-default-routes — enable the use of non-default routes (static or dynamic) to determine if IPSec is used. This applies only to traffic through a BOVPN that is not a virtual interface.

ldap — enable the use of an LDAP server for certificate verification.

pass-through — adds a policy that allows outbound IPSec traffic from IPSec VPN clients on the trusted or optional network.

security-readonly — make the security policy read-only in the Mobile VPN with IPSec client.

tos-tunnel-flag — enable TOS (Type of Service) for IPSec.

Use **no vpn-setting** (*setting*) **enable** to disable a global VPN setting.

vpn-setting ldap server (*address*) [*port*]

Set the LDAP server to use for certificate verification.

address is the IP address of the LDAP server, in the format A.B.C.D.

port is the port number to use on the LDAP server.

vpn-setting notification notification enable [**action-type** (**email**|**pop-window**)] [**launch-interval** *launch-interval*] [**repeat-count** *repeat-count*]

Configure VPN notification settings.

You can set the notification action to one of these action types:

email — the Log Server sends an email to the configured email address when the event occurs.

pop-window — the Log Server opens a dialog box when the event occurs.

launch-interval is the minimum time (in minutes) between different notifications, default is 15.

repeat-count is the number of events to include in a repeat log notification, default is 10.

vpn-setting notification snmp-trap enable

Enable the Firebox to send event notifications to the configured SNMP management system.

vpn-setting ipsec-pkt-error-log *loglevel*

Enable or disable IPSec log message error types.

loglevel must be one of these settings:

0 — disable all IPSec error log messages
1 — enable Invalid SPI log messages
2 — enable Replay Window Check failure log messages
4 — enable Replay Check failure log messages
8 — enable AH integrity check failure log messages
16 — enable ESP integrity check failure log messages
31 — enable all IPSec error logs

Example

```
vpn-setting pass-through

vpn-setting tos-tunnel-flag

vpn-setting ldap enable

vpn-setting ldap server 100.100.100.50 389

vpn-setting notification notification enable action-type email

vpn-setting notification snmp-trap enable

vpn-setting ipsec-pkt-error-log 2

vpn-setting ipsec-pkt-error-log 0
```

web-server-cert

Description

Configure the web server certificate to use for authentication to Fireware Web UI.

Syntax

web-server-cert custom (*common-name*) (*org-name*) (*org-unit-name*) [**dns** *dns-ip*] [**ip** *extended-ip]*

Use a custom certificate signed by your Firebox. The certificate automatically includes all trusted interface IP addresses.

common-name is a string for the common name of your organization. This is usually the domain name.

org-name is a string for the organization name.

org-unit-name is a string for the organizational unit name.

dns-ip is a string for an additional IP address to include in the certificate.

extended-ip is a string for an additional domain name to include in the certificate.

web-server-cert default

Use the default certificate.

web-server-cert third-party (*certificate-id*)

Use a certificate you have imported previously.

certificate-id is the certificate identification number, between 0 and 99999.

Example

```
web-server-cert default

web-server-cert third-party 1234

web-server-cert custom example.com exampleco hq
```

wireless access-point

Description

Configure Wi-Fi settings for an Firebox wireless device. The **wireless access-point** command starts a separate command mode with commands you can use to configure the wireless access points. In **wireless access-point** command mode, the command prompt changes to "WG(config/wireless-<ap#>" where ap# is the number of the wireless access point.

Use the **Exit** command to exit this mode.

Syntax

wireless access-point *index*

This command puts you in wireless access-point mode to configure a specific wireless access point interface.

index must be one of these options: **1**, **2**, or **3**.

enable

Enable the access point.

use **no enable** to disable the access point.

broadcast enable

Enable SSID broadcasts for the specified access point.

use **no broadcast enable** to disable SSID broadcasts for this access point.

security-zone *zone ipaddr ipmask* | *net*

Select the security zone and IP address for the specified access point.

zone must be one of these options: **custom**, **optional**, or **trusted**.

ipaddr is the IP address for the interface.

ipmask is the netmask for the interface.

net is the address in network slash notation.

ip address *ipaddr ipmask* | *net*

Configure the IP address for the specified access point.

ipaddr is the IP address for the interface.

ipmask is the netmask for the interface.

net is the address in network slash notation.

dhcp server start-addr *start-addr end-addr*

Configure the DHCP server address range.

start-addr is the start IP address of the range.

end-addr is the end IP address of the range.

dhcp server reservation *hostname mac-addr*

Configure a DHCP address reservation for a host name and associated MAC address.

hostname is the host name of the client with the DHCP reservation.

mac-addr is the MAC address of the client with the DHCP reservation.

dhcp server wins *wins*

Configure the WINS server for the DHCP server.

wins is the IP address of your WINS server.

dhcp server dns-server *dns*

Configure DNS for the DHCP server.

dns is the IP address of your DNS server.

dhcp server domain *domain*

Configure a domain for the DHCP server.

domain is the domain name for the DHCP server, such as *example.com*.

dhcp server *lease-time*

Configure the lease time for the DHCP server.

lease-time is the DHCP address lease time in hours. The value must be from 1-596523.

dhcp server tftp-server *domain* | *addr*

Configure the domain name or IP address of a TFTP server for the DHCP server.

domain is the domain name of the TFTP server.

addr is the IP address of the TFTP server.

dhcp server tftp-boot-file *file-name*

Configure the TFTP boot file for the DHCP server.

file-name is the TFTP server configuration file.

log-auth enable

Enable authentication event logging for the specified access point.

Use **nolog-auth enable** to disable authentication event logging for this access point.

mac-acl enable

Enable MAC access control for the specified access point.

Use **no mac-acl enable** to disable MAC access control for this access point.

mac-acl *mac-address*

Add a MAC address to the list of allowed address for MAC access control.

mac-address is the MAC address of a computer you want to give access to this access point.

name*name*

Define an alias name for this wireless interface.

name is the alias name you want to provide for this wireless interface.

require-mvpn enable

Require encrypted Mobile VPN with IPSec connections to the specified access point.

Use **no require-mvpn enable** to not require encrypted Mobile VPN with IPSec connections to this access point.

prohibit enable

Prohibit client to client wireless network traffic.

Use **noprohibit enable** to disable the prohibition of client to client wireless network traffic.

wireless (*ssid*) (*auth*) (**enc** *enc-option*) (*auth-server*) (*eap-protocol*) (*eap-tunnel-protocol*) (*cert-type*) (*cert-id*) [*validate-client* (*cert-name)*] [*eap-auth-period*]

Configure wireless authentication and encryption settings.

ssid is the wireless network name.

auth is the authentication method. The available option depends on the Wi-Fi option you select.

auth must be one of these options:

open-system — Open system authentication
shared-key — shared key authentication
wpa-only — wpa psk authentication
wpa-wpa2 — wpa psk and wpa2 psk authentication
wpa2-only — wpa2 psk authentication

wpa-e — wpa enterprise

wpa2-e — wpa2 enterprise authentication

wpa2-wpa-e — wpa and wpa2 enterprise authentication

enc is the encryption option. The encryption option is dependent on the authentication method you select.

for **open-system** authentication, *enc* must be one of these options: **disable**, **wep-128-ascii**, **wep-128-hex**, **wep-40-ascii**, **wep-64-hex**.

for **shared-key** authentication, *enc* must be one of these options: **wep-128-ascii**, **wep-128-hex**, **wep-40-ascii**, **wep-64-hex**.

In Fireware v12.1.1 and higher, you can no longer save a configuration with WEP encryption enabled. WEP is an insecure and deprecated protocol, and we recommend you use WPA2.

for **wpa-only**, **wpa-wpa2**, and **wpa2-only** authentication, *enc* must be one of these options: **aes**, **auto**, or **tkip**.

You cannot use tkip as the encryption method if you use a wireless mode that supports 802.11n.

for **wpa-e**, **wpa-wpa2-e**, and **wpa2-e** authentication, *enc* must be one of these options: **aes**, or **auto**. If you select **auto**, the Firebox automatically uses tkip or aes for encryption.

If **auth** is set to a non-enterprise authentication method (**open-system**, **shared-key**, **wpa-only**, **wpa-wpa2**, or **wpa2-only**), use this option to complete your wireless authentication configuration:

enc-option is the option needed to complete the encapsulation for the non-enterprise authentication methods. This dependent on the encryption options you select.

for **disable**, *enc-option* is Null.

for **wep-128-ascii**, **wep-128-hex**, **wep-40-ascii**, and **wep-64-hex**, *enc-option* must be a combination of *key*, length and type of which is defined on the selected encapsulation, and *key-index*, which is an integer from 1 to 4

for **aes**, **auto** and **tkip**, *enc-option* is the passphrase.

If **auth** is set to one of the enterprise authentication methods (wpa-e, wpa2-e, or wpa2-wpa-e), use these settings to configure the authentication server.

auth-server is the authentication server to use; *auth-server* must be one of these options:

- **Firebox-DB** — use the Firebox as the authentication server for wireless user authentication

- **RADIUS** — use a configured RADIUS authentication server for wireless user authentication

eap-protocol — EAP protocol. It must be one of **eap-peap**, **eap-ttls**, or **eap-tls**.

eap-tunnel-protocol — the available options depend on the selected EAP protocol. It must be one of these options:

- for **eap-tls**, *eap-tunnel-protocol* is Null.

- for **eap-peap**, *eap-tunnel-protocol* must be MSCHAPv2.

- for **eap-ttls**, *eap-tunnel-protocol* must be one of these options: **auth**, **MSCHAPv2**, **MSCHAP1**, **CHAP**, **PAP**, or **MD5**.

If *auth-server* is set to **Firebox-DB**, use these settings to configure certificates for authentication.

cert-type — the certificate type to use for Firebox-DB authentication. It must be one of these options:

- **default** — use the default certificate signed by the Firebox

- **third-part-cert** — use third party certificates for authentication.

cert-id — If cert-type is third-part-cert, cert-id is the third party certificate ID.

validate-client — If cert-type is third-part-cert, you can use a Certificate Authority to validate the client certificate. If you specify validate-client, you must also include the name of the certificate.

eap-auth-period — the EAP authentication period, in seconds. It must be an integer between 0 and 2147483647; default is 3600 seconds.

Example

```
wireless access-point 1
 security-zone custom
 broadcast enable
```

wireless client

Description

Enable and configure a wireless client as an external interface.

Syntax

wireless client enable

Enable wireless client as an external interface.

Use **no wireless client enable** to disable this setting.

wireless client dhcp-client (**client** *clientname*) [**host-name** *hostname*] [*leasetime*] [*ip-address*]

Configure wireless client settings when negotiating with a DHCP server.

clientname is a string for the optional client name.

hostname is a string for the optional host name.

leasetime is a string for the optional lease time from 1 to 2147483647.

ip-address is a string for the optional preferred IP address.

any use this option instead of *ip-address* to enable DHCP to assign an IP address automatically.

wireless client manual-conf (*ip-address*) (*mask*) (*gateway*)

Manually configure the wireless client IP address.

ip-address is the wireless client IP address.

mask is the subnet mask in dotted decimal notation.

gateway is the default gateway of the wireless external interface.

name*name*

Define an alias name for this wireless interface.

name is the alias name you want to provide for this wireless interface.

wireless client wireless (*ssid*) (*auth*) (**enc** *enc-option*) (*auth-server*) (*eap-protocol*) (*eap-tunnel-protocol*) (*cert-type*) (*cert-id*) [*validate-client* (*cert-name)*] [*eap-auth-period*]

Configure wireless authentication and encryption settings.

ssid is the wireless network name.

auth is the authentication method. The available option depends on the Wi-Fi option you select.

[*auth*] must be one of these options: **open-system**, **shared-key**, **wpa-only**, **wpa-wpa2**, **wpa2-only**.

enc is the encryption option. The encryption option is dependent on the authentication method you select.

for **open-system** authentication, *enc* must be one of these options: **disable**, **wep-128-ascii**, **wep-128-hex**, **wep-40-ascii**, **wep-64-hex**.

for **shared-key** authentication, *enc* must be one of these options: **wep-128-ascii**, **wep-128-hex**, **wep-40-ascii**, **wep-64-hex**.

In Fireware v12.1.1 and higher, you can no longer save a configuration with WEP encryption enabled. WEP is an insecure and deprecated protocol, and we recommend you use WPA2.

for **wpa-only**, **wpa-wpa2**, and **wpa2-only** authentication, *enc* must be one of these options: **aes**, **auto**, or **tkip**.

You cannot use tkip as the encryption method if you use a wireless mode that supports 802.11n.

for **wpa-e**, **wpa-wpa2-e**, and **wpa2-e** authentication, *enc* must be one of these options: **aes**, or **auto**. If you select **auto**, the Firebox automatically uses tkip or aes for encryption.

If **auth** is set to a non-enterprise authentication method (**open-system**, **shared-key**, **wpa-only**, **wpa-wpa2**, or **wpa2-only**), use this option to complete your wireless authentication configuration:

enc-option is the option needed to complete the encapsulation for the non-enterprise authentication methods. This dependent on the encryption options you select.

for **disable**, *enc-option* is Null.

for **wep-128-ascii**, **wep-128-hex**, **wep-40-ascii**, and **wep-64-hex**, *enc-option* must be a combination of *key*, length and type of which is defined on the selected encapsulation, and *key-index*, which is an integer from 1 to 4

for **aes**, **auto** and **tkip**, *enc-option* is the passphrase.

If **auth** is set to one of the enterprise authentication methods (wpa-e, wpa2-e, or wpa2-wpa-e), use these settings to configure the authentication server.

auth-server is the authentication server to use; *auth-server* must be one of these options:

- **Firebox-DB** — use the Firebox as the authentication server for wireless user authentication

- **RADIUS** — use a configured RADIUS authentication server for wireless user authentication

eap-protocol — EAP protocol. It must be one of **eap-peap**, **eap-ttls**, or **eap-tls**.

eap-tunnel-protocol — the available options depend on the selected EAP protocol. It must be one of these options:

- for **eap-tls**, *eap-tunnel-protocol* is Null.

- for **eap-peap**, *eap-tunnel-protocol* must be MSCHAPv2.

- for **eap-ttls**, *eap-tunnel-protocol* must be one of these options: **auth**, **MSCHAPv2**, **MSCHAP1**, **CHAP**, **PAP**, or **MD5**.

If *auth-server* is set to **Firebox-DB**, use these settings to configure certificates for authentication.

cert-type — the certificate type to use for Firebox-DB authentication. It must be one of these options:

- **default** — use the default certificate signed by the Firebox

- **third-part-cert** — use third party certificates for authentication.

cert-id — If cert-type is third-part-cert, cert-id is the third party certificate ID.

validate-client — If cert-type is third-part-cert, you can use a Certificate Authority to validate the client certificate. If you specify validate-client, you must also include the name of the certificate.

eap-auth-period — the EAP authentication period, in seconds. It must be an integer between 0 and 2147483647; default is 3600 seconds.

Example

```
wireless client enable

wireless client dhcp-client 100.100.100.10 172800

wireless client manual-conf 100.100.100.10 255.255.255.0 100.100.100.1
```

wireless radio-settings

Description

Configure wireless radio settings for a WatchGuard wireless device.

Syntax

wireless radio-settings *band* [*mode channel*] *frag_threshold rts_threshold tx_power vulnerability-mitigation*

Configure wireless radio settings for a WatchGuard wireless device.

The available values for band, mode and channel are different for each wireless region.

band is the wireless band. It must be one of these values:

24 — 2.4 Ghz

5 — 5 Ghz

mode is the wireless mode.

For the 2.4 Ghz band, *mode* must be one of these values:

IEEE80211bg — 802.11b and 802.11g
IEEE802.11bonly — 802.11b only
IEEE80211gn — 801.11n and 802.11g
IEEE80211nbg — 801.11n, 802.11b, and 802.11g

For the 5 Ghz band, *mode* must be one of these values:

IEEE80211an — 80211a and 802.11n
IEEE80211aonly — 802.11a only
IEEE80211nac — 802.11n and 802.11ac

channel is the wireless channel.

For the 2.4 GHz band, *channel* must be one of these values: **auto**, **channel-01**, **channel-02**, **channel-03**, **channel-04**, **channel-05**, **channel-06**, **channel-07**, **channel-08**, **channel-09**, **channel-10**, **channel-11**, **channel-12**, **channel-13**, or **channel-14**.

For the 5 Ghz band, *channel* must be one of these values: **auto**, **channel-36**, **channel-40**, **channel-44**, **channel-48**, **channel-149**, **channel-153**, **channel-157**, **channel-161**, or **channel-165**. The available channels depend on the country where the Firebox is operating and the wireless mode you select.

When you set channel to **auto**, the wireless device automatically selects a quiet channel from the available channels in the selected band.

frag_threshold is the fragmentation threshold in bytes for the specified access point. It must be an integer from 256 to 2346.

rts_threshold is the request to send threshold in bytes for the specified access point. It must be an integer from 256 to 2346.

tx_power is the maximum transmit power to limit or expand the transmission distance of your wireless signals. You can set the transmit power between 3dBm to 20dBm, or set the value to Auto. The default (Auto) is 20dBm. The transmit power cannot exceed the regulatory limits set by your region.

vulnerability-mitigation is used to enable WPA/WPA2 KRACK vulnerability mitigation that blocks handshake messages that can potentially exploit clients and forces clients to reauthenticate.

Example

```
wireless radio-settings both
```

wireless rogue-ap

Description

Configure settings for wireless rogue access point detection.

Syntax

wireless rogue-ap enable

Enable wireless rogue access point detection.

Use **no wireless rogue-ap enable** to disable scheduled wireless rogue access point detection scans.

wireless rogue-ap log enable

Enable logging for wireless rogue access point scans.

wireless rogue-ap notification notification enable [**action-type** (**email**|**pop-window**)] [**launch-interval** *launch-interval*] [**repeat-count** *repeat-count*]

Configure notification settings for wireless rogue access point scans.

You can set the notification action to one of these action types:

email — the Log Server sends an email to the configured email address when the event occurs.

pop-window — the Log Server opens a dialog box when the event occurs.

launch-interval is the minimum time (in minutes) between different notifications, default is 15.

repeat-count is the number of events to include in a repeat log notification, default is 10.

wireless rogue-ap notification snmp enable

Enable the Firebox to send event notifications to the configured SNMP management system.

wireless rogue-ap scannow

Start an immediate scan for rogue wireless access points

wireless rogue-ap schedule always

Schedule a rogue access point detection scan to run continuously. The scan starts automatically every 15 minutes.

wireless rogue-ap schedule daily *hour* [**minute** *minute*]

Schedule a rogue access point detection scan to run daily.

hour is the hour of day to start the scan. It must be an integer from 1 to 24.

minute is the optional minute of the hour to start the scan.

wireless rogue-ap schedule date (*day*) (*hour*) [**minute** *minute*]

Schedule a rogue access point detection scan to run monthly on a specified day of the month.

day is the day of the month you want to run the scan. It must be an integer from 1 to 31.

hour is the hour of day to start the scan. It must be an integer from 1 to 24.

minute is the optional minute of the hour to start the scan.

wireless rogue-ap schedule monthly (**first**|**last**) *weekday hour* [**minute** (*minute*)]

Schedule a rogue access point detection scan to run monthly on a specified day of the week.

You can specify whether to run the scan on the **first** or **last** occurrence of that day of the week.

weekday is the day of the week you want to run the scan. It must be one of these options: **sunday**, **monday**, **tuesday**, **wednesday**, **thursday**, **friday**, or **saturday**.

hour is the hour of day to start the scan. It must be an integer from 1 to 24.

minute is the optional minute of the hour to start the scan.

wireless rogue-ap schedule weekly *weekday hour* [**minute** (*minute*)]

Schedule a rogue access point detection scan to run weekly at a specified time.

weekday is the day of the week you want to run the scan. It must be one of these options: **sunday**, **monday**, **tuesday**, **wednesday**, **thursday**, **friday**, or **saturday**.

hour is the hour of day to start the scan. It must be an integer from 1 to 24.

minute is the optional minute of the hour to start the scan.

wireless rogue-ap trust-ap *index* [**ssid** *ssid*] [**channel** *channel*] [**encryption** *encryption*] (*tag-type*) [**authentication** *authentication*] [**group-encryption** *group-encryption*] [**pair-encryption** *pair-encryption*] [**mac-address** *mac-address*]

Add or edit a wireless trusted access point in the trusted access points list. To add a new trusted access point, you must specify the ssid. To edit an existing trusted access point, you must specify the index. You can optionally specify other options to help your Firebox identify an access point as trusted.

index — the index number of an existing trusted access point in the trusted access point list. To see the trusted access point list, use show wireless rogue-ap trust-ap.

ssid — the network name (SSID) configured for the trusted access point. The ssid is optional.

channel — the channel used by the trusted access point. The channel must be a number from 1 to 14. The default value is **Any**.

encryption — the encryption method used by the trusted access point. The default value is **Any**. If specified, it must be one of these options:

wpa-only — The trusted access point uses only WPA Wi-Fi Protected Access
wpa-wpa2 — The trusted access point uses WPA and WPA2 Wi-Fi Protected Access
wpa2-only — The trusted access point uses only WPA2 Wi-Fi Protected Access

tag-type - if the encryption method is **wpa-wpa2**, you must specify the tag-type to show whether the authentication, group-encryption and pair-encryption settings in the command apply to the wpa or wpa2 encryption method for this trusted access point. It must be one of these options:

wpa-tag — configure wpa settings used by the trusted access point

wpa2-tag — configure wpa2 settings used by the trusted access point

authentication - the authentication type used by the trusted access point. It must be one of these options:

psk — The trusted access point uses psk (pre-shared key) authentication. This is the default value.

enterprise — The trusted access point uses enterprise authentication.

group-encryption - the group encryption algorithm used by the trusted access point. It must be one of these options: **wep40**, **tkip-only**, **ccmp-aes**, **wep104**, or **tkip-ccmp-aes**. The default value is **wep40**.

pair-encryption — the pair encryption algorithm used by the trusted access point. It must be one of these options: **wep40**, **tkip-only**, **ccmp-aes**, **wep104**, or **tkip-ccmp-aes**. The default value is **wep40**.

mac-address — the MAC address of the trusted access point. The default value is **Any**.

no wireless rogue-ap trust-ap (*index*)

Remove a trusted access point from the trusted access point list.

index — the index number of an existing trusted access point in the trusted access point list.

no wireless rogue-ap trust-ap (*index*) [*mac-address*] [*channel*] [*encryption*]

Remove configured settings for a trusted access point.

index — the index number of an existing trusted access point in the trusted access point list.

mac-address — removes the MAC address, and resets the MAC address to the default value, Any.

channel — removes the channel setting, and resets the channel to the default value, Any.

encryption — removes the encryption settings, and resets the encryption method to the default value, Any.

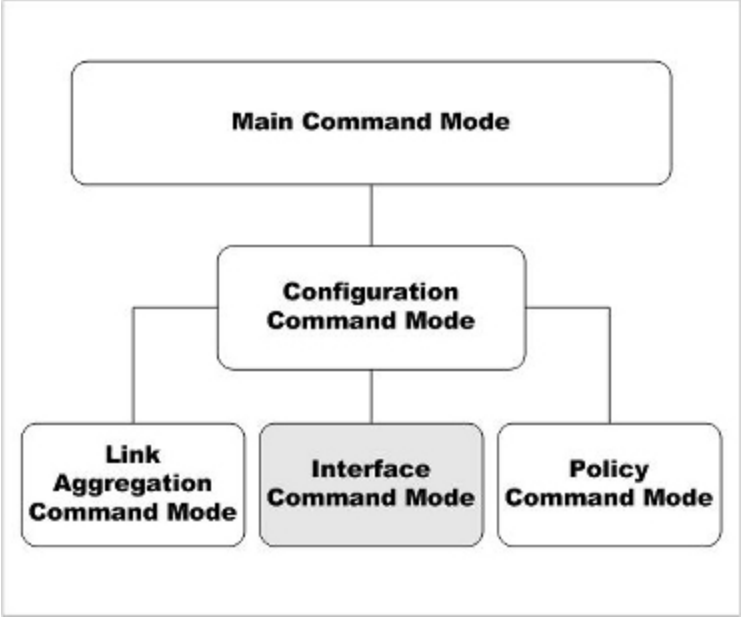
Example

```
wireless rogue-ap schedule always

wireless rogue-ap schedule daily 5 minute 30

wireless rogue-ap schedule date 1 5 minute 30

wireless rogue-ap schedule monthly first sunday 5 minute 30

wireless rogue-ap schedule weekly sunday 5 minute 30

wireless rogue-ap trust-ap ssid ssid5 encryption wpa2-only authentication
psk

wireless rogue-ap trust-ap 2 encryption wpa-wpa2 wpa-tag authentication
enterprise group-encryption tkip-ccmp-aes pair-encryption tkip-ccmp-aes

no wireless rogue-ap trust-ap 2 encryption

no wireless rogue-ap trust-ap 2
```

6 Interface Command Mode

Interface Commands

The WatchGuard Command Line Interface (CLI) Interface command mode is used to configure the separate Ethernet interfaces available on your Firebox.



In the Interface mode, you can:

- Configure the IP address and addressing options for the interface
- Configure the interface as a gateway
- Control MTU and link speed preferences
- Configure the interface as a DHCP server or DHCP relay
- Configure the interface for QoS

Enter the Interface Command Mode

To enter the Interface command mode:

1. Open the CLI in the Configuration command mode.
2. Type the interface fastethernet <if-index> command, where <if-index> is the interface number, from 0 to the number of interfaces minus 1.
3. Press **Enter**.
   In Interface command mode, the CLI prompt changes to
   WG(config/if-fe<if-index>)# where <if-index> is the selected interface.

You can only configure a single Ethernet interface at a time. To configure another interface, exit the Interface mode. From the Configuration mode, use the interface command again to select the second interface.

List of Interface Mode Commands

You can use all common commands in the Interface command mode.

These commands are available only in Interface mode:

Command	Usage
dhcp	Enable the interface as either a DHCP server or relay.
enable	Enable or disable the physical interface.
intra-if-inspection	Enable application of firewall policies to intra-interface traffic on the current interface.
ip	Configure the IP address and addressing options for the interface.
link-speed	Set the link speed and duplex for the interface.
mac-access-control	Configure a trusted or optional interface to restrict access based on MAC address.
mac-ip-binding	Bind the Ethernet MAC address to a particular IP address.
mtu	Control the interface MTU settings.
name	Set the name for the interface as it appears in reports and the user interface.
pppoe	Configure the Point-to -Point over Ethernet Protocol for the external interface.
qos	Enable QoS Marking for traffic that goes out of the interface.

Command	Usage
secondary	Configure the secondary IP addresses that the interface uses to route traffic.
system-dhcp	Configure a trusted or optional interface to use the same DHCP settings you configured for drop-in mode.
type	Set the interface type.
v6	Configure the interface IPv6 settings.
vpn-pmtu	Configure the Per Interface Maximum Transmission Unit for external interface only.

Interface Command Mode Reference

dhcp

Description

Enable the interface as either a DHCP server or relay. Or, enable the external interface as a DHCP client to dynamically get an IP address from an external DHCP server.

Syntax

dhcp relay (*serverip*) [*serverip*] [*serverip]*

Configure a trusted, optional, or custom interface to relay DHCP requests to up to three DHCP servers.

serverip is the IP address of a DHCP server that is used for computers on the interface. You can specify the IP addresses up to three DHCP servers. The Firebox sends DHCP requests to the IP addresses of all DHCP servers you specify.

Use **no dhcp enable** to disable DHCP relay on the interface.

dhcp server (**start-addr** *startip endip leasetime*) [**dns-server** *dns*...] [**domain** *domainname*] [**reservation** *resvname macaddress ipaddress*] [**wins** *wins*...]

Configure a trusted, optional, or custom interface as a DHCP server for computers on that interface.

start-addr defines a DHCP address pool. In the same line, you can use the start-addr command multiple times with these parameters:

startip is the first IP address in the DHCP address pool.

endip is the last IP address in the DHCP address pool.

leasetime is the duration in hours that addresses are leased to devices on the network. The value must be an integer.

dns is the address of one or more valid DNS servers.

domainname is the default DNS domain name used by devices on the network.

reservation defines a pair of MAC address and IP address that are reserved within the DHCP address pool. In the same command, you can use the reservation option multiple times with these parameters:

resvname is a string to identify a reserved address.
macaddress is the MAC address of the device with a reserved address.
ipaddress is the IP address assigned to the reserved address.

wins is the IP address of one or more valid WINS servers.

Use **no dhcp enable** to disable DHCP server on the interface.

dhcp server *option*

Configure a predefined DHCP option. DHCP options are used by many VoIP phones.

option must be one of these predefined options:

capwap-ac-v4 *ipaddress* specifies the IP address of a CAPWAP access controllers. You can specify multiple IP addresses, separated by spaces. This corresponds to DHCP option 138 (CAPWAP access controller).

dhcp-state *state* specifies the DHCP state. This is used by ShoreTel phones for an FTP boot option. This corresponds to DHCP option 156 (DHCP state).

sip-server *ipaddress* specifies the IP address of a Session Initiation Protocol (SIP) server. You can specify multiple IP addresses, separated by spaces. This corresponds to DHCP option 120 (SIP servers).

[**tftp-server***address*] specifies the IP address or domain name of the TFTP server where a DHCP client can download the boot configuration. *address* can be a domain name or an IP address. This corresponds to DHCP option 66 (TFTP server name) and option 150 (TFTP server IP address).

[**tftp-boot-file***bootfile*] specifies the name of the boot file. This corresponds to DHCP option 67 (boot file name).

time-offset *seconds* specifies the time offset in seconds from Coordinated Universal Time (UTC). This corresponds to DHCP option 2 (time offset).

vendor-spec *option* specifies vendor-specific information. This corresponds to DHCP option 43 (vendor specific information).

default-gateway *ipaddress* specifies a default gateway other than the Firebox IP address. This option is supported in Fireware v12.1.1 and higher.

dhcp custom-option *option-code option-name option-type value*

Configure a custom DHCP option, as described in RFC 2132. If you configure more than one interface to use the same DHCP option code, the *option-type* must be the same on each interface.

option-code is the DHCP option code. It must be an integer from 1 - 255. DHCP options 1, 3, and 28 are not supported.

name is a name to describe this DHCP option

option-type is the type of value required by this option. It must be one of these types:

boolean Specify a Boolean DHCP option value (true or false)

four-byte-integer Specify a DHCP option value as a four bytes integer

hexadecimal Specify the DHCP option value as a hexadecimal number

ip-address-list Specify the DHCP option value as a list of IP addresses, separated by spaces

one-byte-integer Specify the DHCP option value as a one byte integer

text Specify the DHCP option value as a text string

two-byte-integer Specify the DHCP option value as a two bytes integer

unsigned-four-byte-integer Specify the DHCP option value as an unsigned four bytes integer

unsigned-one-byte-integer Specify the DHCP option value as an unsigned one byte integer

unsigned-two-byte-integer Specify the DHCP option value as an unsigned two bytes integer

value is the value to assign to the option. The value must match the type specified in *type*.

dhcp any (*leasetime*)

Configure the external interface to get a DHCP-assigned IP address from the ISP.

leasetime is the duration in hours that addresses are leased to devices on the network. The value must be an integer.

Use **no dhcp** to disable DHCP client on the interface.

The dhcp address option is not supported for an external interface on a FireCluster.

dhcp [**host-id** *hostid*] [**host-name** *hostname ipaddress leasetime*]

Configure a detailed DHCP client on an external interface.

hostid is the Host ID to use to negotiate an IP address from the DHCP server.

hostname is the Host Name to use to negotiate an IP address from the DHCP server.

ipaddress is to force the DHCP server to lease a specific IP address.

leasetime is the duration in hours that addresses are leased to devices on the network. The value must be an integer.

Use **no dhcp** *host-name host-id lease-time* to disable detailed DHCP client on the interface.

dhcp release

Release the IP address assigned by DHCP.

dhcp renew

Renew the IP address assigned by DHCP.

dhcp force-renew [**shared-key** *key*] [**enable**]

Enable the Firebox to handle a FORCERENEW message from your ISP or DHCP provider.

key is the shared key specified by the ISP or DHCP provider to authorize the FORCERENEW message. If a shared key is not specified, the Firebox responds to any FORCERENEW message, whether a shared key is present or not.

Use **no dhcp forcerenew** enable to disable this option.

Example

```
dhcp relay 10.0.1.254

dhcp server start-addr 10.0.1.2 10.0.1.30 8

dhcp server start-addr 10.0.1.2 10.0.1.30 8 dns-server 203.23.124.1
203.23.124.2 domain example.com reservation ceo 00:44:FF:33:00:AC 10.0.1.35
wins 10.0.1.100
```

enable

Description

Enable or disable the physical interface.

Syntax

enable

No options available.

Use **no enable** to disable the interface.

intra-if-inspection

Description

Enable application of firewall policies to intra-interface traffic on the current interface.

Syntax

intra-if-inspection enable

(Fireware v12.8 or higher) Enable intra-interface inspection on physical and link aggregation interfaces. If you enable this setting, the Firebox applies firewall policies to intra-interface traffic for the specified interface.

Use **no intra-if-inspection enable** to disable intra-interface inspection on the current interface.

ip

Description

Configure the address and addressing options for the interface.

Syntax

ip address (*option*)

Set the IP address of an interface.

option must be one of these options: *addr mask net*or *default-gw*

addr is an IP address, and must be in the format of A.B.C.D.

mask is an IP subnet mask, and must be in the format of A.B.C.D.

net is the IP address and subnet prefix in the format of A.B.C.D/#, where # must be in the range of 0 to 32.

default-gw is the default gateway. This is only required if you set an IP address for an external interface.

ip df (*flag*)

Configure the Don't Fragment bit on the external interface.

flag must be one of these options: **clear**, **set**, or **copy**.

ip ip-node-type (*option*)

Configure whether to enable IPv6 addressing on the interface.

option must be one of these options:

ip4-only — use the configured IPv4 address only.

ip4-6 — enable an IPv6 address for this interface in addition to the configured IPv4 address. When you select this option, Fireware assigns a link-local IPv6 address to that interface, when the interface is active. Use the show interface command to see the assigned IPv6 address.

Example

```
ip address 192.168.116.1 255.255.255.0
ip address 192.168.116.1/24
ip df set
ip ip-node-type ip4-6
```

If you set an IP address for an external interface, you must include a default gateway.

Example

```
192.168.116.1/24 default-gw 192.168.116.2
```

link-speed

Description

Set the interface link speed and duplex.

Syntax

link-speed (*option*)

option must be one of these options:

10-full — Force 10 Mbps full-duplex operation

10-half — Force 10 Mbps half-duplex operation

100-full — Force 100 Mbps full-duplex operation

100-half — Force 100 Mbps half-duplex operation

1000-full — Force 1000 Mbps full-duplex operation (available only if the interface supports it)

1000-half — Force 1000 Mbps half-duplex operation (available only if the interface supports it)

For a description of which interfaces support a link speed of 1000 Mbps, see the Hardware Guide for your device.

Example

```
link-speed 100-full
```

mac-access-control

Description

Control access to the trusted or optional interface of a Firebox by computer MAC address.

Syntax

mac-access-control enable (*mac-address*)

Enable MAC access control on an interface, or add a MAC address to the allowed list.

mac-address is the MAC address of a computer that is allowed to send traffic on this interface. The MAC address must be in the format of 00:01:23:45:67:89. You must add at least one MAC address before you enable MAC access control.

Use **no mac-access control enable** (*mac-address*) to remove a MAC address of a computer from the list of MAC addresses that are allowed to send traffic on this interface.

Use **no mac-access control enable** to disable MAC access control on the interface.

Example

```
mac-access-control 00:01:23:45:67:89

mac-access-control enable
```

mac-ip-binding

Description

Control access to a Firebox interface from an IP address by computer hardware address.

Syntax

mac-ip-binding (*ipaddress*...) (*macaddr*...)

Use to add MAC addresses to a network interface.

ipaddress is the IP address of the interface.

macaddr is one or more hardware device addresses that can connect to the interface.

This command can have more than one IP address to MAC address pairs.

Use **no mac-ip-binding** (*ipaddress*) (*macaddr*) to disable MAC address binding on this interface.

mac-ip-binding restrict-traffic enable

Use to restrict traffic based on the IP address and MAC addresses already configured for the interface.

Use **no mac-ip-binding restrict-traffic enable** to disable binding traffic restrictions on this interface.

Example

```
mac-ip-binding 100.100.100.3 00:44:FF:33:00:AC 00:44:FF:33:00:F0
mac-ip-binding restrict-traffic enable
```

mtu

Description

Set the Maximum Transmission Unit value of an interface.

Syntax

mtu (*size*)

size is the size in bytes of the maximum transmission unit. Must be an integer from 68 to 9000.

If you enable IPv6, it must be a minimum of 1280.

Example

```
mtu 1280
```

name

Description

Set the interface name or alias as it appears in log messages and user interfaces.

Syntax

name *string*

string is the new name of the interface.

Example

```
name publicservers
```

pppoe

Description

Configure the external interface to negotiate PPPoE with the ISP.

Syntax

pppoe auth (*reauth*) (**ac-name** *acname*) (**auth-timeout** *timeout*) (**service-name** *serv*)

Configure PPPoE authentication settings.

reauth is the allowed number of authentication retries from 0 to 20.

acname is the Access Concentrator Name.

timeout is the number of seconds between each connection attempt from 0 to 60.

serv is the PPPoE Service Name.

Use **no pppoe auth** with any of the previous parameters to disable the setting.

pppoe auto-reboot enable (*day*) (*hour*) (*minute*)

Configure a scheduled automatic restart of the PPPoE session.

day is the day of the week to restart. It must be one of these options:

- **0** — Sunday
- **1** — Monday
- **2** — Tuesday
- **3** — Wednesday
- **4** — Thursday
- **5** — Friday
- **6** — Saturday
- **7** — Daily

hour is the hour of the day to restart. It must be an integer from 0 to 23.
minute is the minute of the hour to restart. It must be an integer from 0 to 59.

Use **no pppoe auto-reboot enable** to disable automatic restart.

pppoe connection (*type*) (*time*)

Configure PPPoE connection settings.

type must be either: **always-on** or **dial-on-demand**.

time must be one of these settings:

if *type* is **always-on**, *time* is the auto-reconnect time in seconds from 0 to 3600.
if *type* is **dial-on-demand**, *time* is the inactivity timeout in minutes from 0 to 60.

pppoe host-uniq enable

Enable the host-uniq tag in PPPoE discovery packets.

Use **no pppoe host-uniq enable** to disable the host-uniq tag.

pppoe lcp-echo enable (*retries*) (**lcp-timeout** *lcptimeout*)

Configure the use of LCP echo requests to detect lost PPPoE connections.

retries is the number of LCP retries in seconds from 1 to 60.

lcptimeout is the LCP echo timeout in seconds from 1 to 1200.

Use **no pppoe lcp-echo enable** to disable LCP echo requests.

pppoe static-ip (*ipaddress*) [**send-ip enable**] [**force-ip enable**]

Configure a static IP address.

ipaddress is a static IP address used for PPPoE.

send-ip enable - enables the Firebox to send the static IP address to the PPPoE server during PPPoE negotiation. This is enabled by default when you configure a static IP address.

Use **no pppoe static-ip** to remove the static IP address and get an IP address automatically.

Use **no pppoe static-ip send-ip enable** if you do not want the Firebox to send the static IP address to the PPPoE server during PPPoE negotiation.

force-ip enable - enables the Firebox to enforce the use of the configured static IP address even if another IP address is obtained from the server.

Use **no pppoe static-ip force-ip enable** if you do not want to enforce the use of the configured static IP address.

pppoe user-info (*username*) (*password*)

Configure the user login information.

username is the PPPoE user name.

password is the PPPoE password.

pppoe use-peer-dns enable

Enable the Firebox to negotiate DNS with the PPPoE server.

Use **no pppoe use-peer-dns enable** if you do not want the Firebox to negotiate DNS with the PPPoE server.

Example

```
pppoe user-info myuser mypasswd
pppoe static-ip 100.100.100.10
pppoe connection always-on 30
pppoe auth 3 ac-name concentrator1 auth-timeout 10
pppoe auth service-name serviceA
pppoe connection dial-on-demand 60
no pppoe auth ac-name
pppoe auto-reboot enable day 3
pppoe auto-reboot enable hour 2
pppoe lcp-echo enable 3 lcp-timeout 30
```

qos

Description

Configure Quality of Service settings for the interface.

Syntax

qos marking dscp (*state*) (**priority-method** *method*)

state is the DSCP state and must be one of these values: **assign** *type*, **clear**, or **preserve**.

If *state* is *assign*, you must add a string for *type*.

type is the DSCP assign method and must be one of these values: **Best-effort**, **CS1-Scavenger**, **AF11**, **AF12**, **AF13**, **CS2**, **AF21**, **AF22**, **AF23**, **CS3**, **AF31**, **AF32**, **AF33**, **CS4**, **AF41**, **AF42**, **AF43**, **CS5**, **EF**, **Control-CS6**, or **Control-CS7**.

method is the method used to assign priority and must be one of these values: **No_Priority**, **Customer**, or **Mapped-from-Marking**.

qos marking precedence (*state*) (**priority-method** *method*)

state is the precedence state and must be one of these values: **assign** *value*, **clear**, or **preserve**.

If *state* is **assign**, you must add a string for *value*.

value is the precedence value. It must be an integer from 0 to 7.

method is the method used to assign priority and must be one of these values: **No_Priority**, **Customer**, or **Mapped-from-Marking**.

qos max-link-bandwidth (*value*)

value is the maximum link bandwidth in bytes. It must be an integer from 0 to 1,000,000.

Example

```
qos marking dscp assign best-effort priority-method mapped-from-marking
qos marking precedence clear
qos max-link-bandwidth 500000
```

secondary

Description

Configure a secondary network on the interface.

Syntax

secondary (*address*)

address must be one of these options: *addr mask* or *net*

addr is an IP address, and must be in the format of A.B.C.D.

mask is an IP subnet mask, and must be in the format of A.B.C.D.

net is the IP address and subnet prefix in the format of A.B.C.D/# where # must be in the range of 0 to 32.

This command can take multiple address entries.

Use **no secondary** to remove all secondary addresses from this interface.

Example

```
secondary 100.100.101.0 255.255.255.0
secondary 100.100.101.0/24
secondary 100.100.101.0/24 100.100.103.0/24
```

system-dhcp

Description

Configure a trusted or optional interface to use the same DHCP settings you configured for drop-in mode. This command is available only when drop-in mode is enabled.

Syntax

system-dhcp enable

Enable the interface to use the same DHCP settings configured for drop-in mode.

Use **no system-dhcp enable** to disable DHCP for the interface.

type

Description

Set the interface type

Syntax

type (*option*)

option must be one of these options: **trusted**, **optional**, **custom**, or **external** *addressmethod*

If option value is **external**, you must add the parameter *addressmethod* whose value is: **default-gw** *gateway*, **dhcp**, or **pppoe**.

If *addressmethod* is **default-gw**, you must add the parameter *gateway*.

gateway is IP address of the default gateway. In Fireware v11.9 and lower, it must be on the same subnet as the IP address assigned to the interface. In Fireware v11.9.1 and higher, it can be on a different IP address than the interface IP address.

Example

```
type trusted

type external default-gw 100.100.101.0/24
```

v6

Description

Configure IPv6 settings for an interface. You must use the **ip ip-node-type** command to enable IPv6 for the interface before you can configure IPv6 settings.

Syntax

v6 advert [**max-rtr-interval** *max-rtr*] [**min-rtr-interval** *min-rtr*] [**life-time** *default-life-time*] [**reachable-time** *reachable-time*] [**retrans-time** *retrans-time*]

Configure the IPv6 router advertisement settings for an trusted, optional, or custom interface.

max-rtr is the maximum time allowed between sending unsolicited multicast router advertisements from the interface. It must be an value from 4 to 1800 seconds. Default is 600 seconds.

min-rtr is the minimum time allowed between sending unsolicited multicast router advertisements from the interface. It must be a value from 3 to 1350 seconds. Default is 200 seconds.

default-life-time is the lifetime associated with the default router. It must be a value from 0 to 9000 seconds. Default is 1800 seconds.

reachable-time is the reachable time of a neighbor. It must be a value from 0 to 3600000 milliseconds. Default is 30000 milliseconds

retrans-time is the transmitted time. It must be a value from 0 to 10000 milliseconds. Default is 1000 milliseconds.

v6 advert (*option* **enable**)

Configure prefix advertisement options for a trusted, optional, or custom interface.

option must be one of these values:

send-advert — Enable the device to send periodic router advertisements and respond to router solicitations.

hop-limit — Enable : A flag indicating whether sends hop limit.

manage-flag — Enable the device to use the administered (stateful) protocol for address auto configuration in addition to any addresses auto configured using stateless address auto configuration

other-flag — Enable the device to use the administered (stateful) protocol for auto configuration of other (non-address) information

Use **no v6 advert** *option* **enable** to disable any of these options.

v6 advert prefix (**address***address*) [*prefix-name*] [**valid-life-time** *valid-life-time*] [**preferred-lifetime** *preferred-lifetime*] [**autonomous enable**] [**onlink enable**]

Add a prefix advertisement to a trusted, optional, or custom interface.

address is the IPv6 address. It must be in the format A:B:C:D:E:F:G:H/I.

prefix-name is the name of a delegated prefix. For example, **eth0_prefix**.

valid-life-time is the length of time after the packet is sent that the prefix is valid for the purpose of on-link determination. It must be a value from 1 to 4294967295 seconds. The default value is 2592000 seconds (30 days).

preferred-lifetime is the length of time after the packet is sent that addresses generated from the prefix via stateless address autoconfiguration remain preferred. It must be a value from 1 to 4294967295. The default value is 604800 seconds (7 days).

autonomous enable — enable the prefix to be used for autonomous address configuration

onlink enable — enable the prefix to be used for on-link determination

v6 autoconf enable

Enable IPv6 address autoconfiguration on an external interface. When autoconfiguration is enabled, the Firebox automatically assign an IPv6 link-local address to the interface. IPv6 autoconfiguration is disabled by default.

Use **no v6 autoconf enable** to disable IPv6 address autoconfiguration.

v6 dhcp enable

Enable the DHCPv6 client on an external interface.

Use **no v6 dhcp enable** to disable the DHCPv6 client.

v6 dhcp rapid-commit enable

Enable the external interface to use a rapid two-message exchange to get an IPv6 address.

Use **no dhcp rapid-commit enable** to disable rapid commit.

v6 dhcp prefix-delegation enable

Enable the external interface as a client for DHCPv6 prefix delegation.

When you enable client prefix delegation, you can use the delegated prefix to configure IPv6 addresses on your private networks. The delegated prefix name begins with the external interface device name. For example, if you enable DHCPv6 client prefix delegation on interface 0, the delegated prefix name is **eth0_prefix**.

Use **no dhcp prefix-delegation enable** to disable prefix delegation in the DHCP client.

v6 dhcp prefix-delegation rapid-commit enable

Enable an external interface to use a rapid two-message exchange to get a delegated prefix.

Use **no dhcp prefix-delegation rapid-commit enable** to disable rapid commit.

v6 dhcp server (**start-addr** [*start-prefix-name*] *start-ip* [*end-prefix-name*] *end-ip*) | (**start--prefix** *start-prefix end-prefix prefix-length*) | (**reservation** *reserved_hostname reserved-duid (reserved-ip* | *reserved-prefix* | (*prefix-name reserved-ip*))) | [**domain** *domain-name*] [**dns-server** *dns-server-ip*] | [**sip-server** *sip-server-ip*] | [**sip-domain** *sip-domain-name*] | (**preferred-life-time** *preferred-life*) | (**valid-life-time** *valid-life*) | (**rapid-commit enable**)

Configure a trusted or optional interface as a DHCPv6 server for computers that connect to that interface. When you define a DHCPv6 address pool, the DHCPv6 server is automatically enabled on the interface.

If the external interface is enabled as a prefix delegation client, you can use the delegated prefix name to configure the DHCPv6 server address pool or reserved DHCP addresses to use the delegated prefix.

start-addr — Specify a DHCPv6 address pool. You can define up to 256 non-overlapping IPv6 address ranges. Starting and ending IPv6 addresses for each range must be on the same subnet. The IPv6 addresses in the pool must have the same prefix as one of the interface's IPv6 addresses. Do not include the interface IPv6 address in the address pool.

start-addr [*start-prefix-name*] *start-ip* [*end-prefix-name*] *end-ip*

start-prefix-name is a delegated prefix name to use with the *start-ip*. For example **eth0_prefix**.

start-ip is the first address in the DHCPv6 address range. It must be in the format <A:B:C:D:E:F:G:H>, <A::G:H> or <::H>.

end-prefix-name is the name of the delegated prefix to use with the *end-ip*. For example **eth0_prefix**.

*end-ip*is the last address in the DHCPv6 address range. It must be in the format <A:B:C:D:E:F:G:H>, <A::G:H> or <::H>.

start-prefix — Specify a DHCP prefix pool for prefix delegation.

start--prefix *start-prefix end-prefix prefix-length*

start-prefix is a first prefix in the prefix pool range. It must be in the format <A:B:C:D:E:F:G:H>, <A::G:H> or <::H>.

end-prefix is the last prefix in the prefix pool range. It must be in the format <A:B:C:D:E:F:G:H>, <A::G:H> or <::H>.

prefix-length is the prefix length. It must a value between 1 and 127.

reservation — Specify a reserved IP addresses or prefix for an IPv6 client. You can use the reservation option multiple times in the same command.

reservation *reserved_hostname reserved-duid (reserved-ip* | *reserved-prefix* | (*prefix-name reserved-ip*))

reserved-hostname is the reservation name.

reserved-duid is the DHCPv6 Client DUID. You must use colons (:) to separate each part of the DUID.

reserved-ip is the IPv6 IP address to reserve for this client. It must have the same prefix as one of the interface's IPv6 addresses.

*reserved-prefix*is the prefix to reserve for this DUID client.

prefix-name is the name of the delegated prefix to use with the IPv6 IP address reserved for this client. For example, *eth0_prefix*.

domain — Specify a DNS server domain name to assign to DHCP client devices on the network.

domain-name is a domain name, such as example.com

dns-server — Specify a DNS server to use. You can use the dns-server option up to three times in the same command.

dns-server-ip is the IPv6 address of a DNS server. It must be in the format A:B:C:D:E:F:G:H.

sip-server — Specify the SIP server IP address to provide to clients that request it.

sip-server-ip is the IPv6 address of a SIP server. It must be in the format A:B:C:D:E:F:G:H.

sip-domain — Specify the SIP server domain to provide to clients that request it.

sip-domain-name is a SIP domain name, such as example.com.

preferred-life-time — Specify the length of time that an assigned IPv6 address is preferred. The default value is 24 hours.

preferred-life is the duration, in hours, that addresses leased to devices on the network are preferred. It must be less than or equal to the *valid-life*.

valid-life-time — Specify the length of time that addresses leased to devices on the network are valid. The default value is 48 hours.

valid-life is the duration, in hours, that IPv6 addresses are valid. It must be greater than or equal to the *preferred-life*.

rapid-commit enable — Enable the DHCP server to use the rapid two-message exchange to assign an IP address.

Use **no v6 dhcp server** with the same options to remove any configured DHCPv6 server settings.

v6 ip (**address** [*prefix-name*] *address*) [**advert-prefix enable**]

Set the IPv6 address for an interface.

prefix-name is the name of a delegated prefix to use for this IP address. For example, **eth0_prefix**.

address is the IPv6 address and subnet prefix to assign to the interface. It must be in the format A:B:C:D:E:F:G:H/I.

advert-prefix enable — For a trusted, optional, or custom interface, enables prefix advertisement on this interface and adds the prefix for the specified *address* to the prefix advertisement list.

use **no v6 ip address** (*address*) to remove the specified IPv6 address for this interface.

v6 ip (**default-gw** *gateway*)

Configure the IPv6 default gateway for an external interface.

gateway is the IPv6 address of the default gateway. It must be in the format A:B:C:D:E:F:G:H.

v6 (**hop-limit** *hop-limit*)

Configure the IPv6 hop limit for an interface.

hop-limit must be an integer from 0 to 255. Default value is 64.

v6 (**dad-transmit** *dad-transmit*)

Configure the DAD (Duplicate Address Detection) transmit setting for an interface.

dad-transmit is the number of DAD transmits. It must be an integer between 0 and 10. If set to 0, duplicate address detection is not performed. Default value is 1.

Example

```
v6 ip address 2001::4545:3:200:F8FF:FE21:67CF/64 advert-prefix enable

v6 ip address eth0_prefix ::450/64

v6 ip default-gw 2001:4545:3:300:32CB::D837:FC76:12FC

v6 advert max-rtr-level 1000 min-rtr-level 200 default-life-time 1800
reachable-time 35000 retrans-time 1500

v6 advert prefix-address 2001::4545:3:200:F8FF:FE21:67CF/64 onlink enable

v6 dhcp server start-ip 2001::100 2001::200

v6 advert hop-limit enable

v6 mtu 1500

v6 hop-limit 64

v6 dad-transmit 1
```

vpn-pmtu

Description

Configure PMTU settings for IPSec for an external interface.

Syntax

vpn-pmtu (**minimum-size** *size*) (**life-time** *time*)

size is the minimum MTU in bytes from 68 to 1550; default is 512.

time is the aging time of learned PMTU in seconds from 60 to 2147483647; default is 600.

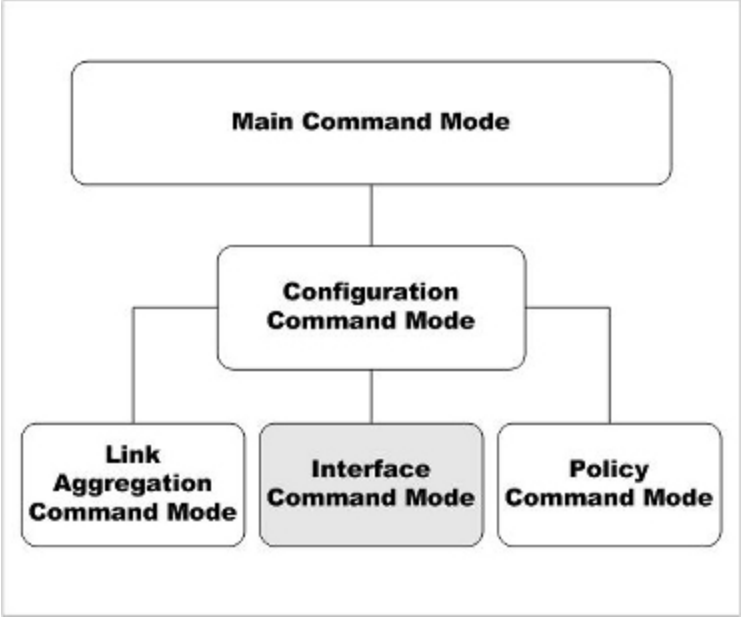
Example

```
vpn-pmtu minimum-size 768 life-time 1200
```

7 Link Aggregation Command Mode

Link Aggregation Commands

The WatchGuard Command Line Interface (CLI) Link Aggregation command mode is used to configure link aggregation interfaces for your Firebox.



In Link Aggregation command mode, you can:

- Add and remove link aggregation member interfaces
- Configure the link aggregation interface mode
- Configure the IP address and addressing options for the link aggregation interface
- Configure the link aggregation interface as a gateway

- Control link speed
- Configure the link aggregation interface as a DHCP server or DHCP relay

Enter Link Aggregation Command Mode

To enter the Link Aggregation command mode:

1. Open the CLI in the Configuration command mode.
2. Type the link-aggregation <la-name> command, where <la-name> is the name of the link aggregation interface.
3. Press **Enter**.
   In Link Aggregation Interface command mode, the CLI prompt changes to WG(config/link-aggregation-<la-name>)# where <la-name> is the selected link aggregation interface.

You can configure only a single link aggregation interface at a time. To configure another link aggregation interface, exit Link Aggregation command mode. From the Configuration mode, use the link-aggregation command again to configure another link aggregation interface.

List of Link Aggregation Mode Commands

You can use all common commands in Link Aggregation Interface command mode. Many of these commands are similar to commands available in Interface mode.

Command	Usage
dhcp	Enable the interface as either a DHCP server or relay.
enable	Enable or disable the physical interface.
ip	Configure the IP address and addressing options for the interface.
link-speed	Set the link speed and duplex for the interface.
member	Add a physical interface to this link aggregation interface
mode	Configure the link aggregation interface mode
mtu	Control the interface MTU settings.
pppoe	Configure the Point-to -Point over Ethernet Protocol for the external interface.
secondary	Configure the secondary IP addresses for the link aggregation interface
security-zone	Set the link aggregation interface security zone
system-dhcp	Configure a trusted or optional interface to use the same DHCP settings you configured for drop-in mode.

Link Aggregation Command Mode Reference

dhcp

Description

Enable the link aggregation interface as either a DHCP server or relay. Or, configure an external link aggregation interface as a DHCP client to dynamically get an IP address from an external DHCP server.

Syntax

dhcp relay (*serverip*) [*serverip*] [*serverip]*

Configure a trusted, optional, or custom interface to relay DHCP requests to the specified server.

serverip is the IP address of a DHCP server that is used for computers on the interface. You can specify the IP addresses up to three DHCP servers. The Firebox sends DHCP requests to the IP addresses of all DHCP servers you specify.

Use **no dhcp enable** to disable DHCP relay on the interface.

dhcpserver (**start-addr***startipendipleasetime*) [**dns-server***dns*...] [**domain** *domainname*] [**reservation***resvnamemacaddressipaddress*] [**wins***wins*...]

Configure a trusted, optional, or custom link aggregation interface as a DHCP server for computers on that interface.

start-addr defines a DHCP address pool. In the same line, you can use the start-addr command multiple times with these parameters:

startip is the first IP address in the DHCP address pool.

endip is the last IP address in the DHCP address pool.

leasetime is the duration in hours that addresses are leased to devices on the network. The value must be an integer.

dns is the IP address of one or more valid DNS servers.

domainname is the DNS domain name used by devices on the network.

reservation defines a pair of MAC address and IP address that are reserved within the DHCP address pool. In the same line, you can use the reservation command multiple times with these parameters:

resvname is a string to identify a reserved address.

macaddress is the MAC address of the device with a reserved address.

ipaddress is the IP address assigned to the reserved address.

wins is the IP address of one or more valid WINS servers.

Use **no dhcp enable** to disable DHCP server on the interface.

dhcp *option*

Configure a predefined DHCP option. DHCP options are used by many VoIP phones.

option must be one of these predefined options:

capwap-ac-v4 *ipaddress* specifies the IP address of a CAPWAP access controllers. You can specify multiple IP addresses, separated by spaces. This corresponds to DHCP option 138 (CAPWAP access controller).

dhcp-state *state* specifies the DHCP state. This is used by ShoreTel phones for an FTP boot option. This corresponds to DHCP option 156 (DHCP state).

sip-server *ipaddress* specifies the IP address of a Session Initiation Protocol (SIP) server. You can specify multiple IP addresses, separated by spaces. This corresponds to DHCP option 120 (SIP servers).

[**tftp-server***address*] specifies the IP address or domain name of the TFTP server where a DHCP client can download the boot configuration. *address* can be a domain name or an IP address. This corresponds to DHCP option 66 (TFTP server name) and option 150 (TFTP server IP address).

[**tftp-boot-file***bootfile*] specifies the name of the boot file. This corresponds to DHCP option 67 (boot file name).

time-offset *seconds* specifies the time offset in seconds from Coordinated Universal Time (UTC). This corresponds to DHCP option 2 (time offset).

vendor-spec *option* specifies vendor-specific information. This corresponds to DHCP option 43 (vendor specific information).

dhcp custom-option *option-code option-name option-type value*

Configure a custom DHCP option, as described in RFC 2132. If you configure more than one interface to use the same DHCP option code, the *option-type* must be the same on each interface.

option-code is the DHCP option code. It must be an integer from 1 - 255. DHCP options 1, 3, and 28 are not supported.

name is a name to describe this DHCP option

option-type is the type of value required by this option. It must be one of these types:

boolean Specify a Boolean DHCP option value (true or false)

four-byte-integer Specify a DHCP option value as a four bytes integer

hexadecimal Specify the DHCP option value as a hexadecimal number

ip-address-list Specify the DHCP option value as a list of IP addresses, separated by spaces

one-byte-integer Specify the DHCP option value as a one byte integer

text Specify the DHCP option value as a text string

two-byte-integer Specify the DHCP option value as a two bytes integer

unsigned-four-byte-integer Specify the DHCP option value as an unsigned four bytes integer

unsigned-one-byte-integer Specify the DHCP option value as an unsigned one byte integer

unsigned-two-byte-integer Specify the DHCP option value as an unsigned two bytes integer

value is the value to assign to the option. The value must match the type specified in *type*.

dhcp any (*leasetime*)

Configure an external link aggregation interface to get a DHCP-assigned IP address from the ISP.

leasetime is the duration in hours that addresses are leased to devices on the network. The value must be an integer.

Use **no dhcp** to disable DHCP client on the interface.

dhcp [**host-id** *hostid*] [**host-name** *hostname ipaddress leasetime*]

Configure detailed DHCP client settings for an external link aggregation interface.

hostid is the Host ID to use to negotiate an IP address from the DHCP server.

hostname is the Host Name to use to negotiate an IP address from the DHCP server.

ipaddress is to force the DHCP server to lease a specific IP address.

leasetime is the duration in hours that addresses are leased to devices on the network. The value must be an integer.

Use **no dhcp** *host-name host-id lease-time* to disable detailed DHCP client on the interface.

dhcp release

For an external link aggregation interface, release the IP address assigned by DHCP.

dhcp renew

For an external link aggregation interface, renew the IP address assigned by DHCP.

Example

```
dhcp relay 10.0.1.254

dhcp server start-addr 10.0.1.2 10.0.1.30 8

dhcp server start-addr 10.0.1.2 10.0.1.30 8 dns-server 203.23.124.1
203.23.124.2 domain example.com reservation ceo 00:44:FF:33:00:AC 10.0.1.35
wins 10.0.1.100
```

ip

Description

Configure the address and addressing options for the interface.

Syntax

ip address (*option*)

Set the IP address of a link aggregation interface.

option must be one of these options: (*addr mask*) or *net*

addr is an IP address, and must be in the format of A.B.C.D.

mask is an IP subnet mask, and must be in the format of A.B.C.D.

net is the IP address and subnet prefix in the format of A.B.C.D/#, where # must be in the range of 0 to 32.

ip ip-node-type (*option*)

Configure whether to enable IPv6 addressing on the interface.

option must be one of these options:

ip4-only — use the configured IPv4 address only.

ip4-6 — enable an IPv6 address for this interface in addition to the configured IPv4 address. When you select this option, Fireware assigns a link-local IPv6 address to that interface, when the interface is active. Use the show interface command to see the assigned IPv6 address.

Example

```
ip address 192.168.116.1 255.255.255.0

ip address 192.168.116.1/24

ip ip-node-type ip4-6
```

link-speed

Description

Set the link aggregation interface link speed and duplex.

Syntax

link-speed (*option*)

option must be one of these options:

10-full — Force 10 Mbps full-duplex operation

10-half — Force 10 Mbps half-duplex operation

100-full — Force 100 Mbps full-duplex operation

100-half — Force 100 Mbps half-duplex operation

1000-full — Force 1000 Mbps full-duplex operation

1000-half — Force 1000 Mbps half-duplex operation

auto-negotiate — Automatically negotiate the speed and duplex.

For some devices, not all interfaces support 1000 Mbps link speed. Make sure that all member interfaces support the link speed you configure. For a description of which interfaces support a link speed of 1000 Mbps, see the Hardware Guide for your device.

Example

```
link-speed 100-full
```

member

Description

Configure link aggregation interface members.

Syntax

member (*if-number if-number* ...)

if-number is the interface number of the physical interface to add as a member of the link aggregation interface. You can specify more than one interface number.

The interfaces you specify must already be enabled.

Example

```
if-number 10 11
```

mode

Description

Configure the link aggregation interface mode.

Syntax

mode (*la-mode*)

la-mode is the link aggregation interface mode. It must be one of these options:

active-backup — In this mode, at most only one member interface in the link aggregation group is active at a time. The other member interfaces in the link aggregation group become active only if the active interface fails. This is the default mode.

dynamic — In dynamic (802.3ad) link aggregation mode, all physical interfaces that are members of the link aggregation interface can be active. The physical interface used for traffic between any source and destination is selected based on Link Aggregation Control Protocol (LACP), as described in the IEEE 802.3ad dynamic link aggregation specification.

Dynamic link aggregation mode is not supported on XTM 25, XTM 26, and XTM 33 devices.

static — All physical interfaces that are members of the link aggregation interface can be active. The same physical interface is always used for traffic between a given source and destination based on source/destination MAC address and source/destination IP address. This mode provides load balancing and fault tolerance.

To use **dynamic** or **static** link aggregation mode, you must also configure the connected switches to use the same mode. To use Active-backup mode it is not necessary to enable link aggregation on your switches.

Example

```
mode active-backup
```

mtu

Description

Set the Maximum Transmission Unit value of a link aggregation interface.

Syntax

mtu (*size*)

size is the size in bytes of the maximum transmission unit. Must be an integer from 68 to 9000.

Example

```
mtu 1024
```

override-mac

Description

Override the MAC address for an external link aggregation interface.

If your ISP uses a MAC address to identify your computer, you must change the MAC address for the external link aggregation interface to the MAC address your ISP expects. Use the MAC address of the cable modem, DLS modem, or router that connects directly to the ISP.

Syntax

override-mac (*mac-address*)

mac-address is the MAC address to use. It must be a valid MAC address in the format <01:23:45:67:89:ab>.

pppoe

Description

Configure the external interface to negotiate PPPoE with the ISP.

Syntax

pppoe auth (*reauth*) (**ac-name** *acname*) (**auth-timeout** *timeout*) (**service-name** *serv*)

Configure PPPoE authentication settings.

reauth is the allowed number of authentication retries from 0 to 20.

acname is the Access Concentrator Name.

timeout is the number of seconds between each connection attempt from 0 to 60.

serv is the PPPoE Service Name.

Use **no pppoe auth** with any of the previous parameters to disable the setting.

pppoe auto-reboot enable (*day*) (*hour*) (*minute*)

Configure a scheduled automatic restart of the PPPoE session.

day is the day of the week to restart. It must be one of these options:

0 — Sunday
1 — Monday
2 — Tuesday
3 — Wednesday
4 — Thursday
5 — Friday
6 — Saturday
7 — Daily

hour is the hour of the day to restart. It must be an integer from 0 to 23.

minute is the minute of the hour to restart. It must be an integer from 0 to 59.

Use **no pppoe auto-reboot enable** to disable automatic restart.

pppoe connection (*type*) (*time*)

Configure PPPoE connection settings.

type must be either: **always-on** or **dial-on-demand**.

time must be one of these settings:

if *type* is **always-on**, *time* is the auto-reconnect time in seconds from 0 to 3600.
if *type* is **dial-on-demand**, *time* is the inactivity timeout in minutes from 0 to 60.

pppoe host-uniq enable

Enable the host-uniq tag in PPPoE discovery packets.

Use **no pppoe host-uniq enable** to disable the host-uniq tag.

pppoe lcp-echo enable (*retries*) (**lcp-timeout** *lcptimeout*)

Configure the use of LCP echo requests to detect lost PPPoE connections.

retries is the number of LCP retries in seconds from 1 to 60.

lcptimeout is the LCP echo timeout in seconds from 1 to 1200.

Use **no pppoe lcp-echo enable** to disable LCP echo requests.

pppoe static-ip (*ipaddress*) [**send-ip enable**]

Configure a static IP address.

ipaddress is a static IP address used for PPPoE.

send-ip enable - enables the Firebox to send the static IP address to the PPPoE server during PPPoE negotiation. This is enabled by default when you configure a static IP address.

Use **no pppoe static-ip** to remove the static IP address and get an IP address automatically.

Use **no pppoe static-ip send-ip enable** if you do not want the Firebox to send the static IP address to the PPPoE server during PPPoE negotiation.

pppoe user-info (*username*) (*password*)

Configure the user login information.

username is the PPPoE user name.

password is the PPPoE password.

pppoe use-peer-dns enable

Enable the Firebox to negotiate DNS with the PPPoE server.

Use **no pppoe use-peer-dns enable** if you do not want the Firebox to negotiate DNS with the PPPoE server.

Example

```
pppoe user-info myuser mypasswd
pppoe static-ip 100.100.100.10
pppoe connection always-on 30
pppoe auth 3 ac-name concentrator1 auth-timeout 10
pppoe auth service-name serviceA
pppoe connection dial-on-demand 60
no pppoe auth ac-name
pppoe auto-reboot enable day 3
pppoe auto-reboot enable hour 2
pppoe lcp-echo enable 3 lcp-timeout 30
```

secondary

Description

Configure a secondary network on the interface.

Syntax

secondary (*address*)

address must be one of these options: *addr mask* or *net*

addr is an IP address, and must be in the format of A.B.C.D.

mask is an IP subnet mask, and must be in the format of A.B.C.D.

net is the IP address and subnet prefix in the format of A.B.C.D/# where # must be in the range of 0 to 32.

This command can take multiple address entries.

Use **no secondary** to remove all secondary addresses from this interface.

Example

```
secondary 100.100.101.0 255.255.255.0
secondary 100.100.101.0/24
secondary 100.100.101.0/24 100.100.103.0/24
```

security-zone

Description

Configure the required settings for a link aggregation interface. For a new link aggregation interface, you must use this command first, to create the basic interface configuration before you can use other link aggregation command mode commands.

Syntax

security-zone (*int-type*) (*address*) (**member** *if-number if-number ...*)

Configure the settings for a new link aggregation interface

int-type is the interface type. It must be one of these options: **external**, **trusted**, or **optional**.

address is the IP address to assign to the link aggregation interface.

For a **trusted** or **optional** interface, it is either an address with mask in the format of A.B.C.D A.B.C.D. or a net in the format of A.B.C.D/# where # must be in the range of 8 to 30.

For an **external** interface it must be one of these options: **static-ip**, **dhcp** or **pppoe**.

If *address* is **static-ip** you must also specify the static *ipaddress*. It is either an address with mask in the format of A.B.C.D A.B.C.D. or a net in the format of A.B.C.D/# where # must be in the range of 8 to 30.

If *address* is **pppoe**, you must also specify the PPPoE *username* and *password*.

If *address* is **dhcp**, use the **dhcp** command to configure dhcp settings.

if-number is the interface number of the physical interface to add as a member of the link aggregation interface. The interface you specify must already be enabled.

You can specify more than one interface as a member of the link aggregation interface.

After you configure a link aggregation interface to use PPPoE, use the **pppoe** command to configure other PPPoE options.

Example

```
security-zone optional 10.0.20.1/24 member 4 5
```

system-dhcp

Description

Configure a trusted, optional, or custom interface to use the same DHCP settings you configured for drop-in mode. This command is available only when drop-in mode is enabled.

Syntax

system-dhcp enable

Enable the interface to use the same DHCP settings configured for drop-in mode.

Use **no system-dhcp enable** to disable DHCP for the interface.

v6

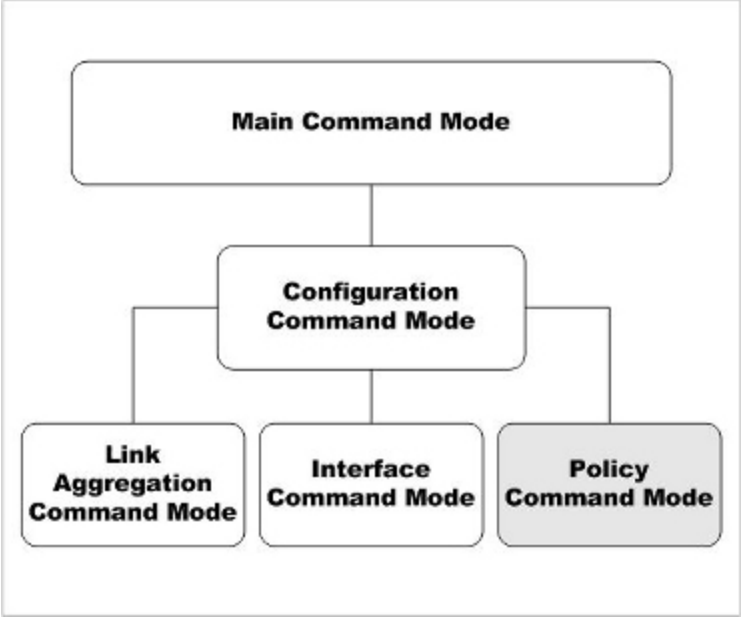
Configure IPv6 settings for the VLAN interface. You must use the **ip ip-node-type** command to enable IPv6 for the interface before you can configure IPv6 settings.

The available v6 command options for DHCPv6 are the same as for a physical interface. For more information, see the *v6*

8 Policy Command Mode

Policy Commands

The WatchGuard Command Line Interface (CLI) Policy command mode is used for system and network configuration of your Firebox.



In the Policy mode, you can:

- Create and modify policies and schedules
- Manage user accounts
- Define user, groups and aliases for use in policies
- Control branch office VPN gateways and tunnels

- Configure branch office and mobile user VPN policies
- Configure Subscription Service global settings

Enter the Policy Command Mode

To enter the Policy command mode:

1. Open the CLI in the Configuration command mode.
2. Type the **policy** command.
3. Press **Enter**.
   The CLI prompt changes to WG(config/policy)#.

*For most policy commands, you must use the **Apply** command to save and apply your policy changes to the Firebox configuration.*

List of Policy Mode Commands

You can use all common commands in the Policy command mode. For more information, see *About Common Commands* on page 17.

In addition, these commands are available only in the Policy mode:

Command	Usage
alias	Create aliases for a group of hosts, networks, or interfaces.
antivirus	Configure Gateway AntiVirus settings.
apply	Save a newly added or edited configuration.
apt-blocker	Configure settings for the APT Blocker service.
auth-server	Configure authentication server settings.
auth-user-group	Define user groups for authentication.
bovpn-gateway	Configure a branch office VPN gateway policy.
bovpn-tunnel	Configure a branch office VPN tunnel policy.
bovpn-vif	Configure a branch office VPN virtual interface.
bovpntls-client	Configure client settings for a branch office VPN over TLS server.
dns-proxy	Configure a DNS Proxy policy.
dynamic-nat	Enable a dynamic NAT policy for traffic through specific interfaces.
explicit-proxy	Configure an Explicit Proxy policy.
ftp-proxy	Configure an FTP Proxy policy.

Command	Usage
geolocation	Configure the geographic location of connections.
http-proxy	Configure an HTTP Proxy policy.
https-proxy	Configure an HTTPS Proxy policy.
l2tp	Configure Mobile VPN with L2TP.
mvpn-ikev2	Configure Mobile VPN with IKEv2.
mvpn-ipsec	Configure Mobile VPN with IPSec groups.
mvpn-rule	Configure Mobile VPN with IPSec policy rules.
one-to-one-nat	Create a 1-to-1 NAT table.
policy-tag	Configure policy tags.
policy-type	Create a custom policy template.
pop3-proxy	Configure a POP3 Proxy policy.
proposal	Create Phase 2 proposals for IPSec VPN.
quarantine-server	Configure the location of a Quarantine Server.
reputation-enabled-defense	Configure feedback settings for Reputation Enabled Defense.
rule	Configure the rules of the security policy.
schedule	Build a schedule for use in policies.
sip-proxy	Configure a SIP Proxy policy.
smtp-proxy	Configure an SMTP Proxy policy.
spamblocker	Configure global settings for the spamBlocker service.
sslvpn	Configure the device to enable Mobile VPN with SSL connections.
traffic-management	Configure a traffic management action to use with policies.
user-group	Define a user group for Firebox authentication.
users	Define a user for Firebox authentication.
webblocker	Configure global settings for the WebBlocker service.

Policy Command Mode Reference

*For most policy commands, you must use the **Apply** command to save and apply your policy changes to the Firebox configuration.*

alias

Description

Create shortcuts to identify a group of hosts, networks, or interfaces.

Syntax

alias (*name*) [**description** *desc*] (*option*)

Configure an alias for a single device, network, or IP address range.

name is the unique string that identifies the alias. You cannot use spaces.

desc is a string that describes the use of the alias. You cannot use spaces.

option must be one of these options:

host-ip (*address*)
address is the IPv4 address of a device on the network, in the format A.B.C.D.

host-range (*startip*) (*endip*)
startip is the first IP address in the range. It must be in the format A.B.C.D.

endip is the last IP address in the range. It must be in the format A.B.C.D.

host6-ip (*ipv6-address*)
ipv6-address is an IPv6 address of a device, in the format A:B:C:D:E:F:G:H.

host6-range (*ipv6-startip*) (*ipv6-endip*)
ipv6-startip is the first IPv6 address in the range. It must be in the format A:B:C:D:E:F:G:H.

ipv6-endip is the last IPv6 address in the range. It must be in the format A:B:C:D:E:F:G:H.

network-ip (*net*)
net is the IPv4 address of a device on the network. It must be in the format A.B.C.D./#, where # is a number from 0 to 32.

network6-ip (*ipv6-net*)
net is the IPv6 address of a device on the network. It must be in the format A.B.C.D.E.F.G.H/I.

FQDN (*fqdn-site*)
fqdn-site is a Fully Qualified Domain Name. This includes wildcard domains. For example: *host.example.com*, or *"*.example.com"*.

wildcard (wildcard IP address) (wildcard netmask)
wildcard is an IPv4 wildcard address and netmask. For example, you could specify 10.0.0.3 as the wildcard IP address and 255.255.0.255 as the wildcard netmask.

alias (*name*) [**description** *desc*] **tunnel-address** (**tunnel** *tunnelname*) (**address** *address*) [**device-group** *group-name* [**user-group** *type name authmethod*]

Configure an alias for a tunnel to define the user or group, address, and tunnel name.

name is the unique string that identifies the alias. You cannot use spaces.

desc is a string that describes the use of the alias. You cannot use spaces.

tunnelname is a string that identifies the tunnel.

address must be one of these options: *address*, **network-ip** (*net*), or **host-range** (*startip*) (*endip*).

address is the IP address of a device on the network. It must be in the format A.B.C.D.

net is the IP address of a device on the network. It must be in the format A.B.C.D./#, where # is a number from 0 to 32.

startip is the first IP address in the range. It must be in the format A.B.C.D.

endip is the last IP address in the range. It must be in the format A.B.C.D.

device-group defines the a mobile device group to add to the alias. *group-name* is case-sensitive and must be one of these values.

Any-Android specifies all Android devices.

Any-iOS specifies all iOS devices.

Any-Mobile specifies all iOS and Android devices.

user-group defines a user or group for the tunnel. It is composed of:

type specifies a user or group. It must be one of these options: **user** or **group**.

name is the name of a user or group as already defined on the device.

authmethod is one of these options: **Firebox-DB**, **RADIUS**, **LDAP**, **SecurID**, or **Active-Directory**.

alias (*name*) [**description** *desc*] **custom-address** (**interface** *if-name*) [**address** *tunneladdress*] [**device-group** *group-name*] [**user-group** *type name authmethod*]

Configure an alias to define the user or group, address, and an interface on the device.

name is the unique string that identifies the alias. You cannot use spaces.

desc is a string that describes the use of the alias. You cannot use spaces.

if-name is the name of the device interface.

address must be one of these options: *address*, **network-ip** (*net*), **host-range** (*startip*) (*endip*), or **FQDN** (*fqdn-site*).

address is the IP address of a device on the network. It must be in the format A.B.C.D.

net is the IP address of a device on the network. It must be in the format A.B.C.D./#, where # is a number from 0 to 32.

startip is the first IP address in the range. It must be in the format A.B.C.D.

endip is the last IP address in the range. It must be in the format A.B.C.D.

fqdn-site is a Fully Qualified Domain Name. This includes wildcard domains. For example, *host.example.com*, or *"*.example.com"*.

device-group defines the a mobile device group to add to the alias. *group-name* is case-sensitive and must be one of these values.

Any-Android specifies all Android devices.

Any-iOS specifies all iOS devices.

Any-Mobile specifies all iOS and Android devices.

user-group defines a user or group for the tunnel. It is composed of:

type specifies a user or group. It must be one of these options: **user** or **group**.

name is the name of a user or group as already defined on the device.

authmethod is one of these options: **Firebox-DB**, **RADIUS**, **LDAP**, **SecurID**, or **Active-Directory**.

alias (*name*) [**description** *desc*] (**alias** *aliasname*)

Configure an alias to another alias.

name is the unique string that identifies the alias. You cannot use spaces.

desc is a string that describes the use of the alias. You cannot use spaces.

aliasname is an alias already configured on the device.

alias (*name*) [**description***desc*] (**device-group***group-name*)

Configure an alias to a mobile device group. Device groups are populated automatically based on the device type that connects.

name is the unique string that identifies the alias. You cannot use spaces.

desc is a string that describes the use for the alias. You cannot use spaces.

device-group defines the a mobile device group to add to the alias. *group-name* is case-sensitive and must be one of these values.

Any-Android specifies all Android devices.

Any-iOS specifies all iOS devices.

Any-Mobile specifies all iOS and Android devices.

alias (*name*) [**description** *desc*] (**user-group** *type name authmethod)*)

Configure an alias to an authentication user or group.

name is the unique string that identifies the alias. You cannot use spaces.

desc is a string that describes the use for the alias. You cannot use spaces.

user-group defines a user or group for the alias. It is composed of:

type specifies a user or group. It must be one of these options: **user** or **group**.

name is the name of a user or group as already defined on the device.

authmethod is one of these options: **Firebox-DB**, **RADIUS**, **LDAP**, **SecurID**, or the domain name of an Active Directory server.

Example

```
alias ceo description jacks_box host-ip 192.168.100.23
alias tunnel_mainoffice tunnel-address tunnel headquarters address network-ip 192.168.200.0/24
alias moneyfolk user-group group accounting Active-Directory
alias mobile device-group Any-Mobile
alias retailstores description "Retail Stores" wildcard 10.0.0.3 255.255.0.255
```

antivirus

Description

Configure settings for Gateway AntiVirus.

Syntax

antivirus decompression (*level*|**enable**|**restore**)

(Fireware v12.0 and lower) Configure Gateway AntiVirus decompression settings that control scanning of compressed files. Gateway AntiVirus decompression is disabled by default.

level is the number of compression levels to scan. It must be a number between 1 and 5. The default value is three.

enable enables Gateway AntiVirus to scan inside compressed attachments.

restore Gateway AntiVirus decompression settings to default values.

antivirus settings intelligent-antivirus enable

(Fireware v12.2 and higher) Enable the IntelligentAV service.

Use **no intelligent-antivirus enable** to disable the service.

apply

Description

Apply configuration changes to the device.

Syntax

apply

No options available.

apt-blocker

Description

Configure the APT Blocker service.

Syntax

apt-blocker enable

Enable the APT Blocker service.

Use **no apt-blocker enable** to disable the service.

apt-blockerthreat-level*levelaction* [*record-method* enable]

You can configure an action for each level of APT threat.

level is the threat level the APT threat. You can choose one of these levels:

- high
- medium

- low
- clean

action is the action to take based on the threat level. You can choose one of these actions:

- Allow
- Drop
- Block
- Quarantine

[*record-method]* is the log and alarm functions. You can choose one of these options:

- log
- alarm
- both (for both log and alarm)

apt-blockerpolicy (*action*)

You can apply the APT Blocker service to a specific proxy policy.

action is the name of a policy, for example, *FTP-Server*.

apt-blocker server*enable* [**api-token** api token] **license-key** license key] [**server-name** name] [**username** user name]

You can send APT Blocker requests to a local server.

enable enables the use of a local Lastline On-Premise server.
api-token is the special API token string supplied by Lastline.
license-key is the license information supplied by Lastline.
server-name is the domain name or IP address of your local server.
username is the user name to authenticate to the local sever.

apt-blocker region (*region*)

You can send APT Blocker requests to a server in a specific region.

region must be one of these values:
any — Send APT Blocker requests to the closest Lastline server
europe — Send requests to a Lastline server in Europe

Example

```
apt-blocker enable
apt-blocker threat-level medium allow log enable
apt-blocker policy FTP-Server
apt-blocker region europe
```

apt-blocker notification

Description

Configure settings for APT Blocker notification.

Syntax

apt-blockernotification (**snmp-trap** enable | **notification** enable **action-type** action-type enable [**launch-interval** launch-interval] [**repeat-count** repeat-count])

notification — You can enable a notification in the event an APT is detected.

snmp-trap — You can enable an SNMP trap notification in the event an APT is detected.

action-type — You can set the type of notification as **email** or **pop-window**. The default is **email**.

launch-interval — Set the launch interval in minutes. The default is 15 minutes.

repeat-count — Set the repeat count for the notification. The default is 10.

Example

```
apt-blocker notification notification enable action-type email
```

auth-server

Description

Configure the device to use an authentication server.

Syntax

auth-server active-directory (*domain-name*) (*server-index*) (*address-type*) (*server-address*) (*search-base*) [**deadtime** *deadtimevalue*] [**dns-string** *dnsstring*] [**group-string** *groupstring*] [**idle-timeout-string** *idletimeout*] [**ip-string** *ipstring*] [**ldaps enable**] [**validate-cert enable**] [**lease-time-string** *leasetimestring*] [**login-attribute** *login*] [**netmask-string** *netmask*] [**password** *passwd*] [**port** *portnumber*] [**wins-string** *wins*]

Configure the Firebox to use an Active-Directory authentication server.

domain-name is the domain name of the Active Directory server.

server-index is the index of the Active Directory server. It must be one of these values:

0 — the primary Active Directory server for this domain

1 — the secondary Active Directory server for this domain, if two servers are configured

address-type must be one of these options: **IP** or **dns-name**.

server-address is the IP address or DNS name of the Active Directory server.

If *address-type* is **IP**, *server-address* must be the IP address of the Active Directory server. It must be in the format A.B.C.D.

If *address-type* is **dns-name**, *server-address* must be the DNS name of the Active Directory server.

search-base is the limits on the authentication server directories where the Firebox searches for an authentication match.

For example, if your user accounts are stored in an OU (organizational unit) you refer to as accounts, you want to limit the search to only this OU, and your domain name is mydomain.com, your search base is: ou=accounts dc=mydomain dc=com.

deadtimevalue is the duration in minutes before a dead server is marked as active again. It must be an integer from 0 to 1440. The default value is 600 seconds (10 minutes) in Fireware v12.1.1 or lower. In Fireware v12.2 or higher, the default value is 180 seconds (3 minutes).

dnsstring is the distinguished name of a search operation. The maximum number of characters is 255.

groupstring is an attribute on an LDAP server that holds user group information. The maximum number of characters is 31.

idletimeout is the amount of time that can pass before an idle Mobile VPN user is removed from the authenticated user group. It must be an integer.

ipstring is a virtual IP address assigned to Mobile VPN clients. It must be in the format A.B.C.D.

ldaps enable enables secure SSL connections to your Active Directory server.

validate-cert enable enables validation of the server certificate of the Active Directory server for LDAPS.

leasetimestring controls the absolute amount of time a user can stay authenticated.

login is the name used for the bind to the LDAP database.

netmask is the network mask used with ipstring to define a virtual IP address for assignment to Mobile VPN clients.

passwd is the password of the searching user.

portnumber is the port used to connect to the authentication server. The default value is 389.

wins is an IP address for a WINS server assigned to Mobile VPN clients.

Use **no auth-server active-directory** (*domain-name*) (*server-index*) to remove the Active Directory server.

Use **no auth-server active-directory** (*domain-name*) **ldaps enable** to disable LDAPS for the specified Active Directory server.

auth-server ldap (primary|secondary) enable (*address-type*) (*address*) (*search-base*) [**ldaps enable**] [**validate-cert enable**] [**deadtime** *deadtimevalue*] [**dns-string** *dnsstring*] [**group-string** *groupstring*] **[idle-timeout-string** *idletimeout*] [**ip-string** *ipstring*] [**lease-time-string** *leasetimestring*] [**login-attribute** *login*] [**netmask-string** *netmask*] [**password** *passwd*] [**port** *portnumber*] [**wins-string** *wins*]

Configure the Firebox to use an LDAP authentication server.

(**primary**|**secondary**) defines whether to configure a primary or secondary LDAP server.

address-type must be one of these options: **IP** or **dns-name**

address is the IP address or DNS name of the authentication server.

If *address*-type is **IP**, *address* must be the IP address of the authentication server. It must be in the format A.B.C.D.

If *address-type* is **dns-name**, *address* must be the DNS name of the primary authentication server.

search-base limits the authentication server directories where the Firebox searches for an authentication match.

For example, if your user accounts are stored in an OU (organizational unit) you refer to as accounts, you want to limit the search to only this OU, and your domain name is mydomain.com, your search base is: ou=accounts dc=mydomain dc=com

ldaps enable enable secure SSL connections to your LDAP server.

validate-cert enable enable validation of the certificate of the LDAP server.

(Fireware v12.9 or higher) **client-cert** is the client certificate ID number.

deadtimevalue is the duration in minutes before a dead server is marked as active again. It must be an integer from 0 to 1440. The default value is 600 seconds (10 minutes) in Fireware v12.1.1 or lower. In Fireware v12.2 or higher, the default value is 180 seconds (3 minutes).

dnsstring is the distinguished name of a search operation. The maximum number of characters is 255.

groupstring is an attribute on an LDAP server that holds user group information. The maximum number of characters is 31.

idletimeout is the amount of time that can pass before an idle Mobile VPN user is removed from the authenticated user group. It must be an integer.

ipstring is a virtual IP address assigned to Mobile VPN clients. It must be in the format A.B.C.D.

leasetimestring controls the absolute amount of time a user can stay authenticated.

login is the name used for the bind to the LDAP database.

netmask is the network mask used with ipstring to define a virtual IP address for assignment to Mobile VPN clients.

passwd is the password of the searching user.

portnumber is the port used to connect to the authentication server. The default value is 389.

wins is an IP address for a WINS server assigned to Mobile VPN clients.

Use **no auth-server ldap** (**primary**|**secondary**) **enable** to remove the primary or secondary LDAP server.

Use **no auth-server ldap** (**primary**|**secondary**) **ldaps enable** to disable LDAPS for the primary or secondary LDAP server.

auth-server (**radius**|**securid**) (**primary**|**secondary**) **enable** (*ipaddr*) (*secret*) [**deadtime** *deadtimevalue*] [**group** *groupnumber*] [**port** *portnumber*] [**retry** *retries*] [**timeout** *timeoutvalue*]

Configure the Firebox to use a RADIUS or SecurID authentication server.

(**radius**|**securid**) specifies whether to configure a RADIUS or SecurID server.

ipaddr is the IP address of the authentication server. It must be in the format A.B.C.D.

secret is the shared secret between the device and the authentication server.

deadtimevalue is the amount of time in minutes before a dead server is marked as active again. It must be an integer from 0 to 86400. The default value is 600 seconds (10 minutes) in Fireware v12.1.1 or lower. In Fireware v12.2 or higher, the default value is 180 seconds (3 minutes).

groupnumber is the Group Attribute value. It must be an integer from 0 to 255. The default value is 11.

portnumber is the port used to connect to the authentication server. It must be an integer from 1 to 65535. The default value is 1812.

retries is the number of times the device tries to reconnect to the server before marking it inactive. It must be an integer from 1 to 10. The default value is 3.

timeoutvalue is the duration in seconds the device waits for a response from the authentication server before it tries to connect again. It must be an integer from 1 to 120. The default value is 5.

Use **no auth-server radius** (**primary**|**secondary**) **enable** to remove the primary or secondary SecurID server.

Use **no auth-server securid** (**primary**|**secondary**) **enable** to remove the primary or secondary SecurID server.

auth-server saml (identity provider) **group-attr-name** (group attribute name)

Configure the Firebox to use SAML single sign-on and an identity provider that you specify.

By default, the *(group attribute name)* is *memberOf*.

Example

```
auth-server active-directory domain1 0 IP 192.168.110.5 dc=mydomain dc=com

auth-server active-directory domain1 1 IP 192.168.110.6 dc=mydomain dc=com

no auth-server active-directory domain1

auth-server ldap primary enable ip 192.168.110.7 dc=mydomain dc=com
secondary enable ip 192.168.110.7 dc=mydomain dc=com

auth-server ldap primary enable ip 192.168.110.50 dc=domain1 ldaps enable
validate-cert enable secondary enable ip 192.168.110.51 dc=domain2 ldaps
enable

auth-server RADIUS primary enable 192.168.110.5 authpassword deadtime 15
group 12 port 1813 retry 5 timeout 10

auth-server RADIUS secondary enable 192.168.110.6 auth2password deadtime 15
group 12 port 1813 retry 5 timeout 15

auth-server saml Okta
```

auth-user-group

Description

Create authentication users and groups in the Firebox device internal database.

Syntax

auth-user-group (*name*) (**user**|**group**) (*server*) [**description** (*desc*)] [**enable** (**unlimited**|(*limit* (*action*))]

Define an authentication group or single user.

name is a string to uniquely identify the authentication group or user.

server must be one of these options: **Any**, **Firebox-DB**, **LDAP**, **RADIUS**, or **SecurID**. Or, to use Active Directory authentication, specify the domain name of a configured Active Directory server.

desc is a string that describes the authentication group or user.

enable enables configuration of concurrent login limits for the user or group.

unlimited — Allow unlimited concurrent firewall authentication logins from the same account.

limit action — Limit the number of concurrent user sessions.

limit is the maximum number of concurrent user sessions to allow.

action is the action to take when the limit is reached. It must be one of these options:

logoff — allow subsequent login attempts and log off the first session .

reject — reject subsequent login attempts.

Example

```
auth-user-group executives group LDAP description VIPs
auth-user-group acctg group my-ad-domain.com description accounting
auth-user-group sales group Any enable 5 reject
```

bovpn-gateway

Description

Configure a branch office virtual private network (BOVPN) gateway.

Syntax

bovpn-gateway (*name*)

Assign a unique name to a BOVPN gateway.

name is a string that uniquely identifies the BOVPN gateway. The maximum number of characters is 42.

After you enter the command **bovpn-gateway** (*name*) the configuration continues to the BOVPN Gateway details command mode.

The prompt changes to: `WG(config/policy/bovpngateway-name)#`

Use the **Exit** command to exit this mode.

credential-method certificate (*id*) **addr-family IPv6** (**local-gateway** (*type*) (*interface-name*)) (*interface-ip-address*) (**remote-gateway** (*rgateway*) (*rgatewayid*)) **df** (*df-bit option*) **vpn-pmtu minimum-size** *(pmtu-size)* **life-time** *(life-time value)* [**phase1 mode** *gw-mode*]

Configure the BOVPN gateway to use a certificate for authentication. If the local and remote gateway endpoints are not yet defined, you must include the **local-gateway** and **remote-gateway** parameters in this command to configure the local and remote gateway endpoints for tunnel authentication.

id is the certificate identification number.

addr-family specifies the IP address family in Fireware v12.5 or higher. If you specify this command, the only option is **IPv6**. For IPv4, do not specify the **addr-family** command.

The **local-gateway** parameter starts the configuration of the local gateway settings.

type is the certificate ID type. It must be one of these options: **ip-address**, **domain**, **user-domain**, or **x500**. The specified certificate must contain the selected type of certificate ID information.

interface-name is the name of the external interface to use for this gateway endpoint. If you configured the wireless client as an external interface, specify the interface **WG-Wireless-Client**.

(Fireware v12.2 or higher) *interface-ip-address* is the IP address of the external interface you specified. Use **primary** to specify the primary IP address of the specified interface. Or, type an IP address that is a secondary IP address for the specified interface.

The **remote-gateway** parameter starts the configuration of the remote gateway settings

rgateway must be either: **dynamic** or *ip-address*.

ip-address is an IP address for the remote gateway in the format A.B.C.D.

rgatewayid must be one of these options:

ip-address

ip-address is an IP address for the remote gateway in the format A.B.C.D.

by-domain*methoddomainnameresolvable*

method is one of these options: **domain-name** or **user-domain**

domainname is the domain name or user domain.

resolvable specifies whether the domain is resolvable. Specify **yes** if the domain name is resolvable or **no** if it is not.

interface-name is the name of the external interface to use for this gateway endpoint. If you configured the wireless client as an external interface, specify the interface **WG-Wireless-Client**.

X500 *x500-name*

x500-name is the x500 name for the remote gateway

(Fireware v12.2.1 or higher) The **df** parameter starts the configuration of the df bit settings.

df-bit option must be one of these options: **Copy**, **Set**, or **Clear**.

(Fireware v12.2.1 or higher) The **vpn-pmtu** parameter starts the configuration of the PMTU settings.

pmtu-size is the minimum size in bytes, and must be between 68-1550.

life-time value must be between 60 and 2147483647.

gw-mode is the gateway mode. It must be one of these options: **Main**, **Aggressive**, or **Main-Fallback-Aggressive**.

credential-method pre-shared (*secret*) **addr-family IPv6** (**local-gateway** (*lgatewayid*) (*interface-name*) (*interface-ip-address*)) (**remote-gateway** (*rgateway*) (*rgatewayid*)) **df** (*df-bit option*) **vpn-pmtu minimum-size** *(pmtu-size)* **life-time** *(life-time value)* [**phase1 mode** *gw-mode*]

Configure the BOVPN gateway to use a pre-shared key for authentication. If the local and remote gateway endpoints are not yet defined, you must include the **local-gateway** and **remote-gateway** parameters in this command to configure the local and remote gateway endpoints for tunnel authentication.

secret is the pre-shared secret used to negotiate the tunnel.

addr-family specifies the IP address family in Fireware v12.5 or higher. If you specify this command, the only option is **IPv6**. For IPv4, do not specify the **addr-family** command.

The **local-gateway** parameter starts the configuration of the local gateway settings.

lgatewayid must be one of these options:

ip-address
ip-address is an IP address for the remote gateway in the format A.B.C.D.

by-domain*methoddomainnameresolvable*
method is one of these options: **domain-name** or **user-domain**

domainname is the domain name or user domain.

interface-name is the name of the external interface to use for this gateway endpoint. If you configured the wireless client as an external interface, specify the interface **WG-Wireless-Client**.

(Fireware v12.2 or higher) *interface-ip-address* is the IP address of the external interface you specified. Use **primary** to specify the primary IP address of the specified interface. Or, type an IP address that is a secondary IP address for the specified interface.

The **remote-gateway** parameter starts the configuration of the remote gateway settings

rgateway specifies the remote gateway IP address method. It must be either: **dynamic** or *ip-address*.

ip-address is an IP address for the remote gateway in the format A.B.C.D.

rgatewayid must be one of these options:

ip-address
ip-address is an IP address for the remote gateway in the format A.B.C.D.

by-domain*methoddomainnameresolvable*
method is one of these options: **domain-name** or **user-domain**

domainname is the domain name or user domain.

resolvable specifies whether the domain is resolvable. Specify **yes** if the domain name is resolvable or **no** if it is not.

X500 *x500-name*
x500-name is the x500 name for the remote gateway

(Fireware v12.2.1 or higher) The **df** parameter starts the configuration of the df bit settings.

df-bit option must be one of these options: **Copy**, **Set**, or **Clear**.

(Fireware v12.2.1 or higher) The **vpn-pmtu** parameter starts the configuration of the PMTU settings.

pmtu-size is the minimum size in bytes, and must be between 68-1550.

life-time value must be between 60 and 2147483647.

gw-mode is the gateway mode. It must be one of these options: **Main**, **Aggressive**, or **Main-Fallback-Aggressive**.

enable

Enable a configured BOVPN gateway. The BOVPN gateway is enabled by default when you configure it. To disable a configured gateway, use the **no enable** command. This command prevents traffic from going through tunnels that use this gateway.

endpoint [*index*] (**local-gateway** (*lgatewayid*) (*interface-name*) (*interface-ip-address*)) (**remote-gateway** (*rgateway*) (*rgatewayid*) **df** (*df-bit option*) **vpn-pmtu minimum-size** *(pmtu-size)* **life-time** *(life-time value)*

Change or add a gateway endpoint pair to the BOVPN gateway configuration.

index specifies the index of an existing gateway endpoint pair to update. If *index* is not specified, this command adds a new gateway endpoint pair.

The **local-gateway** parameter starts the configuration of the local gateway settings.

lgatewayid must be one of these options:

ip-address

ip-address is an IP address for the remote gateway in the format A.B.C.D.

by-domain*methoddomainnameresolvable*

method is one of these options: **domain-name** or **user-domain**

domainname is the domain name or user domain.

interface-name is the name of the external interface to use for this gateway endpoint. If you configured the wireless client as an external interface, specify the interface **WG-Wireless-Client**.

(Fireware v12.2 or higher) *interface-ip-address* is the IP address of the external interface you specified. Use **primary** to specify the primary IP address of the specified interface. Or, type an IP address that is a secondary IP address for the specified interface.

The **remote-gateway** parameter starts the configuration of the remote gateway settings

rgateway specifies the remote gateway IP address method. It must be either: **dynamic** or *ip-address*.

ip-address is an IP address for the remote gateway in the format A.B.C.D.

rgatewayid must be one of these options:

ip-address

ip-address is an IP address for the remote gateway in the format A.B.C.D.

by-domain*methoddomainnameresolvable*

method is one of these options: **domain-name** or **user-domain**

domainname is the domain name or user domain.

resolvable specifies whether the domain is resolvable. Specify **yes** if the domain name is resolvable or **no** if it is not.

X500*x500-name*

x500-name is the x500 name for the remote gateway

(Fireware v12.2.1 or higher) The **df** parameter starts the configuration of the df bit settings.

df-bit option must be one of these options: **Copy**, **Set**, or **Clear**.

Use **no endpoint** (endpoint ID) **df** to disable the per-gateway DF bit setting. For example: **no endpoint 1 df**

(Fireware v12.2.1 or higher) The **vpn-pmtu** parameter starts the configuration of the PMTU settings.

pmtu-size is the minimum size in bytes, and must be between 68-1550.

life-time value must be between 60 and 2147483647.

Use no endpoint (endpoint ID) vpn-pmtu to disable the per-gateway PMTU settings. For example: **no endpoint 1 vpn-pmtu**

endpoint (*index*) (**up** | **down** | *index2*)

Move a configured gateway endpoint pair up, down, or to a specific indexed location.

index is the current index of the gateway endpoint pair you want to move.

up moves the specified gateway endpoint pair up in the list.

down moves the specified gateway endpoint pair down in the list.

index 2 is the index position you want to move it to.

Use the command **show bovpn-gateway** (*gateway-name*) to see the index numbers for the configured gateway endpoint pairs.

no endpoint (*index*)

Remove the configured gateway endpoint pair with the specified index.

index is the index of the gateway endpoint pair you want to remove.

Use the command **show bovpn-gateway** (*gateway-name*) to see the index numbers for the configured gateway endpoint pairs.

auto-start enable

Configure the BOVPN tunnel to start negotiation as soon as the device restarts.

No options available.

modem enable

Enable modem failover for this branch office VPN gateway. Before you can enable modem failover in a branch office VPN gateway, you must first configure modem settings for dial-up serial modem failover. To do this, use the **modem** command in Configuration mode.

Use **no modem enable** to disable modem failover for this branch office VPN gateway.

phase1 (*attribute*)

Add or edit phase 1 configurations for BOVPN. Use the **version** command to set the IKE version to **IKEv1** or **IKEv2**. IKEv1 is used by default.

For the **phase1** command, *attribute* is one of these options:

dead-peer-detection enable enables dead peer detection for IKEv1

dpd-max-retries *tries* **traffic-idle-timeout** *time*

tries is an integer from 1 to 30.

time is an integer from 10 to 300.

ike-keep-alive enable enables IKE keep-alive for IKEv1

keep-alive-interval *k-time*

k-time is an integer from 1 to 65535. The IKE keep-alive interval for NAT traversal.

max-failures *count*

count is an integer from 1 to 30.

For IKEv1, the maximum number of failures that can occur before the BOVPN no longer sends IKE keep-alive messages.

For IKEv2 with timer-based DPD, the maximum number of failures that can occur before the BOVPN no longer sends DPD messages.

message-interval *mi-time*

mi-time is an integer from 0 to 300.

For IKEv1, the message interval for IKE keep-alive messages .

For IKEv2 with timer-based DPD, the message interval for DPD messages.

mode *gw-mode* for IKEv1

gw-mode is the gateway mode. It must be one of these options: **Main**, **Aggressive**, or **Main-Fallback-Aggressive**.

nat-traversal enable enables NAT traversal for IKEv1

transform *index method encrypt life group*

index is the transform index to edit the previously configured transform settings.

method is one of these options : **MD5**, **SHA1**, **SHA2-256**, **SHA2-384**, or **SHA2-512**.

SHA2 options are not available on XTM 5 Series, 810, 820, 830, 1050, and 2050 devices. The hardware cryptographic acceleration in those models does not support SHA2.

encrypt is one of these options:

DES *life* **unit** *t-unit*

DES-3 *life* **unit** *t-unit*

AES *life* **encrypt-key-length** *length* **unit** *t-unit*

where:

- *life* is the SA life; maximum life time is 35791394 minutes or 596523 hours

- *t-unit* is either: **minute**, or **hour**

- *length* is the AES encryption key length in bytes. It must be one of these values: **16**, **24**, or **32**.

group is one of these options: **Diffie-Hellman-Group1**, **Diffie-Hellman-Group2**, **Diffie-Hellman-Group5**, **Diffie-Hellman-Group14**, **Diffie-Hellman-Group15**, **Diffie-Hellman-Group19**, or **Diffie-Hellman-Group20**.

version (*ike-version*)

Set the version of the Internet Key Exchange (IKE) protocol to use in the phase 1 settings for this BOVPN gateway. *ike-version* is one of these options:

IKEv1 configures the VPN to use IKEv1

IKEv2 [**dpd-type** *type*] configures the VPN to use IKEv2

For IKEv2, you can optionally specify **dpd-type**, which controls the configurable options for dead peer detection in the phase 1 attributes for the gateway.

type must be one of these options:

timer is the timer-based DPD method. With this method, the Firebox initiates a DPD exchange with the remote gateway at a specified message interval, regardless of any other traffic received from the remote gateway. To configure the message-interval and max-failures settings, use the phase1 command options.

traffic is the traffic-based DPD method. With this method, the Firebox sends a DPD message to the remote gateway only if no traffic is received from the remote gateway for a specified length of time and a packet is waiting to be sent to the remote gateway. To configure the

If you do not specify the **dpd-type**, it is set to **traffic** by default.

For a BOVPN that uses IKEv2:

- Dead peer detection and NAT traversal are always enabled.
- IKE keep-alive is not supported.
- If the gateway has a remote gateway endpoint with a dynamic IP address, the gateway uses shared IKEv2 settings for NAT traversal and transforms. To see the IKEv2 shared settings, use the **show ikev2-shared-settings** command. To edit the IKEv2 shared settings, use the **ike-v2-shared** command.

Example

```
bovpn-gateway Headquarters

credential-method pre-shared n0s3cr3+! local-gateway 198.51.100.2 External
remote-gateway 198.51.100.2 203.0.113.2

phase1 transform MD5 DES 120 encryp-key-length 16 unit hour Diffie-Hellman-
Group1

bovpn modem enable
```

bovpn-tunnel

Description

Create or modify a tunnel for a branch office virtual private network.

Syntax

bovpn-tunnel (*name*)

Assign a unique name to a BOVPN tunnel.

name is a string that uniquely identifies the BOVPN tunnel.

After you type the command **bovpn-tunnel** (*name*) the configuration continues to the BOVPN tunnel details command.

The prompt changes to: `WG(config/policy/bovpntunnel-name)#`

Use the **Exit** command to exit this mode.

gateway (*gateway*) (*localaddress*) (*remoteaddress*) (*direction*) [*enable-broadcast*]

Configure tunnel route settings for a gateway already configured on the device. After you enter the gateway command, other BOVPN Tunnel commands become available. At first, *localaddress* and *remoteaddress* are required fields, but when you edit a tunnel these fields are no longer required.

gateway is the gateway name.

localaddress must use one of these formats:

any — any local address

host (*ipaddress*) where *ipaddress* is an IP address for the local end point in the format A.B.C.D.

range (**start-ip** *startip*) (**end-ip** *endip*) where:

startip is the first IP address of a range in the format A.B.C.D.

endip is the last IP address of a range in the format A.B.C.D.

subnet *net* where *net* is a network address and mask in the format A.B.C.D./#.

remoteaddress must use one of these formats:

any — any remote address

host (*ipaddress*) where *ipaddress* is an IP address for the local end point in the format A.B.C.D.

range (**start-ip** *startip*) (**end-ip** *endip*) where:

startip is the first IP address of a range in the format A.B.C.D.

endip is the last IP address of a range in the format A.B.C.D.

subnet *net* where *net* is a network address and mask in the format A.B.C.D./#.

direction sets the direction of the traffic through the tunnel. You must use one of these options:

bi-direction (*nat-type*) — traffic routed both ways through the tunnel (default).

inbound (*nat-type*) — traffic routed from the remote address to the local address.

outbound (*nat-type*) — traffic routed from the local address to the remote address.

nat-type must be *type ip-address* where:

type is one of these options:

dnat — Dynamic NAT IP address for either inbound or outbound only.

host-ip — 1-to-1 NAT host IP address.

network-ip — 1-to-1 NAT network IP address.

range-ip — 1-to-1 range of IP addresses.

ip-address is in the format A.B.C.D. or A.B.C.D/(0 to 32) whichever is applicable.

enable-broadcast must be **broadcast-over-tunnel enable** to enable broadcast over BOVPN.

add-to-policy enable

Add the tunnel to the BOVPN-Allow policies.

No options available.

address-pair (*index*) (*localaddress*) (*remoteaddress*) [*direction*] [*enable-broadcast*]

Add or edit an address pair in the tunnel configuration.

index is the index of the address pair to be edited.

localaddress must use one of these formats:

host (*ipaddress*) where *ipaddress* is an IP address for the local end point in the format A.B.C.D.

range (**start-ip** *startip*) (**end-ip** *endip*) where:
startip is the first IP address of a range in the format A.B.C.D.
endip is the last IP address of a range in the format A.B.C.D.

subnet *net* where *net* is a network address and mask in the format A.B.C.D./#.

remoteaddress must use one of these formats:

host (*ipaddress*) where *ipaddress* is an IP address for the local end point in the format A.B.C.D.

range (**start-ip** *startip*) (**end-ip** *endip*) where:
startip is the first IP address of a range in the format A.B.C.D.
endip is the last IP address of a range in the format A.B.C.D.

subnet *net* where *net* is a network address and mask in the format A.B.C.D./#.

direction sets the direction of the traffic through the tunnel. You must use one of these options:

bi-direction (*nat-type*) — traffic routed both ways through the tunnel (default).

inbound (*nat-type*) — traffic routed from the remote address to the local address.

outbound (*nat-type*) — traffic routed from the local address to the remote address.

nat-type must be *type ip-address* where:

type is one of these options:

dnat — Dynamic NAT IP address for either inbound or outbound only.

host-ip — 1-to-1 NAT host IP address.

network-ip — 1-to-1 NAT network IP address.

range-ip — 1-to-1 range of IP addresses.

ip-address is in the format A.B.C.D. or A.B.C.D/(0 to 32) whichever is applicable.

enable-broadcast must be **broadcast-over-tunnel enable** to enable Broadcast over BOVPN.

move (*where*)

Move the tunnel either up, down, or to a certain indexed location.

where must be one of these options:

up [*index1*]

down [*index1*]

to (*index2*)

index1 or *index2* is the arbitrary location to which the tunnel moves. If *index1* is omitted it is understood to be a value of 1.

multicast-settings enable (*origin-ip*) (*group-ip*) (*direction*) (*if-number*|**name** *if-name*) **tunnel-endpoints** *local-helper-ip remote-helper-ip*]

Configure the tunnel to allow multicast packets.

origin-ip is the origination IP address of the multicast.

group-ip is the multicast address of the receiving hosts.

direction is either:

input (*if-index*) — where *if-index* is the interface number of one of the trusted or optional interfaces, where the multicast origin host is connected.

input (*if-index*) (*if-index*) — where *if-index* is the interface number or numbers of the trusted or optional interfaces, where the receiving hosts are connected.

if-number is the interface number to send or receive multicast traffic.

if-name is the name of a physical or link aggregation interface to send or receive multicast traffic.

Use the **tunnel-endpoints** option to configure local and remote helper IP addresses. The Firebox uses these addresses as the endpoints of the multicast GRE tunnel inside the BOVPN tunnel. We recommend that you use IP addresses that are not used on any network known to the Firebox.

local-helper-ip is an IP address to use for the local end of the tunnel.

remote-helper-ip is n IP address to use for the remote end of the tunnel.

Use **no multicast-settings enable** to disable multicast settings for the tunnel.

phase2 pfs enable (*group*)

Enable Perfect Forwarding Secrecy for the tunnel.

group is the IKE Diffie-Hellman group. It must be one of these options: **dh-group1**, **dh-group2**, or **dh-group5**, **dh-group14**, **dh-group15**, **dh-group19**, **dh-group20**.

phase2 proposals (*p2name*) [**replace** [**yes**]]

Assign a phase 2 proposal to the tunnel.

p2name is an existing phase 2 proposal on the device.

replace — replaces the existing phase 2 proposal for this tunnel with the specified proposal.
If **replace** is not specified, then the phase2 proposal is added to the existing phase 2 proposals for this tunnel. Use **yes** with **replace** to confirm that you want to replace the existing phase 2 proposals for this tunnel. This avoids the confirmation prompt.

Use **show proposal p2** to see a list of existing phase 2 proposals. Use **proposal p2** to create a new one.

tunnel-endpoints (*local-helper-ip*) (*remote-helper-ip*)

Define the route for encapsulation of broadcast and multicast traffic. The Firebox uses these addresses as the endpoints of the multicast GRE tunnel inside the BOVPN tunnel. We recommend that you use IP addresses that are not used on any network known to the Firebox.

Used only when broadcast or multicast is enabled.

local-helper-ip is an IP address on the local network of the tunnel address pair.

remote-helper-ip is an IP address on the remote network of the tunnel address pair.

Example

```
bovpn-tunnel SeattleNewYork

gateway GWSeattleNewYork network-ip 192.168.111.0/24 network-ip
10.10.10.0/24 broadcast-over-tunnel enable

gateway GWSeattleNewYork network-ip 192.168.111.0/24 network-ip
10.10.10.0/24 outbound dnat 172.16.30.5
```

bovpn-vif

Description

Create or modify a BOVPN virtual interface.

Syntax

bovpn-vif (*name*)

Assign a unique name to a BOVPN virtual interface.

name is a string that uniquely identifies the BOVPN virtual interface. It is case sensitive.

After you type the command **bovpn-vif** (*name*) the configuration continues to the BOVPN virtual interface details commands.

The prompt changes to: `WG(config/policy/bovpnvif-name)#`

Use the **Exit** command to exit this mode.

credential-method certificate (*id*) **addr-family IPv6** (**local-gateway** (*type*) (*interface-name*) (*interface-ip-address*)) (**remote-gateway** (*rgateway*) (*rgatewayid*)) **df** (*df-bit option*) **vpn-pmtu minimum-size** *(pmtu-size)* **life-time** *(life-time value)* [**phase1 mode** *gw-mode*]

Configure the BOVPN virtual interface to use a certificate for authentication. If the local and remote gateway endpoints are not yet defined, you must include the **local-gateway** and **remote-gateway** parameters in this command to configure the local and remote gateway endpoints for tunnel authentication.

id is the certificate identification number.

addr-family specifies the IP address family in Fireware v12.5 or higher. If you specify this command, the only option is **IPv6**. For IPv4, do not specify the **addr-family** command.

The **local-gateway** parameter starts the configuration of the local gateway settings.

type is the certificate ID type. It must be one of these options: **ip-address**, **domain**, **user-domain**, or **x500**. The specified certificate must contain the selected type of certificate ID information.

interface-name is the name of the external interface to use for this gateway endpoint. If you configured the wireless client as an external interface, specify the interface **WG-Wireless-Client**.

(Fireware v12.2 or higher) *interface-ip-address* is the IP address of the external interface you specified. Use **primary** to specify the primary IP address of the specified interface. Or, type an IP address that is a secondary IP address for the specified interface.

The **remote-gateway** parameter starts the configuration of the remote gateway settings

rgateway must be either: **dynamic** or *ip-address*.

ip-address is an IP address for the remote gateway in the format A.B.C.D.

rgatewayid must be one of these options:

ip-address
ip-address is an IP address for the remote gateway in the format A.B.C.D.

by-domain*methoddomainnameresolvable*
method is one of these options: **domain-name** or **user-domain**

domainname is the domain name or user domain.

resolvable specifies whether the domain is resolvable. Specify **yes** if the domain name is resolvable or **no** if it is not.

X500 *x500-name*
x500-name is the x500 name for the remote gateway

(Fireware v12.2.1 or higher) The **df** parameter starts the configuration of the df bit settings.

df-bit option must be one of these options: **Copy**, **Set**, or **Clear**.

(Fireware v12.2.1 or higher) The **vpn-pmtu** parameter starts the configuration of the PMTU settings.

pmtu-size is the minimum size in bytes, and must be between 68-1550.

life-time value must be between 60 and 2147483647.

gw-mode is the gateway mode. It must be one of these options: **Main**, **Aggressive**, or **Main-Fallback-Aggressive**.

credential-method pre-shared (*secret*) **addr-family IPv6** (**local-gateway** (*lgatewayid*) (*interface-name*) (*interface-ip-address*)) (**remote-gateway** (*rgateway*) (*rgatewayid*)) **df** (*df-bit option*) **vpn-pmtu minimum-size** *(pmtu-size)* **life-time** *(life-time value)* [**phase1 mode** *gw-mode*]

Configure the BOVPN virtual interface to use a pre-shared key for authentication. If the local and remote gateway endpoints are not yet defined, you must include the **local-gateway** and **remote-gateway** parameters in this command to configure the local and remote gateway endpoints for tunnel authentication.

secret is the pre-shared secret used to negotiate the tunnel.

addr-family specifies the IP address family in Fireware v12.5 or higher. If you specify this command, the only option is **IPv6**. For IPv4, do not specify the **addr-family** command.

The **local-gateway** parameter starts the configuration of the local gateway settings.

lgatewayid must be one of these options:

ip-address
ip-address is an IP address for the remote gateway in the format A.B.C.D.

by-domain*methoddomainnameresolvable*
method is one of these options: **domain-name** or **user-domain**

domainname is the domain name or user domain.

(Fireware v12.2 or higher) *interface-ip-address* is the IP address of the external interface you specified. Use **primary** to specify the primary IP address of the specified interface. Or, type an IP address that is a secondary IP address for the specified interface.

(Fireware v12. or higher) *interface-ip-address* is the IP address of the external interface you specified. You can specify the primary or secondary interface IP address.

The **remote-gateway** parameter starts the configuration of the remote gateway settings

rgateway specifies the remote gateway IP address method. It must be either: **dynamic** or *ip-address*.

ip-address is an IP address for the remote gateway in the format A.B.C.D.

rgatewayid must be one of these options:

ip-address
ip-address is an IP address for the remote gateway in the format A.B.C.D.

by-domain*methoddomainnameresolvable*
method is one of these options: **domain-name** or **user-domain**

domainname is the domain name or user domain.

resolvable specifies whether the domain is resolvable. Specify **yes** if the domain name is resolvable or **no** if it is not.

X500 *x500-name*
x500-name is the x500 name for the remote gateway

(Fireware v12.2.1 or higher) The **df** parameter starts the configuration of the df bit settings.

df-bit option must be one of these options: **Copy**, **Set**, or **Clear**.

(Fireware v12.2.1 or higher) The **vpn-pmtu** parameter starts the configuration of the PMTU settings.

pmtu-size is the minimum size in bytes, and must be between 68-1550.

life-time value must be between 60 and 2147483647.

gw-mode is the gateway mode. It must be one of these options: **Main**, **Aggressive**, or **Main-Fallback-Aggressive**.

enable

Enable a configured BOVPN virtual interface. The BOVPN virtual interface is enabled by default when you configure it. To disable a configured BOVPN virtual interface, use the **no enable** command. This command prevents traffic from going through tunnels that use this gateway. BOVPN virtual interface routes for a disabled BOVPN virtual interface are not added to the routing table.

endpoint [*index*] (**local-gateway** (*lgatewayid*) (*interface-name*) (*interface-ip-address*)) (**remote-gateway** (*rgateway*) (*rgatewayid*) **df** (*df-bit option*) **vpn-pmtu minimum-size** *(pmtu-size)* **life-time** *(life-time value)*

Change or add a gateway endpoint pair to the BOVPN gateway configuration.

index specifies the index of an existing gateway endpoint pair to update. If *index* is not specified, this command adds a new gateway endpoint pair.

The **local-gateway** parameter starts the configuration of the local gateway settings.

lgatewayid must be one of these options:

ip-address

ip-address is an IP address for the remote gateway in the format A.B.C.D.

by-domain*methoddomainnameresolvable*

method is one of these options: **domain-name** or **user-domain**

domainname is the domain name or user domain.

interface-name is the name of the external interface to use for this gateway endpoint. If you configured the wireless client as an external interface, specify the interface **WG-Wireless-Client**.

(Fireware v12.2 or higher) *interface-ip-address* is the IP address of the external interface you specified. Use **primary** to specify the primary IP address of the specified interface. Or, type an IP address that is a secondary IP address for the specified interface.

The **remote-gateway** parameter starts the configuration of the remote gateway settings

rgateway specifies the remote gateway IP address method. It must be either: **dynamic** or *ip-address*.

ip-address is an IP address for the remote gateway in the format A.B.C.D.

rgatewayid must be one of these options:

ip-address

ip-address is an IP address for the remote gateway in the format A.B.C.D.

by-domain*methoddomainnameresolvable*

method is one of these options: **domain-name** or **user-domain**

domainname is the domain name or user domain.

resolvable specifies whether the domain is resolvable. Specify **yes** if the domain name is resolvable or **no** if it is not.

X500*x500-name*

x500-name is the x500 name for the remote gateway

(Fireware v12.2.1 or higher) The **df** parameter starts the configuration of the df bit settings.

df-bit option must be one of these options: **Copy**, **Set**, or **Clear**.

Use **no endpoint** (endpoint ID) **df** to disable the per-gateway DF bit setting. For example: **no endpoint 1 df**

(Fireware v12.2.1 or higher) The **vpn-pmtu** parameter starts the configuration of the PMTU settings.

pmtu-size is the minimum size in bytes, and must be between 68-1550.

life-time value must be between 60 and 2147483647.

Use no endpoint (endpoint ID) vpn-pmtu to disable the per-gateway PMTU settings. For example: **no endpoint 1 vpn-pmtu**

add-to-policy enable

Add the BOVPN virtual interface tunnel to the BOVPN-Allow policies.

No options available.

auto-start enable

Configure the BOVPN tunnel to start negotiation as soon as the tunnel is available.

No options available.

modem enable

Enable modem failover for this BOVPN virtual interface. Before you can enable modem failover in a BOVPN virtual interface, you must first configure modem settings for dial-up serial modem failover. To do this, use the **modem** command in Configuration mode.

Use **no modem enable** to disable modem failover for this BOVPN virtual interface.

multicast-settingsenable (*origin-ip*) (*group-ip*) (*direction*) (*if-number*|**name***if-name*) **tunnel-endpoints***local-helper-ipremote-helper-ip*]

Configure the tunnel to allow multicast packets.

origin-ip is the origination IP address of the multicast.

group-ip is the multicast address of the receiving hosts.

direction is either:

input (*if-index*) — where *if-index* is the interface number of one of the trusted or optional interfaces, where the multicast origin host is connected.

input (*if-index*) (*if-index*) — where *if-index* is the interface number or numbers of the trusted or optional interfaces, where the receiving hosts are connected.

if-number is the interface number to send or receive multicast traffic.

if-name is the name of a physical or link aggregation interface to send or receive multicast traffic.

Use the **tunnel-endpoints** option to configure local and remote helper IP addresses. The Firebox uses these addresses as the endpoints of the multicast GRE tunnel inside the BOVPN tunnel. We recommend that you use IP addresses that are not used on any network known to the Firebox.

local-helper-ip is an IP address to use for the local end of the tunnel.

remote-helper-ip is n IP address to use for the remote end of the tunnel.

Use **no multicast-settings enable** to disable multicast settings for the tunnel.

phase1 (*attribute*)

Add or edit phase 1 configurations for BOVPN. Use the **version** command to set the IKE version to **IKEv1** or **IKEv2**. IKEv1 is used by default.

For the **phase1** command, *attribute* is one of these options:

dead-peer-detection enable enables dead peer detection for IKEv1 (For IKEv2 this is always enabled)

dpd-max-retries*tries***traffic-idle-timeout***time*

tries is an integer from 1 to 30.

time is an integer from 10 to 300.

ike-keep-alive enable enables IKE keep-alive for IKEv1

keep-alive-interval*k-time*

k-time is an integer from 1 to 65535. The IKE keep-alive interval for NAT traversal.

max-failures*count*

count is an integer from 1 to 30.

For IKEv1, the maximum number of failures that can occur before the BOVPN no longer sends IKE keep-alive messages.

For IKEv2 with timer-based DPD, the maximum number of failures that can occur before the BOVPN no longer sends DPD messages.

message-interval*mi-time*

mi-time is an integer from 0 to 300.

For IKEv1, the message interval for IKE keep-alive messages .

For IKEv2 with timer-based DPD, the message interval for DPD messages.

mode*gw-mode*

gw-mode is the gateway mode. It must be one of these options: **Main**, **Aggressive**, or **Main-Fallback-Aggressive**.

nat-traversal enable enables NAT traversal

transform*indexmethodencryptlifegroup*

index is the transform index to edit the previously configured transform settings.

method is one of these options : **MD5**, **SHA1**, **SHA2-256**, **SHA2-384**, or **SHA2-512**.

SHA2 options are not available on XTM 5 Series, 810, 820, 830, 1050, and 2050 devices. The hardware cryptographic acceleration in those models does not support SHA2.

encrypt is one of these options:

DES*life* **unit***t-unit*

DES-3*life* **unit***t-unit*

AES*life* **encrypt-key-length**/*length* **unit***t-unit*

where:

- *life* is the SA life; maximum life time is 35791394 minutes or 596523 hours

- *t-unit* is either: **minute**, or **hour**

- *length* is the AES encryption key length in bytes. It must be one of these values: **16**, **24**, or **32**.

group is one of these options: **Diffie-Hellman-Group1**, **Diffie-Hellman-Group2**, **Diffie-Hellman-Group5**, **Diffie-Hellman-Group14**, **Diffie-Hellman-Group15**, **Diffie-Hellman-Group19**, or **Diffie-Hellman-Group20**.

phase2 pfsenable (*group*)

Enable Perfect Forwarding Secrecy for the BOVPN virtual interface.

group is the IKE Diffie-Hellman group. It must be one of these options: **dh-group1**, **dh-group2**, or **dh-group5**, **dh-group14**, **dh-group15**, **dh-group19**, **dh-group20**.

phase2proposals (*p2name*) [**replace** [**yes**]]

Assign a phase 2 proposal to the BOVPN virtual interface.

p2name is an existing phase 2 proposal on the device.

replace — replaces the existing phase 2 proposal for this tunnel with the specified proposal.
If **replace** is not specified, then the phase2 proposal is added to the existing phase 2 proposals for this tunnel. Use **yes** with **replace** to confirm that you want to replace the existing phase 2 proposals for this tunnel. This avoids the confirmation prompt.

Use **show proposal p2** to see a list of existing phase 2 proposals. Use **proposal p2** to create a new one.

type (*attribute*)

Configure the gateway endpoint type (Fireware 11.12 or higher).

Attribute must be one of these options:

firebox – Use this option for a VPN tunnel to another Firebox or to a third-party endpoint that supports GRE over IPSec.

cloud-vpn-gateway – Use this option for a VPN tunnel to a third-party endpoint, including a cloud-based virtual network like Microsoft Azure, that supports wildcard traffic selectors. This endpoint type does not use GRE.

version (*ike-version*)

Set the version of the Internet Key Exchange (IKE) protocol to use in the phase 1 settings for this BOVPN gateway. *ike-version* is one of these options:

IKEv1 configures the VPN to use IKEv1

IKEv2 [**dpd-type***type*] configures the VPN to use IKEv2

For IKEv2, you can optionally specify **dpd-type**, which controls the configurable options for dead peer detection in the phase 1 attributes for the gateway.

type must be one of these options:

timer is the timer-based DPD method. With this method, the Firebox initiates a DPD exchange with the remote gateway at a specified message interval, regardless of any other traffic received from the remote gateway. To configure the message-interval and max-failures settings, use the phase1 command options.

traffic is the traffic-based DPD method. With this method, the Firebox sends a DPD message to the remote gateway only if no traffic is received from the remote gateway for a specified length of time and a packet is waiting to be sent to the remote gateway. To configure the

If you do not specify the **dpd-type**, it is set to **traffic** by default.

For a BOVPN that uses IKEv2:

- Dead peer detection and NAT traversal are always enabled.
- IKE keep-alive is not supported.
- If the gateway has a remote gateway endpoint with a dynamic IP address, the gateway uses shared IKEv2 settings for NAT traversal and transforms. To see the IKEv2 shared settings, use the **show ikev2-shared-settings** command. To edit the IKEv2 shared settings, use the **ike-v2-shared** command.

virtual-ip (*local-ip*) (*peer-ip*)

Configure virtual IP addresses for a BOVPN virtual interface.

local-ip is the IP address to use for the local end of the tunnel.

peer-ip is the IP address of the remote peer or the subnet mask.

For a VPN to another Firebox, specify the local virtual IP address configured on the peer Firebox.

For a VPN to a third-party endpoint, specify the subnet mask.

Use **no virtual-ip enable** to remove the virtual IP addresses.

vpn-route (*destination*) [**distance** *distancevalue*]

Create an IPv4 BOVPN virtual interface route.

destination must be one of these options: *ipaddress* or *net*.

ipaddress is the IPv4 address for the destination in the format of A.B.C.D.

net is the IPv4 subnet for the destination in the format of A.B.C.D/# where # must be in the range of 0 to 32.

distancevalue is the route distance (metric). It must be an integer from 1 to 254. The default distance is 1

Use **no ip route vpn-route** (*destination*) to remove a static route.

In Fireware v12.9 or higher, **distance** replaces **metric**. In FIreware v12.8.x or lower, enter this command: **vpn-route** (*destination*) [**metric** *metricvalue*]

v6 vpn-route (*destination*) [**distance** *distancevalue*]

Create an IPv6 BOVPN virtual interface route.

destination must be one of these options: *ipaddress* or *net*.

ipaddress is the IPv6 address for the destination in the format of A:B:C:D:E:F:G:H.

net is the IPv6 subnet for the destination in the format of A:B:C:D:E:F:G:H/I.

distancevalue is the route distance (metric). It must be an integer from 1 to 254. The default distance is 1.

Use **no v6 ip route vpn-route** (*destination*) to remove a static route.

In Fireware v12.9 or higher, **distance** replaces **metric**. In FIreware v12.8.x or lower, enter this command: **v6 vpn-route** (*destination*) [**metric** *metricvalue*]

Examples

SHA2 options are not available on XTM 5 Series, 810, 820, 830, 1050, and 2050 devices. The hardware cryptographic acceleration in those models does not support SHA2.

This example shows a connection to another Firebox (Fireware v11.12 and higher). The default Phase 1 transform is replaced with SHA2-256–AES(256-bit).

```
bovpn-vif BovpnVif.FireboxSiteB

credential-method pre-shared s2R4YqgV96RFXgMs local-gateway 198.51.100.2
External remote-gateway 203.0.113.2 203.0.113.2

type firebox

virtual-ip 10.1.1.1 10.2.2.2

phase1 transform SHA2-256 AES 8 Encryp-key-length 32 unit hour Diffie-
Hellman-Group2

apply

no phase1 transform 1

apply
```

This example shows dynamic routing to a Cisco router configured with a VTI (Fireware v11.12 and higher). The default Phase 1 transform is replaced with SHA2-256–AES(256-bit).

```
bovpn-vif BovpnVif.CiscoVTI

credential-method pre-shared s2R4YqgV96RFXgMs local-gateway 198.51.100.2
External remote-gateway 203.0.113.3 203.0.113.3

type cloud-vpn-gateway

phase1 transform SHA2-256 AES 8 Encryp-key-length 32 unit hour Diffie-
Hellman-Group2

virtual-ip 10.3.3.3 255.255.255.0

apply

no phase1 transform 1

apply
```

This example shows a static route to a Microsoft Azure virtual network (Fireware v11.12 and higher). The default Phase 1 transform is replaced with SHA2-256–AES(256-bit), and IKEv2 is specified.

```
bovpn-vif BovpnVif.AzureCloud

credential-method pre-shared s2R4YqgV96RFXgMs local-gateway 198.51.100.2
External remote-gateway 203.0.113.4 203.0.113.4

type cloud-vpn-gateway

vpn-route 10.4.4.4

version IKEv2
```

```
phase1 transform SHA2-256 AES 8 Encryp-key-length 32 unit hour Diffie-
Hellman-Group2
apply
no phase1 transform 1
apply
```

bovpntls-client

Description

Configure a BOVPN over TLS client to connect to this Firebox, which is configured as a BOVPN over TLS server. You must enable BOVPN over TLS in Server mode on the Firebox before you can specify a client in the BOVPN over TLS Server settings.

Syntax

bovpntls-client *(tunnel ID)*

To specify a BOVPN over TLS client that can connect to this Firebox, specify a tunnel ID for the BOVPN over TLS tunnel. The tunnel ID must be between 1 and 42 characters in length. After a carriage return, you must use **pre-shared** to specify a pre-shared key for tunnel authentication. The pre-shared key must be between 1 and 79 characters in length.

After you specify a pre-shared key, the client configuration commands are available:

local-route — Configure client routes. Client routes are destinations behind the BOVPN over TLS server that are accessible by the BOVPN over TLS client. To send all traffic through the tunnel, specify 0.0.0.0. To specify the destination addresses that the client will route through the tunnel, specify an IP address, or an IP address and subnet.

remote-route — Configure server routes. Server routes are destinations behind the BOVPN over TLS client that are accessible by the BOVPN over TLS server.

enable — You must specify this command to enable the BOVPN over TLS clients you specify as clients the BOVPN over TLS server can connect to. To see a list of BOVPN over TLS clients enabled in the BOVPN over TLS server configuration, use **show bovpntls-client**.

To save your changes, you must use **apply**.

Examples

```
bovpntls-client tunnel2
pre-shared Pswrd24892
local-route 0.0.0.0
local route 10.0.1.1
local route 10.0.1.0/24
remote-route 10.50.1.1
remote-route 10.50.1.0/24
```

dynamic-nat

Description

Configure the device to use dynamic network address translation.

Syntax

dynamic-nat from (*local*) **to** (*remote*) [**from** (*source*)]

Add a dynamic NAT rule to apply to all firewall policies.

local is a host address, host range, network, or alias for a location on the protected network.

remote is a host address, host range, network, or alias for a location outside of the protected network.

local and *remote* must be one of these options:

alias *alias* — *alias* must be a configured alias, such as Any-Trusted

host-ip *ip* — *ip* must be an IPv4 host address in the format A.B.C.D

host-name *hostname* — *hostname* must be a host name. The Firebox does an immediate DNS lookup to resolve the host name you specify and add the IP address.

host-range *startip endip* — *startip* and *endip* must be IPv4 addresses in the format A.B.C.D

network-ip *net* — *net* must be an IPv4 subnet in the format A.B.C.D/# where # is in the range of 0 to 32

source is an optional source IP address to use for this rule. It must be an IPv4 IP address in the format A.B.C.D that is on the same subnet as the primary or secondary IP address of the outgoing interface. In Fireware v12.2 or higher, you can specify a source IP address that is on the same subnet as the loopback interface.

dynamic-nat (*id*) (*where*)

Change the order of dynamic NAT rules. You can move a rule up, down, or to a specified location. The rule ID number is the location of the rule in the list.

id is the ID number of an existing dynamic NAT rule you want to move. Use **show dynamic-nat** to see the ID numbers of dynamic NAT rules.

where indicates where you want to move the rule. It must be one of these options:

up — move the item one higher in the list

down — move the rule one lower in the list

position (*number*) — move the rule to the specified numeric position in the list.

Example

```
dynamic-nat from alias webservers to alias Any-External

dynamic-nat from network-ip

dynamic-nat from host-ip 1.1.1.1 to host-ip 2.2.2.2 source-ip 3.3.3.3
```

ike-v2-shared

Description

Configure the IKEv2 shared settings for NAT traversal and Phase 2 transforms for branch office VPN gateways that use IKEv2 and have a remote gateway with a dynamic IP address.

Use the command **show ikev2-shared-settings** to see the current settings, and a list of configured transforms and their indexes.

Syntax

ike-v2-shared keep-alive-interval (*k-time*)

Define the IKEv2 shared settings for NAT traversal and Phase 2 transform settings.

keep-alive-interval*k-time*

k-time is the IKE keep-alive interval for NAT traversal. It must be an integer between 1 and 65535.

ike-v2-shared transform [*index*] (*method*) (*encrypt*) (*life*) (*group*)

Add or edit Phase 1 transforms in the IKEv2 shared settings.

index is the current position in the transform list of the transform you want to edit. To add a new transform, do not specify the index.

method is one of these options: **MD5**, **SHA1**, **SHA2-256**, **SHA2-384**, or **SHA2-512**.

encrypt is one of these options:

DES *life* **unit** *t-unit*

DES-3 *life* **unit** *t-unit*

AES *life* **encrypt-key-length***length* **unit***t-unit*

(Fireware v12.2 or higher) **AES-GCM** *life* **encrypt-key-length** *length* **unit** *t-unit*

where:

- *life* is the SA life; maximum life time is 35791394 minutes or 596523 hours

- *t-unit* is the time unit for the SA life. It must be: **minute** or **hour**

- *length* is the AES encryption key length in bytes. It must be one of these values: **16**, **24**, or **32**.

group is one of these options: **Diffie-Hellman-Group1**, **Diffie-Hellman-Group2**, **Diffie-Hellman-Group5**, **Diffie-Hellman-Group14**, **Diffie-Hellman-Group15**, **Diffie-Hellman-Group19**, or **Diffie-Hellman-Group20**.

transform *index*(**up** | **down** | *index2*)

Move a configured transform up or down in the transform list. The gateways use the transforms based on the order they appear in the list.

index is the current position in the transform list of the transform you want to move.

up moves the specified transform up one position in the transform list.

down moves the specified transform down one position in the transform list.

index2 is the index position you want to move it to.

Use the command **show ikev2-shared-settings** to see the index numbers for the configured transforms.

l2tp

Description

Configure settings for Mobile VPN with L2TP.

Syntax

l2tp address-pool (*address*)

Define the L2TP address pool.

address must be either **host** *ipaddress*, **network** *networkip* or **range** *firstip lastip*.

ipaddress, *firstip*, and *lastip* are all IPv4 addresses with the format A.B.C.D.

networkip is an IPv4 network IP address with the format A.B.C.D/(0 to 32).

l2tp auth-server (*authentication*) [**default**]

Define the type of authentication server to use for Mobile VPN with L2TP. You can use more than one authentication server. The authentication servers you specify must already be configured for the device.

authentication must be one of these options:

Firebox-DB — use the Firebox as the authentication server for L2TP user authentication.

RADIUS — use a configured RADIUS authentication server for L2TP user authentication.

Use **default** to designate the specified *authentication* server as the default authentication method.

l2tp auth-user-group (*option*) (*type*) (*name*) (*authentication*)

Add a new user or group for Mobile VPN with L2TP authentication.

option must be **default** or **specify-user-group**.

Use **default** to use the default group name, L2TP-Users.

Use **specify-user-group** to add a new user or group for Mobile VPN with L2TP authentication.

type is only needed if *option* is **specify-user-group**. *type* must be one of these options:

Use **user** to add a new user.

Use **group** to add a new group.

name must be the name of a user or group to add. The user or group must also exist on the *authentication* server specified for the group or user.

authentication must be the name of an authentication server enabled in the L2TP configuration. It must be one of these options:

Any — Any authentication server

Firebox-DB — Firebox database
RADIUS — RADIUS server

l2tp enable

No options available.

Use **no l2tp enable** to disable Mobile VPN with L2TP.

l2tp ipsec enable

Enable IPSec for Mobile VPN with L2TP.

Use **no ipsec enable** to disable IPSec for Mobile VPN with L2TP.

l2tp ipsec phase1 certificate (*id*) (*type*) (*algorithm*)

Configure IPSec phase 1 settings to use a certificate for IPSec tunnel authentication.

id is the local certificate identification number.

type is the certificate type. It must be one of these options: **none**, **ip-address**, **domain**, **user-domain**, or **x500**.

algorithm is either: **rsa** or **dsa**.

l2tp ipsec phase1 pre-shared (*key*)

Configure IPSec phase 1 settings to use a pre-shared key for IPSec tunnel authentication.

key is the pre-shared key. You must use the same pre-shared key in the IPSec settings on the L2TP clients.

l2tp ipsec phase1 dpd enable

Enable traffic-based dead peer detection. This is enabled by default. When you enable dead peer detection, the Firebox connects to a peer only if no traffic is received from the peer for a specified length of time and a packet is waiting to be sent to the peer.

Use **no l2tp ipsec phase1 dpd enable** to disable dead peer detection.

l2tp ipsec phase1 idle-timeout (*timeout*)

Configure the traffic idle timeout for dead peer detection. When dead peer detection is enabled, this controls the amount of time that passes before the Firebox tries to connect to the peer.

timeout is the traffic idle timeout, in seconds. It must be an integer in the range 10–300.

l2tp ipsec phase1 max-retries (*retries*)

Configure the max retries for dead peer detection. When dead peer detection is enabled, this controls the number of times the Firebox tries to connect before the peer is declared dead.

retries is the traffic idle timeout, in seconds. It must be an integer in the range 10–300.

l2tp ipsec phase1 nat-traversal enable

Enable NAT traversal. This is enabled by default. NAT Traversal, or UDP Encapsulation, enables traffic to get to the correct destinations when L2TP VPN clients are behind a NAT device.

Use **no l2tp ipsec phase1 nat-traversal enable** to disable NAT traversal.

l2tp ipsec phase1 keep-alive-interval (*interval*)

Configure the keep-alive interval for NAT traversal. When NAT traversal is enabled, this controls the number of seconds that pass before the next NAT keep-alive message is sent.

interval is the keep-alive interval, in seconds. It must be an integer in the range 0–65535.

l2tp ipsec phase1 transform (*index*) (*method*) (*encrypt*) (*life*) (*group*)

index is the index of a previously configured transform to edit. It represents the position of the transform in the list of transforms in the Mobile VPN with L2TP configuration. If *index* is not specified, the other settings add a new phase1 transform to the configuration.

method is one of these options : **MD5**, **SHA1**, **SHA2-256**, **SHA2-384**, or **SHA2-512**.

SHA2 options are not available on XTM 5 Series, 810, 820, 830, 1050, and 2050 devices. The hardware cryptographic acceleration in those models does not support SHA2.

encrypt is one of these options:

DES *life* **unit** *t-unit*

DES-3 *life* **unit** *t-unit*

AES *life* **encrypt-key-length** *length* **unit** *t-unit*

where:

- *life* is the SA life; maximum life time is 35791394 minutes or 596523 hours
- *t-unit* is either: **minute**, or **hour**
- *length* is the AES encryption key length

group is one of these options: **Diffie-Hellman-Group1**, **Diffie-Hellman-Group2**, **Diffie-Hellman-Group5**, **Diffie-Hellman-Group14**, **Diffie-Hellman-Group15**, **Diffie-Hellman-Group19**, or **Diffie-Hellman-Group20**.

l2tp ipsec phase1 transform (*index*) (*new-index* | *move*)

Change the position of an existing phase1 transform in the Mobile VPN with L2TP configuration.

index is the current position in the list of the transform you want to move (1 is the first one).

new-index is the position in the transform list where you want to move the transform.

move can move a transform up or down in the transform list. It must be **up** or **down**.

Use **show l2tp** to see a list of current transforms.

l2tp ipsec phase2 pfs enable (*group*)

Enable Perfect Forwarding Secrecy. PFS is disabled by default because many L2TP clients do not support it.

group is the IKE Diffie-Hellman group. It must be one of these options: **Diffie-Hellman-Group1**, **Diffie-Hellman-Group2**, **Diffie-Hellman-Group5**, **Diffie-Hellman-Group14**, **Diffie-Hellman-Group15**, **Diffie-Hellman-Group19**, or **Diffie-Hellman-Group20**.

l2tp ipsec phase 2 proposal (*p2name*) [**replace** [**yes**]]

Assign a phase 2 proposal to the tunnel.

p2name is an existing phase 2 proposal on the device.

replace — replaces the existing phase 2 proposal for this tunnel with the specified proposal.
If **replace** is not specified, then the phase2 proposal is added to the existing phase 2 proposals for this tunnel. Use **yes** with **replace** to confirm that you want to replace the existing phase 2 proposals for this tunnel. This avoids the confirmation prompt.

Use **show proposal p2** to see a list of existing phase 2 proposals. Use **proposal p2** to create a new one.

l2tp (*network-attribute*)

Set the network options in the Mobile VPN for L2TP configuration.

network-attribute must be one of these options:

keep-alive-interval (*timeout*) — Set the keep alive timeout. The specifies how often the Firebox sends the L2TP "Hello" message. *timeout* is the number of seconds. The default value is 60 seconds.

max-retries (*retries*) — Set the maximum retries. This is the maximum number of times the Firebox will retransmit a message. If the maximum retries is exceeded, the Firebox closes the connection. *retries* must be a value from 3 to 30. The default value is 5.

mru (*mru-size*) — Set the Maximum Receive Unit (MRU). This is the maximum packet size to send in the PPP session through the L2TP tunnel. *mru-size* must be a value from 500 to 1500. The default value is 1400 bytes.

mtu (*mtu-size*) — Set the Maximum Transmission Unit (MTU). This is the maximum packet size to send in the PPP session through the L2TP tunnel. *mtu-size* must be a value from 500 to 1500. The default value is 1400 bytes.

retransmit-timeout (*timeout*) — Set the retransmission timeout. This is the number of seconds the Firebox waits for a message acknowledgement. A message will be retransmitted if the Firebox does not receive an acknowledgment in this time frame. *timeout* must be a value from 0 to 300. The default value is 5 seconds.

l2tp password (*password*)

The **l2tp password** command is a legacy command for the WatchGuard Mobile VPN app for iOS. This app is no longer available or supported.

Set the password to use for encryption of the .wgm file that you can generate for the WatchGuard Mobile VPN app for iOS. iOS users must use this password to decrypt the file.

password is the encryption password. It must be a string between 1 and 32 characters in length.

l2tp server (*address*)

Set the IP address or domain name of the Firebox you want the WatchGuard Mobile VPN app to use for L2TP connections.

address must be one of these options:

domain-name *domain-name* — The domain you want the L2TP clients to connect to. *domain-name* is the string that represents the domain name.

ip *ip-address* — The IP address of the Firebox interface you want the L2TP clients to connect to. *ip-address* must be an IPv4 address in the format A.B.C.D.

Example

```
l2tp address-pool range 10.0.10.1 10.0.10.100
l2tp auth-server RADIUS default
l2tp auth-user-group specify-user-group
l2tp auth-user-group specify-user-group group sales radius
l2tp enable
l2tp ipsec phase1 pre-shared S3kretKey
l2tp ipsec phase1 transform 2 up
l2tp ipsec phase1 transform sha1 AES 8 unit hour Diffie-Hellman-Group5
```

mvpn-ikev2

Description

Configure your Firebox to use Mobile VPN with IKEv2.

mvpn-ikev2 all-traffic-allow enable

(Fireware v12.9 or higher) Send all traffic from VPN clients through the VPN tunnel. This option is also known as full tunneling or default route. This is the default setting.

To enable split tunneling, enter **no mvpn-ikev2 all-traffic-allow enable**. Next, enter **mvpn-ikev2 resource-addr** to specify which network resources mobile VPN users can connect to.

mvpn-ikev2 auth-server (*authentication server*) **default**

auth-server must be Firebox-DB or RADIUS.

Use **mvpn-ikev2 auth-server RADIUS default** to configure RADIUS as the default authentication server.

Use **mvpn-ikev2 auth-server Firebox-DB default** to configure Firebox-DB as the default authentication server.

mvpn-ikev2 auth-user-group default

Select the default user group, which is *IKEv2-Users*.

mvpn-ikev2 auth-user-group specify-user-group *(authentication user type) (user or group name) (authentication server)*

authentication user type must be **user** or **group**.

authentication server must be Firebox-DB or RADIUS.

mvpn-ikev2 certificate *(certificate type) (certificate ID number)*

Certificate type must be one of these options:

default — Default certificate signed by the Firebox.

third-party — A third-party certificate. *(certificate ID number)* is the ID number that identifies the certificate. Use **show certificate** to see a list of certificates and certificate IDs.

mvpn-ikev2 certificate default dns*(domain name)*

Specify a domain name for IKEv2 user connections to this Firebox.

mvpn-ikev2 certificate default ip *(ip address)*

Specify an IP address for IKEv2 user connections to this Firebox.

mvpn-ikev2 phase1 dpd enable *(traffic idle timeout) (max retries)*

Enable dead peer detection (DPD) and configure the timeout and max retries values.

mvpn-ikev2 phase1 ike-keep-alive enable *(message interval) (max retries)*

Enable IKE keep alive and configure the message interval and max retries values.

mvpn-ikev2 phase2 pfs *(Diffie-Hellman group number)*

Enable perfect forward secrecy (PFS) and specify a Diffie-Hellman group.

mvpn-ikev2 phase2 proposal *(Phase 2 proposal name)*

Specify a Phase 2 proposal from the Phase 2 Proposals list.

mvpn-ikev2resource-addr(Host IP address or network IP address)

(Fireware v12.9 or higher) Allow Mobile VPN with IKEv2 users to connect to only specified resources on your internal networks. This option is also known as split tunneling.

To configure split tunneling, use this command to specify allowed resources before you enter the **no mvpn-ikev2 all-traffic-allow enable** command to enable split tunneling.

To delete a resource from the list, enter **no mvpn-ikev2 resource-addr** and the host IP address or network IP address.

mvpn-ikev2 virtual-addr

Configure the virtual IP address pool. **virtual-addr** must be one of these options:

host-ip — Specify an IP address for the virtual IP address pool.
network — Specify a network IP address for the virtual IP address pool.
range-ip — Specify an IP address range for the virtual IP address pool.

Example

```
mvpn-ikev2 phase1 dpd enable 120 5
mvpn-ikev2 phase1 ike-keep-alive enable 120 5
mvpn-ikev2 phase2 pfs enable dh-group2
mvpn-ikev2 phase2 proposal ESP-AES256-SHA256
mvpn-ikev2 cert default dns server.example.com
mvpn-ikev2 cert default ip 203.0.113.2
```

mvpn-ipsec

Description

Configure your Firebox to use Mobile VPN with IPSec.

Syntax

mvpn-ipsec (*name*)

Add or edit a Mobile VPN with IPSec group.

name is the Mobile VPN with IPSec group name.

Use **no mvpn-ipsec** (*name*) to disable.

After you type the command **mvpn-ipsec** *name*, the CLI continues to the initial Mobile VPN with IPSec configuration command.

The prompt changes to: `WG(config/policy/mvpn-name)#`

Use the **Exit** command to exit this mode.

auth-server (*auth-svr*) (*authmethod*) (*is-force-all*) (*ip-pool*)

Set initial configuration of Mobile VPN with IPSec.

auth-svr is the authentication server used for Mobile VPN with IPSec. It must be one of these options: **Firebox-DB**, **RADIUS**, **LDAP**, or **SecurID**. Or, to use Active Directory authentication, specify the domain name of a configured Active Directory server.

authmethod is the authentication method used for the tunnel. Must be one of these options:

(*rsa-svr-IP*) (*admin-passphrase*)

rsa-svr-IP is the RSA certificate server IP address

admin-passphrase is the administrator passphrase of the RSA server.

tunnel-passphrase is the tunnel encryption passphrase.

is-force-all is a boolean to denote if it is a Captive Tunnel or Split Tunnel. Must be one of these options: **no** (*tunnel-resource*) or **yes**

tunnel-resource is the address of the allowed resource in the format: *hostip* or *network-ip*

hostip is an IP address in the format A.B.C.D.

network-ip is a network address and mask in the format A.B.C.D./#, where # is a number from 0 to 32.

ip-pool is the address to assign to mobile computers that connect with Mobile VPN with IPSec. The address has the format: **host-ip** (*hostip*) or **range-ip** (*start-ip*) (*end-ip*)

hostip is an IP address in the format A.B.C.D.

start-ip is the start of a range of IP addresses in the format A.B.C.D.

end-ip is the end of a range of IP addresses in the format A.B.C.D.

After you use the **auth-server** command, the other Mobile VPN with IPSec configuration commands are available. Use these commands to edit the initial configuration if you do not want to use the default values. You must use the **Apply** command before your changes are enabled.

all-traffic-allow enable

Force all traffic through the tunnel.

Use **no all-traffic-allow** (*tunnel-resource*) to disable this command.

tunnel-resource is the address of the allowed resource in the format: *hostip* or *network-ip*

hostip is an IP address in the format A.B.C.D.

network-ip is a network address and mask in the format A.B.C.D./#, where # is a number from 0 to 32.

auth-method (*authmethod*) [*timeout*]

Configure or edit the authentication method.

authmethod is the authentication method used for the tunnel. It must be one of these options:

rsa-svr-IP) (*admin-passphrase*)

rsa-svr-IP is the RSA certificate server IP address

admin-passphrase is the administrator passphrase of the RSA server.

tunnel-passphrase is the tunnel encryption passphrase.

timeout is the time in seconds before the certificate authority request times out. It must be an integer from 0 to 600; default is 25.

auth-server (*auth-svr*)

Set or replace the authentication server.

auth-svr is the authentication server used for Mobile VPN with IPSec. It must be one of these options: **Firebox-DB**, **RADIUS**, **LDAP**, **Active-Directory**, or **SecurID**.

firebox-ip [**primary** *primary-ip*] [**backup** *backup-ip*]

Set the primary and backup IP address of the Firebox or remove the backup IP address used in Mobile VPN with IPSec.

primary-ip is the primary external interface IP address.

backup-ip is the secondary external interface IP address.

You can use the command **no firebox-ip backup** to delete only the backup Firebox IP address.

line-management (*mode*) (*timeout*)

Set line management, for users with Mobile VPN with IPSec client software v10 or later.

mode is any of these options: **manual**, **automatic**, or **variable**.

timeout is an integer from 0 to 65535.

phase1 (*setting*)

Set or modify the Phase 1 settings. *setting* is one of these options:

authentication *authmethod* where *authmethod* must be one of these options : **MD5**, **SHA1**, **SHA2-256**, **SHA2-384**, or **SHA2-512**.

SHA2 options are not available on XTM 5 Series, 810, 820, 830, 1050, and 2050 devices. The hardware cryptographic acceleration in those models does not support SHA2.

encryption *encrypmethod* where *encrypmethod* must be: **DES**, **TRIPLE-DES**, **AES-124**, **AES-192**, or **AES-256**.

sa-life *duration* **unit** *unittype*

duration is an integer from 0 to 35791394 minutes or 596523 hours.
unittype is either: **minute** or **hour**.

key-group (*grouptype*) where *grouptype* must be: **dh-group1**, **dh-group2**, or **dh-group5**,**dh-group14**, **dh-group15**, **dh-group19**, **dh-group20**.

nat-traversal enable (*interval*) where *interval* is an integer from 0 to 2147483647.

ike-keep-alive enable (*interval*) (*max-failures*)

interval is an integer from 0 to 300.
max-failures is an integer from 1 to 30.

dpd enable (*timeout*) (*max-retries*)

timeout is an integer from 10 to 300.
max-retries is an integer from 1 to 30.

phase2 (*setting*)

Set or modify a phase 2 settings. *setting* is one of these options:

authentication *authmethod* where *authmethod* must one of these options : **MD5**, **SHA1**, **SHA2-256**, **SHA2-384**, or **SHA2-512**.

SHA2 options are not available on XTM 5 Series, 810, 820, 830, 1050, and 2050 devices. The hardware cryptographic acceleration in those models does not support SHA2.

encryption *encrypmethod* where *encrypmethod* must be: **DES**, **TRIPLE-DES**, **AES-124**, **AES-192**, or **AES-256**.

key-expiration-time enable *lifetime kbytes unittype*

lifetime is an integer from 0 to 2147483647; default is 8.
kbytes is an integer from 1 to 2147483647.
unittype is either **hour** or **minute**.

If you set both the *lifetime* and *kbytes* to 0, the key expiration interval is set to 8 hours. If you set *kbytes* to less than 24,576 kilobytes, then 24,576 kilobytes is used. The maximum time before a forced key expiration is one year.

pfs enable (*group*)

group is one of these options: **dh-group1**, **dh-group2**, or **dh-group5**,**dh-group14**, **dh-group15**, **dh-group19**, **dh-group20**.

resource-addr (*tunnel-resource*)

Specify the allowed resources for Mobile VPN with IPSec.

tunnel-resource is the address of the allowed resource in the format: *hostip* or *network-ip*

hostip is an IP address in the format A.B.C.D.

network-ip is a network address and mask in the format A.B.C.D./# where # is a number from 0 to 32.

timeouts (*option*) (*time*)

Set the session and idle timeouts. If the authentication server is also configured with these timeouts, the server configuration takes precedence over these settings

option is either **idle** or **session**.

time is the idle or session timeout in minutes, an integer from 0 to 43200.

virtual-addr (*ip-pool*)

Set the IP address pool that is assigned to mobile computers that connect with Mobile VPN with IPSec.

ip-pool is the pool of IP addresses in the format: : **host-ip** (*hostip*) or **range-ip** (*start-ip*) (*end-ip*)

hostip is an IP address in the format A.B.C.D.

start-ip is the start of a range of IP addresses in the format A.B.C.D.

end-ip is the end of a range of IP addresses in the format A.B.C.D.

Example

```
mvpn-ipsec MVPNIPSecUsers
auth-server Firebox-DB mypassphraze3 yes host-ip 192.168.113.100
auth-server ad-domain.com mypassphraze3 yes host-ip 192.168.113.100
resource-addr host-ip 192.168.110.86
virtual-addr range-ip 192.168.100.50 192.168.100.100
```

mvpn-rule

Description

Configure Mobile User VPN with IPSec policy rules.

Syntax

mvpn-rule (*name*)

name is the rule name to assign to the Mobile VPN IPSec policy rules.

Use **no mvpn-rule** (*name*) to delete rule.

After you type the command **mvpn-rule** (*name*), the CLI continues to the selection of the Mobile VPN with IPSec group to which the Mobile VPN rules are applied.

The prompt changes to: `WG(config/policy/mvpnrule-name)#`

Use the **Exit** command to exit this mode.

mvpn-rule (*name*) (*policy-type*)

Select the policy type to be applied to the Mobile VPN with IPSec group.

name is the existing Mobile VPN with IPSec group name to which the rule is applied.

policy-type is a pre-defined policy types assigned to the rule.

After you enter the command **mvpn-rule** (*name*) (*policy-type*), a range of new commands is available to configure the rule details. You must use the **Apply** command to enable your changes.

(*option*) **enable**

Enable Mobile VPN with IPSec rule options.

option must be one of these options:

auto-block — auto block external sites that attempt to connect.
icmp-message allow-all — permit all ICMP error messages.
icmp-message fragmentation-required — fragmentation is required, but DF bit is set.
icmp-message host-unreachable — the send host is unreachable.
icmp-message network-unreachable — the send network is unreachable.
icmp-message port-unreachable — the send port is unreachable.
icmp-message protocol-unreachable — the send protocol is unreachable.
icmp-message time-exceeded — the time to live is exceeded in transit.
icmp-message use-global — use global settings in the response.

firewall *action*

action must be one of these options: **allowed**, **denied**, or **reject** (*option*).

If you select the *reject* action, *option* must be added as one of these options: ICMP_HOST, ICMP_NETWORK, ICMP_PORT, ICMP_PROTOCOL, or TCP_RST.

idle-time (*time*)

Specify the custom idle timeout for the rule.

time is the timeout in seconds. This must be an integer from 0 to 2147483647. A value of 0 disables this function.

logging (*option*)

Configure logging settings specific to the rule.

option must be one of these options:

log-message enable — send a log message to see in traffic monitor and to use in reports (except for packet filter policies).

log-message-reports enable — (packet filter policies only) send a log message to use in reports.

snmp-trap enable — send an SNMP trap.

notification enable (**action-type** *type*) [**launch-interval** *interval*] [**repeat-count** *count*] — send notification, where:

type is either **email** or **pop-window**. The default is email.

interval is the launch interval in minutes from 1 to 65535. The default is 15.

count is the repeat count; an integer from 1 to 256. The default is 10.

Use **no logging log-message enable** to disable log messages.

Use **no logging log-message-reports enable** to disable log messages used for reports (packet filter policies only)

Use **no logging snmp-message enable** to disable SNMP traps.

Use **no logging notification** to disable notification.

proxy-action (*action*)

Apply the matching default proxy actions for the rule.

action must be one of these options: **DNS-Outgoing**, **DNS-Incoming**, **FTP-Client**, **FTP-Server**, **HTTP-Client**, **HTTP-Server**, **POP3-Client**, **POP3-Server**, **SMTP-Outgoing**, **SMTP-Incoming**, **TCP-UDP-proxy**, **H.323-Client**, **SIP-Client**, **DNS-Incoming**, **HTTPS-Client**, or **HTTPS-Server**.

qos enable

Override QoS settings for an interface if Traffic Management and QoS are enabled.

No available options.

qos marking *type* (*method*) [**priority-method** *p-method*]

type must be either **dscp** or **precedence**.

method must be either **assign** *m-value* or **preserve**.

If *type* is **dscp**, *m-value* must be one of these options: **Best-effort**, **CS1-Scavenger**, **AF11**, **AF12**, **AF13**, **CS2**, **AF21**, **AF22**, **AF23**, **CS3**, **AF31**, **AF32**, **AF33**, **CS4**, **AF41**, **AF42**, **AF43**, **CS5**, **EF**, **Control-CS6**, or **Control-CS7**.

If *type* is **precedence**, *m-value* is an integer from 0 (normal) to 7 (highest).

p-method is a string. It must be one of these options: **No_Priority**, **Customized** *c-value*, **Mapped-from-Marking**.

c-value is an integer from 0 (normal) to 7 (highest).

schedule (*sked-name*)

Assign an existing schedule to the policy.

sked-name is the name of a schedule that was already created.

specify-user (*name*) (*auth-svr*)

Assign a specific user to the policy.

name is an existing user name.

auth-svr must be one of these options: Firebox-DB, RADIUS, LDAP, SecurID, or Active-Directory.

traffic-mgmt (*tm-name*)

Assign an existing traffic management action to the policy.

tm-name is the traffic management rule that was already created.

Example

```
mvpn-rule MVPNIPSecRule1
mvpn-ipsec MVPNIPSecUsers HTTP-proxy
logging notification enable action-type email launch-interval 10 repeat-count 50
qos marking dscp assign AF11 priority-method Customized 5
schedule wkdays-only
```

one-to-one-nat

Description

Create a 1-to-1 NAT table.

Syntax

one-to-one (*type*) (*nataddress*) (*realaddress*) (*interface*)

type must be one of these options: **host**, **subnet**, or **range**.

nataddress is the address visible to the insecure network.

realaddress is the real address on the protected network.

interface is the name of the interface used for 1-to-1 NAT.

Example

```
one-to-one host 203.28.18.2 192.168.110.24 External
```

policy-tag

Description

Configure policy tags to use for policy grouping.

Syntax

policy-tag (*tagname*) **color** (*color-code*)

Create a policy tag that you can assign to policies to organize your policies into easy to manage groups.

tagname is the name of the policy tag.

color-code is the hexadecimal color code. Each code corresponds to a tag color that appear in Policy Manager and Fireware Web UI.

The color code must be one of these options:

Row1:	0x000000	0x808080	0xc0c0c0	0x400000	0x800000	0x804040
Row2:	0x804000	0xff0000	0x004040	0x004000	0x008000	0x408040
Row3:	0x000080	0x000040	0x0000ff	0x800080	0x800040	0xff0080

To remove a policy-tag, use **no policy-tag** (*tagname*).

policy-tag (*oldname*) **rename** (*newname*)

Change the name of an existing policy tag.

oldname is the current name of the policy tag.

newname is the name you want to change it to.

Example

```
policy-tag sales color 0x80400

policy-tab sales rename inside-sales
```

policy-type

Description

Create a custom policy template.

Syntax

policy-type (*name*) [*timeout*] **protocol** (*protocol-type*)

Create a custom policy template that can be used to create firewall policy actions.

name is a unique string to identify the policy template. You cannot use spaces.

timeout is the idle timeout in seconds. It must be an integer from 0 to 65535. The default is 180.

protocol-type must be one of these options:

ah
any
esp
gre
icmp *type code*
type must be an integer from 0 to 255.
code must be an integer from 0 to 255.
icmpv6*typecode*
type must be an integer from 0 to 255.
code must be an integer from 0 to 255.
igmp
ip *protocol-number*
protocol-number must be an inter from 3 to 255.
ospf
tcp port-range *start-port end-port*
start-port and *end-port* must each be an integers from 1 to 65535.
tcp *port*
udp port-range *start-port end-port*
start-port and *end-port* must each be an integers from 1 to 65535.
udp *port*
port must be an integers from 1 to 65535.

Example

```
policy-type funkydb.1 protocol udp 60002
```

proposal

Description

Create phase 2 proposals for IPSec VPN.

Syntax

proposal p2 (*p2name*) (*p2type*) **transform** (*life-time*) (*life-size*) (*encryption*) (*authentication*)

Configure the phase 2 proposal details.

p2name is a unique string to identify the IPSec phase 2 proposal.

p2type is the phase 2 proposal type. It must be either **ah**, or **esp**.

life-time and *life-size* are used to force key expiration

life-time is the SA life time in minutes from 1 to 35791394.

life-size is the SA life size in kilobytes from 1 to 2147483647.

If *life-time* or *life-size* is set to 0, that key expiration option is disabled.

If both *life-time* and *life-size* are set to 0, the key expiration interval is set to 8 hours.

encryption is the encryption algorithm for Encapsulated Security Payload (ESP) type only. If type is Authentication Header (AH) this argument is omitted. It must be one of these options: **none**, **des**, **3des**, **aes128**, or **aes192**. In Fireware v12.2 or higher, you can also specify **aes256**, **aes128-gcm**, **aes192-gcm**, or **aes256-gcm**.

authentication is the authentication algorithm.

For AH proposal type, it must be one of these options: **MD5**, **SHA1**, **SHA2-256**, **SHA2-384**, or **SHA2-512**.

For ESP proposal type , it must be one of these options: **none**, **MD5**, **SHA1**, **SHA2-256**, **SHA2-384**, or **SHA2-512**.

SHA2 options are not available on XTM 5 Series, 810, 820, 830, 1050, and 2050 devices. The hardware cryptographic acceleration in those models does not support SHA2.

Example

```
proposal p2 p2esp esp transform 480 1024 aes256 md5
proposal p2 p2ah ah transform 1440 2048 sha1
```

quarantine-server

Description

Configure the IP address and port number for a WatchGuard Quarantine Server.

Syntax

quarantine-server (*ip-address*) [port]

Configure the IP address and port for the Firebox to connect to a Quarantine Server.

ip-address is the IPv4 address of a configured Quarantine Server in the format A.B.C.D.

port is the port number the Quarantine Server. The default value is 4120.

Use **no quarantine-server** to reset Quarantine Server configuration settings to the default values.

Example

```
quarantine-server 203.0.113.20
```

reputation-enabled-defense

Description

Configure settings for Reputation Enabled Defense feedback.

Syntax

reputation-enabled-defense feedback enable

Enable the Firebox to send encrypted scan results to WatchGuard servers to improve overall coverage and accuracy.

Use **no reputation-enabled-defense feedback enable** to disable feedback.

rule

Description

Configure a firewall policy.

Syntax

rule (*name*)

name is the name of the firewall policy to add or edit.

Use **no rule** (*name*) to delete the firewall policy.

After you type the command rule name the CLI provides additional options to configure policy properties.

The prompt changes to “WG(config/policy/rule-name)#”.

Use the **Exit** command to exit this mode. Use the **Apply** command to apply your policy changes to the device configuration.

policy-type (*p-type*) **from** (*source*) **to** (*destination*)

Select the Policy Type to be applied to the rule.

p-type is the policy type. It is case sensitive. To see the list of available policy types use the command **show policy-type**.

source is any or a combination of these options:

alias *if-alias* — *if-alias* is the interface name (alias) of the traffic source. It is case-sensitive. It must be one of the default aliases: **Trusted**, **Optional**, **External**, **Any-Trusted**, **Any-Optional**, or **Any-External** or any other interface alias you created.

custom-address *if-alias* (**address** *address-format*) (**user-group** *type name authsvr*) (**device-group** *group-name*)

if-alias is an interface name (alias) for the traffic source

address-format must be one of these options:

- **host-ip** *ip* — *ip* must be an IPv4 host address in the format A.B.C.D

- **host-range** *startip endip* — *startip* and *endip* must be IPv4 addresses in the format A.B.C.D

- **network-ip** *net* — *net* must be an IPv4 subnet in the format A.B.C.D/# where # is in the range of 0 to 32

type is either **user** or **group**.

name is the user name or group name.

authsvr is one of these options: **Firebox-DB**, **RADIUS**, **LDAP**, **SecurID**, or **Active-Directory**.

mobile-device-group is one of these options: **Any-Android**, **Any-iOS**, **Any-Mobile**.

group-name must be one of these mobile device groups: **Any-Mobile**, **Any-iOS**, or **Any-Android**.

device-group *group-name* — *group-name* must be one of these mobile device groups: **Any-Mobile**, **Any-iOS**, or **Any-Android**.

host-ip *ip* — *ip* must be an IPv4 host address in the format A.B.C.D

host-range *startip endip* — *startip* and *endip* must be IPv4 addresses in the format A.B.C.D

network-ip *net* — *net* must be an IPv4 subnet in the format A.B.C.D/# where # is in the range of 0 to 32

host6-ip *ip* — *ip* must be an IPv6 host address in the format A:B:C:D:E:F:G:H

host6-range *startip endip* — *startip* and *endip* must be IPv6 addresses in the format A:B:C:D:E:F:G:H

network6-ip *net* — *net* must be an IPv6 subnet in the format A:B:C:D:E:F:G:H/I.

tunnel-address (*bovpn*) — *bovpn* is the branch office VPN tunnel name.

user-group *type* **name** *authsvr*

wildcard *(wildcard IP address) (wildcard netmask)* — *(wildcard IP address)* must be an IPv4 address in the format A.B.C.D. *(wildcard netmask)* must be in the format E.F.G.H.

destination is any or a combination of these options:

alias *if-alias* — *if-alias* is the interface name (alias) of the traffic destination. It is case-sensitive. It must be one of the default aliases: **Trusted**, **Optional**, **External**, **Any-Trusted**, **Any-Optional**, or **Any-External** or any other interface alias you created.

custom-address*if-alias* (**address** *address-format*) (**user-group***typenameauthsvr*) (**device-group** *group-name*)

if-alias is an interface name (alias) for the traffic destination.

address-format must be one of these options:

- **host-ip** *ip* — *ip* must be an IPv4 host address in the format A.B.C.D

- **host-range***startipendip* — *startip* and *endip* must be IPv4 addresses in the format A.B.C.D

- **network-ip***net* — *net* must be an IPv4 subnet in the format A.B.C.D/# where # is in the range of 0 to 32

type is either **user** or **group**.

name is the user name or group name.

authsvr is one of these options: **Firebox-DB**, **RADIUS**, **LDAP**, **SecurID**, or **Active-Directory**.

group-name must be one of these mobile device groups: **Any-Mobile**, **Any-iOS**, or **Any-Android**.

device-group *group-name* — *group-name* must be one of these mobile device groups: **Any-Mobile**, **Any-iOS**, or **Any-Android**.

host-ip *ip* — *ip* must be an IPv4 host address in the format A.B.C.D

host-range *startipendip* — *startip* and *endip* must be IPv4 addresses in the format A.B.C.D

host6-ip *ip* — *ip* must be an IPv6 host address in the format A:B:C:D:E:F:G:H

host6-range *startipendip* — *startip* and *endip* must be IPv6 addresses in the format A:B:C:D:E:F:G:H

network-ip *net* — *net* must be an IPv4 subnet in the format A.B.C.D/# where # is in the range of 0 to 32

network6-ip *net* — *net* must be an IPv6 subnet in the format A:B:C:D:E:F:G:H/I.

snat *snat-name* — *snat-name* must be the name of a static NAT or server load balancing SNAT action.

tunnel-address (*bovpn*) — *bovpn* is the branch office VPN tunnel name.

user-group *type* **name** *authsvr*

wildcard *(wildcard IP address) (wildcard netmask)* — *(wildcard IP address)* must be an IPv4 address in the format A.B.C.D. *(wildcard netmask)* must be in the format E.F.G.H.

After you type the command *policy-type p-type from source to destination*, a new range of commands is available to configure the rule details. You must use the **Apply** command to apply your policy changes to the device configuration.

app-control (*action-name*)

Enable Application Control for the specified rule.

action-name is the name of a configured Application Control action. It is case sensitive.

auto-block enable

Configure the policy to temporarily block sites that try to use a denied service. IP addresses from the denied packets are added to the Temporary Blocked sites list for 20 minutes (by default). This command applies only to a policy that has the firewall action set to **denied** or **reset**.

dynamic-nat (*switch*)

Enable dynamic NAT for traffic controlled by the specified rule.

switch must be one of these options:

disable

enable *function* — where *function* is one of these options:

network-nat-setting — use the dynamic NAT rules set for this Firebox.

all-traffic-in-policy [*ip-address*] — apply dynamic NAT to all traffic in this policy. *ip address* is the dynamic NAT source IP address, in the format A.B.C.D.

When you enable dynamic NAT for all traffic in the policy, the source IP address is optional, unless the policy is also configured for policy-based routing to a BOVPN virtual interface, and the BOVPN virtual interface does not have a virtual IP address configured.

[*no*] **enable**

Enable the specified rule.

Use **no enable** to disable the specified rule.

firewall (*action*)

Set the firewall action for the specified rule.

action must be one of these options:

allowed — Connections are allowed

denied — Connections are denied

reset *resetaction* — Connections are denied (send reset), *resetaction* specifies the reset action. It must be one of these options:

imcp_host — Send ICMP host unreachable

imcp_network — Send ICMP network unreachable

icmp_port — Send ICMP port unreachable

icmp_protocol — Send ICMP protocol unreachable

tcp_rst — Send TCP RST

from (*source*)

Edit the source field of an existing policy.

source is any or a combination of these options:

alias *if-alias* — *if-alias* is the interface name (alias) of the traffic source. It is case-sensitive. It must be one of the default aliases: **Trusted**, **Optional**, **External**, **Any-Trusted**, **Any-Optional**, or **Any-External** or any other interface alias you created.

custom-address *if-alias* (**address** *address-format*) (**user-group** *type name authsvr*) (**device-group** *group-name*)

if-alias is an interface name (alias) for the traffic source

address-format must be one of these options:

- **host-ip** *ip* — *ip* must be an IPv4 host address in the format A.B.C.D

- **host-range** *startip endip* — *startip* and *endip* must be IPv4 addresses in the format A.B.C.D

- **network-ip** *net* — *net* must be an IPv4 subnet in the format A.B.C.D/# where # is in the range of 0 to 32

- **FQDN** *fqdn-site* is a Fully Qualified Domain Name. This includes wildcard domains. For example, *host.example.com*, or *"*.example.com"*.

type is either **user** or **group**.

name is the user name or group name.

authsvr is one of these options: **Firebox-DB**, **RADIUS**, **LDAP**, **SecurID**, or **Active-Directory**.

group-name must be one of these mobile device groups: **Any-Mobile**, **Any-iOS**, or **Any-Android**.

device-group *group-name* — *group-name* must be one of these mobile device groups: **Any-Mobile**, **Any-iOS**, or **Any-Android**.

host-ip *ip* — *ip* must be an IPv4 host address in the format A.B.C.D

host-range *startip endip* — *startip* and *endip* must be IPv4 addresses in the format A.B.C.D

network-ip *net* — *net* must be an IPv4 subnet in the format A.B.C.D/# where # is in the range of 0 to 32

host6-ip *ip* — *ip* must be an IPv6 host address in the format A:B:C:D:E:F:G:H

host6-range *startip endip* — *startip* and *endip* must be IPv6 addresses in the format A:B:C:D:E:F:G:H

network6-ip*net* — *net* must be an IPv6 subnet in the format A:B:C:D:E:F:G:H/I.

tunnel-address (*bovpn*) — *bovpn* is the branch office VPN tunnel name.

user-group *type* **name** *authsvr*

wildcard *(wildcard IP address) (wildcard netmask)* — *(wildcard IP address)* must be an IPv4 address in the format A.B.C.D. *(wildcard netmask)* must be in the format E.F.G.H.

FQDN *fqdn-site* is a Fully Qualified Domain Name. This includes wildcard domains. For example, *host.example.com*, or *"*.example.com"*.

geolocation deny-page enable

Enable the Geolocation deny page for HTTP/HTTPS traffic. The deny page applies to inbound HTTP and HTTPS traffic on ports 80 and 443. Available in Fireware v12.8 and higher.

Use **no geolocation deny-page enable** to disable the deny page.

geolocation enable

Enable Geolocation Blocking for the specified rule. Valid if the Geolocation service is enabled on the Firebox.

Use **no geolocation enable** to disable Geolocation Blocking for the rule.

geolocation (action)

Specify the geolocation action to use for the specified rule.

(action) must be a geolocation action configured on the Firebox.

icmp-message (*action*)

Set the traffic action for ICMP messages.

action must be one of these options: **use-global**, **allow-all**, **deny-all**, or *option*.

option can be any combination of these options: **fragmentation-required**, **time-exceeded**, **network-unreachable**, **host-unreachable**, **protocol-unreachable**, and **port-unreachable**.

idle-timeout (*length*)

Set the idle timeout in seconds.

length is the idle timeout in seconds. It must be an integer from 0 to 2147483647.

ips-monitor

Enable or disable the IPS-Monitor feature of the specified rule.

No options available.

Use **no ips-monitor** to disable the feature.

logging (*option*)

Configure logging settings specific to the rule.

option must be one of these options:

log-message enable — send log message.

snmp-trap enable — send SNMP trap.

notification enable (**action-type** *type*) [**launch-interval** *interval*] [**repeat-count** *count*] — send notification, where:

type is either **email** or **pop-window**. The default is email.

interval is the launch interval in minutes from 1 to 65535. The default is 15.

count is the repeat count; an integer from 1 to 256. The default is 10.

Use **no logging log-message enable** to disable log messages.

Use **no logging snmp-message enable** to disable SNMP traps.

Use **no logging notification** to disable notification.

move (*location*)

Move the policy to a numbered location.

location is the desired location of the policy.

one-to-one-nat (*switch*)

Select whether to use 1-to-1 NAT for the policy. The default is to use 1-to-1 NAT.

switch is either **0** (disable) or **1** (enable).

policy-routing backup (*primary-ext*) **failover** (*backup-ext* ...)

(Fireware v12.2.1 or lower) Configure policy-based routing. In Fireware v12.3 or higher, SD-WAN replaces policy-based routing, and the **sd-wan** command replaces the **policy-routing** command.

primary-ext is the alias of the primary external interface or BOVPN virtual interface for the policy.

backup-ext is the alias of the backup external interface for the policy. You can assign more than one backup external interface to a policy. You cannot assign a backup external interface if *primary-ext* is a BOVPN virtual interface.

policy-tag (*tagname* ...)

Assign one or more policy tags to the policy. To assign more than one policy tag, separate each tag name with a space.

tagname is the name of a configured policy tag.

Use **show policy-tag** to see a list of available policy tags you can assign.

To create a new policy tag, use the **policy-tag** command when you are not editing a rule.

You must use the **Apply** command for a new policy before you can assign a policy tag.

proxy-action (*action*)

Assign a default proxy action to a policy.

action is the default proxy action on the device. To see the list of proxy actions, you can execute the command **show proxy-action**.

qos enable

For each interface, enable or disable the QoS feature of the specified rule.

No options available.

Use **no qos enable** to disable QoS for this rule.

qos marking dscp (*state*) [**priority-method** *method*]

For each interface, override QoS settings for the traffic controlled by the specified rule.

state is the DSCP state and must be either **assign** (*type*) or **preserve**.

type is the DSCP assign method and must be one of these values: **Best-effort**, **CS1-Scavenger**, **AF11**, **AF12**, **AF13**, **CS2**, **AF21**, **AF22**, **AF23**, **CS3**, **AF31**, **AF32**, **AF33**, **CS4**, **AF41**, **AF42**, **AF43**, **CS5**, **EF**, **Control-CS6**, or **Control-CS7**.

method is the method used to assign priority, and must be one of these values: **No_ Priority**, **Customer**, or **Mapped-from-Marking**.

qos marking precedence (*state*) [**priority-method** *method*]

For each interface, override QoS precedence for the traffic controlled by the specified rule.

state is the precedence state and must be either **assign** (*value*) or *preserve*.

value is the precedence value. It must be an integer from 0 to 7.

method is the method used to assign priority, and must be one of these values: **No_ Priority**, **Customer**, or **Mapped-from-Marking**.

quota enable

Enable bandwidth and time quotas for this rule.

Use **no quota enable** to disable quotas for this rule.

schedule (*sched-name*)

Assign an existing schedule to the policy.

sched-name is the name of a schedule that was already created.

sd-wan *(SD-WAN action name)*

Apply an existing SD-WAN action to this policy.

To remove the SD-WAN action from this policy, use **no sd-wan**.

To add a new SD-WAN action, you must use the **sd-wan** command in Configuration mode instead of Policy mode.

to (*destination*)

Edit the destination field of an existing policy.

destination is any or a combination of these options:

alias *if-alias* — *if-alias* is the interface name (alias) of the traffic destination. It is case-sensitive. It must be one of the default aliases: **Trusted**, **Optional**, **External**, **Any-Trusted**, **Any-Optional**, or **Any-External** or any other interface alias you created.

custom-address *if-alias* (**address** *address-format*) (**user-group** *type name authsvr*) (**device-group** *group-name*)

if-alias is an interface name (alias) for the traffic destination.

address-format must be one of these options:

- **host-ip** *ip* — *ip* must be an IPv4 host address in the format A.B.C.D

- **host-range** *startip endip* — *startip* and *endip* must be IPv4 addresses in the format A.B.C.D

- **network-ip** *net* — *net* must be an IPv4 subnet in the format A.B.C.D/# where # is in the range of 0 to 32

- **network6-ip***net* — *net* must be an IPv6 subnet in the format A:B:C:D:E:F:G:H/I.

- **FQDN** *fqdn-site* is a Fully Qualified Domain Name. This includes wildcard domains. For example, *host.example.com*, or *"*.example.com"*.

type is either **user** or **group**.

name is the user name or group name.

authsvr is one of these options: **Firebox-DB**, **RADIUS**, **LDAP**, **SecurID**, or **Active-Directory**.

group-name must be one of these mobile device groups: **Any-Mobile**, **Any-iOS**, or **Any-Android**.

device-group *group-name* — *group-name* must be one of these mobile device groups: **Any-Mobile**, **Any-iOS**, or **Any-Android**.

host-ip *ip* — *ip* must be an IPv4 host address in the format A.B.C.D

host-range *startip endip* — *startip* and *endip* must be IPv4 addresses in the format A.B.C.D

host6-ip *ip* — *ip* must be an IPv6 host address in the format A:B:C:D:E:F:G:H

host6-range *startip endip* — *startip* and *endip* must be IPv6 addresses in the format A:B:C:D:E:F:G:H

network-ip *net* — *net* must be an IPv4 subnet in the format A.B.C.D/# where # is in the range of 0 to 32

network6-ip *net* — *net* must be an IPv6 subnet in the format A:B:C:D:E:F:G:H/I.

snat *snat-name* — *snat-name* must be the name of a static NAT or server load balancing SNAT action.

tunnel-address (*bovpn*) — *bovpn* is the branch office VPN tunnel name.

user-group *type* **name** *authsvr*

wildcard *(wildcard IP address) (wildcard netmask)* — *(wildcard IP address)* must be an IPv4 address in the format A.B.C.D. *(wildcard netmask)* must be in the format E.F.G.H.

FQDN *fqdn-site* is a Fully Qualified Domain Name. This includes wildcard domains. For example, *host.example.com*, or *"*.example.com"*.

traffic-mgmt (*direction*) (*action-name*)

Enable a traffic management action for the policy.

direction is the traffic direction. It must be one of these options:

forward — Configure the forward Traffic Management action. The forward action applies to traffic that originates from IP addresses in the **From** list configured in the policy (the source) to IP addresses in the **To** list (the destination).

reverse — Configure the reverse Traffic Management action. The Reverse action applies to traffic that originates from IP addresses in the **To** list configured in the policy (the destination) to IP addresses in the policy **From** list (the source).

action-name is the name of the configured Traffic Management action to use.

If the reverse action is a per-ip action, the action controls the bandwidth for traffic received per IP address in the **From** list. For example, in an FTP policy that handles traffic from Trusted to External, a per-ip action used as the reverse action controls the FTP download speed for each source IP address on the Trusted network.

You can configure a forward action, a reverse action, or both. If you configure a policy to use the same Traffic Management action as the forward and reverse action, the bandwidth settings in the Traffic Management action apply to the combined bandwidth of traffic in both directions.

Example

```
rule HTTP-proxy-Out
auto-block enable
policy-type HTTP-proxy from alias Any-Trusted to alias Any-External
geolocation enable
logging log-message enable
logging snmp-trap enable
policy-routing backup External-1 failover External-2
sd-wan VOIP.SDWAN
to snat snat.1
policy-tag sales
policy-type DNS from wildcard 10.0.0.3 255.255.0.255 to host-ip 203.0.113.2
```

schedule

Description

Build a schedule for use in policies.

Syntax

schedule (*name*) **time-block** (*entry*)

schedule (*name*) ((*period*) (*starthour*) (*startmin*) (*endhour*) (*endmin*))...

name is the name of the schedule.

period must be one of these options: **daily**, **mon**, **tue**, **wed**, **thu**, **fri**, **sat**, or **sun**.
starthour is the hour the period starts, and must be in the range of 0 to 23.
startmin is the minute the period starts, and must be in the range of 0 to 60.
endhour is the hour the period ends, and must be in the range of 0 to 23.
endmin is the minute the period ends, and must be in the range of 0 to 60.

You can define more than one period in this command.

Example

```
schedule releaseweek mon 5 30 19 30 tue 5 30 19 30
```

sip-proxy

Description

Configure SIP-ALG proxy settings.

Syntax

sip-proxy (*name*) **extended-rewrite** [*enable*]

Configure settings for SIP-ALG proxy action.

name is the name of the proxy action.

enable - Enable the Firebox to rewrite IP address information in the FROM: field in the SIP SDP header.

Use **no extended-rewrite** to disable this feature.

Example

```
sip-proxy STP-Client.1 extended-rewrite enable
```

spamblocker

Description

Configure global settings for the spamBlocker security service.

Syntax

spamblocker http-proxy-server [*enable*] (*hostname*|*ip-address*) [*port*] (*auth-type*) (*domain*) (*username*) (*password*)

Configure settings for the Firebox to connect to the spamBlocker Server through an HTTP proxy server.

enable - Enable the Firebox to connect to the spamBlocker Server through an HTTP proxy server.

hostname is the host name of the HTTP proxy server.

ip-address is the IP address of the HTTP proxy server.

port is the port to connect to for the HTTP proxy server. The default port is 8080.

auth-type specifies the authentication type and credentials to use for connections to the http proxy server. It must be one of these options:

basic — The HTTP proxy server uses basic authentication
noauth — The HTTP proxy server does not require authentication
ntlm — The HTTP proxy server uses NTLM authentication

domain is the domain name used for authentication to the HTTP proxy server.

username is the user name used for authentication to the HTTP proxy server.

password is the password used for authentication to the HTTP proxy server.

If you specify **no-auth**, *username*, *domain*, and *password* are not required.

spamblocker settings (*spam-setting*)

Configure general global spamBlocker settings.

spam-setting must be one of these options:

cache-size (*size*) — set the number of entries spamBlocker caches locally for messages that have been categorized as spam and bulk. *size* is the number of entries.

connection-string (*override*) — for debug use only. Use this only when you work with a WatchGuard technical support representative to troubleshoot a spamBlocker problem. *override* is the override string.

max-scan-size *size* — set the number of kilobytes of an email message to be passed to spamBlocker to be scanned. *size* must be an integer between 1 and 2000. The default value is 100.

proactive-patterns enable — enable proactive patterns.

vod enable [*max-size*] — enable Virus Outbreak Detection (VOD). *max-size* is the VOD maximum file size to scan, in kilobytes. Maximum and default values vary by device model.

spamblocker trusted-email-forwarders "(*address*)"

Configure host names or domain names of SMTP email servers or POP3 providers that you trust. This improves spam scoring accuracy.

address is either the IP address or host name of an SMTP server or POP3 provider. It must be enclosed in quotation marks. When you type a domain name, make sure you add a leading ".", for example ".example.com".

Examples

```
spamblocker http-proxy-server enable 203.0.113.20 basic example.com psmith
secrIt
```

```
spamblocker settings vod enable 1000
```

```
spamblocker trusted-email-forwarders ".example.net"
```

sslvpn

Description

Configure the device to enable Mobile VPN with SSL connections.

Syntax

sslvpn enable

Enable Mobile VPN with SSL on the device.

No options available.

Use **no sslvpn enable** to disable SSL VPN connections.

sslvpn auto-reconnect enable

Enable the Mobile VPN with SSL client to automatically reconnect when the connection is lost.

No options available.

Use **no sslvpn auto-reconnect enable** to disable automatic client reconnection.

sslvpn hand-window(value)

(Fireware v12.5.6, v12.5.7, v12.6.4, or v12.6.5) Configure the TLS handshake negotiation window for Mobile VPN with SSL. The default value is 60 seconds. You can run this command only for Mobile VPN with SSL configurations that use UDP as the data channel. We recommend that you change the default handshake window only if you encounter the issue described in KI 000018672.

value is the maximum amount of time, in seconds, allowed for the TLS negotiation.

sslvpn (**primary**|**backup**) (*address*)

Configure the external IP address or domain name for Mobile VPN with SSL users to connect to.

(**primary**|**backup**) configure the primary or backup IP address or domain name.

address is either the IP address of an external interface in the format A.B.C.D, or an alias for an external interface.

Use **no sslvpn** *server address* to disable a backup external interface for SSL VPN.

sslvpn (*type*) **servers** (*address*)

Configure Mobile VPN with SSL to use specific DNS or WINS servers.

type is either **dns** or **wins**.

address is the address of a WINS or DNS server. You can add up to two servers.

If *type* is **wins**, *address* must be an IP address in the format A.B.C.D.

If *type* is **dns**, *address* must be an IP address in the format A.B.C.D or a qualified domain name.

Use **no sslvpn** *type* **servers** *address* to remove a DNS or WINS server from the configuration.

sslvpn remember-connection enable

Allows the Mobile VPN with SSL client to remember the password.

Use **no sslvpn remember-connection enable** if you do not want the client to remember the password.

sslvpn resource (*method*)

Define what resources are available to Mobile VPN with SSL users.

method must be one of these options:

user-route (*net*), where *net* is a subnet address in the format A.B.C.D./#.

appliance-route — enables access to a directly connected network.

force-traffic — forces all traffic through the tunnel.

Use **no sslvpn resource user-route** (*net*) to remove a specified network from the configuration.

sslvpn resource default-route-client

(Fireware v12.5.3 or higher) When enabled for full-tunnel SSL VPN configurations, the Firebox sends the general route `0.0.0.0/0.0.0.0` to Mobile VPN with SSL clients on Windows computers. This option has no effect on computers with other operating systems. This option is intended as a workaround for an issue that affects Office 365 traffic. For more information, see Known Issue 000015131 in the WatchGuard Knowledge Base.

Use **no sslvpn resource default-route-client** to disable this option. When disabled, the Firebox sends the routes `0.0.0.0/1` and `128.0.0.0/1` to Windows computers.

sslvpn address-pool (*net*)

Define a subnet to be used as a virtual address pool.

net is a subnet address in the format A.B.C.D./#, where # is an integer from 0 to 32.

sslvpn algorithm (*type*) (*method*)

Select the authentication and encryption methods to use to secure SSL VPN connections.

type must be either **authentication** or **encryption**.

type specifies the authentication or encryption method.

If ***type*** is **authentication**, *method* must be one of these options: **SHA-1**, **SHA256**, or **SHA512**. The default method is **SHA256**.

If **type** is **encryption**, *method* must be one of these options: **3DES**, **AES-128**, **AES-192**, or **AES-256**. In Fireware v12.2 or higher, you can also specify **AES-128-GCM**, **AES-192-GCM**, or **AES-256-GCM**. The default method is **AES-256**.

sslvpn auth-server (*authentication*) [**default**][**force**]

Select a method to use to authenticate Mobile VPN with SSL users. You can add more than one authentication server. The authentication servers you specify must already be configured for the device.

authentication must be one of these options: **Firebox-DB**, **RADIUS**, **SecurID**, or **LDAP**. Or, to use Active Directory authentication, specify the domain name of a configured Active Directory server.

authentication must be the name of an authentication server. It must be one of these options:

Any — Any authentication server
Firebox-DB — Firebox database
RADIUS — RADIUS server
SecurID — SecurID server
LDAP — LDAP server
domain — Active Directory server domain name

Use **default** to designate the specified *authentication* server as the default authentication method.

Use **force** to require users to authenticate again after a connection is lost.

sslvpn auth-user-group (*option*) (*type*) (*name*) (*authentication*)

Add a new user or group for Mobile VPN with SSL authentication.

option must be **default** or **specify-user-group**.

Use **default** to use the default group name, SSLVPN-Users.
Use **specify-user-group** to add a new user or group for Mobile VPN with SSL authentication.

type is only needed if you use **specify-user-group**. It must be one of these options:

Use **user** to add a new user.
Use **group** to add a new group.

name must be the name of a user or group to add. The user or group must also exist on the *authentication* server specified for the group or user.

authentication must be the name of an authentication server enabled in the SSLVPN configuration. It must be one of these options:

Any — Any authentication server
Firebox-DB — Firebox database
RADIUS — RADIUS server
SecurID — SecurID server
LDAP — LDAP server
domain — Active Directory server domain name

sslvpn bridge *interface-name* (**start-addr** *startip endip*)

Configure Mobile VPN with IPSec to bridge to a bridge interface.

interface-name is the alias name of a bridge interface.

start-addr defines an address pool for the Mobile VPN with IPSec clients. The *startip* and *endip* IP addresses must be on the same subnet as the bridge interface.

startip is the first IP address in the address pool.
endip is the last IP address in the address pool.

sslvpn keepalive (*setting*) (*value*)

Configure SSL VPN keep-alive settings.

setting must be either **interval** or **timeout**.

value is measured in seconds and must be an integer.

The default value for the keep-alive interval is 10.
The default value for the keep-alive timeout is 60.

sslvpn protocol (*protocol*) (*port*)

Change the protocol and port used for the Mobile VPN with SSL data channel.

protocol must be either TCP or UDP. The default is TCP.

port must be an integer from 0 to 65535. The default is 443.

sslvpn config-port (*config-port*)

The **config-port** command exists only in Fireware v12.0.2 and lower. Use **config-port** to change the TCP port used to negotiate the SSL VPN data channel and to download Mobile VPN for SSL configuration files. You can change the config-port only if the sslvpn protocol is set to UDP. If the sslvpn protocol is set to TCP, the config-port uses the same port you specified with the sslvpn protocol command.

config-port must be an integer from 0 to 65535.

In Fireware v12.1 or higher, use **access-portal portal port** *(port)* in the CLI Configuration mode to specify the TCP port used to negotiate the SSL VPN data channel and to download Mobile VPN for SSL configuration files. This port setting is shared by the Access Portal and Mobile VPN with SSL.

sslvpn renegotiate (*interval*)

Set the number of minutes a connection can be active before the device forces a renegotiation of the tunnel.

interval must be an integer greater than 60. The default value is 60.

sslvpnweb-download

(Fireware v12.5.4 or higher) Configure whether users can download the Mobile VPN with SSL client from the software downloads page hosted by the Firebox at `https://[Firebox IP address]:[port]/sslvpn.html`.

To disable the software downloads page, specify **no sslvpn web-download enable**

To enable the software downloads page, specify **sslvpn web-download enable**

Example

```
sslvpn primary 100.100.100.10
sslvpn backup 50.50.50.20
sslvpn dns servers 10.1.2.4 10.1.2.5
sslvpn dns domain-name watchguard
sslvpn address-pool 192.168.113.0/24
sslvpn authentication SHA-1
sslvpn auth-server Firebox-DB
sslvpn auth-server my-ad-domain.com
sslvpn keepalive timeout 30
sslvpn renegotiate 90
sslvpn bridge BR-1 start-addr 10.0.50.1 10.0.50.100
```

traffic-management

Definition

Configure a traffic management action to use with policies or Application Control.

In the Traffic Management settings, 1 Kbps is equal to 1024 bits per second.

Syntax

traffic-management (*action-name*) (*action-type*) (*guaranteed-bandwidth*) (*max-bandwidth*) (*max-instance*)

action-name is the name of the Traffic Management action.

action-type is the type of Traffic Management action. It must be one of these options:

all-policies — the action settings apply to the combined bandwidth of all policies that use the action.

per-policy — the action settings apply individually to each policy that uses the action.

per-ip — the action settings apply individually to each source IP address for any policy that uses the action.

guaranteed-bandwidth is the minimum bandwidth, in Kbps, you would like to guarantee for traffic managed by this action. If set to 0, the action does not guarantee bandwidth.

max-bandwidth is the maximum bandwidth, in Kbps, to allocate for traffic managed by this action. If set to 0, the action does not limit bandwidth.

max-instance is the number of source IP addresses that can have separate bandwidth constraints, in a per-ip Traffic Management action. It must be an integer from 1 to 256. It is not used for an all-policies or per-policy action.

Use the command **no traffic-management** (*action-name*) to remove a configured Traffic Management action.

Example

```
traffic-management TM-1 all-policies 0 10000
traffic-management TM-2 per-policy 500 10000
traffic-management TM-3 per-ip 0 1500 100
no traffic-management TM-1
```

user-group

Definition

Define a user group for Firebox authentication.

Syntax

user-group (*name*) [**description** *desc*] [**membership** *user* ...]

name is the name of the user group.

desc is a short description of the purpose of the group.

user is a user name already configured on the device.

You can add more than one user.

Example

```
user-group accounting description Finance_and_Accounting_Dept membership
jackn gloriap cindyk karentc
```

users

Definition

Define a user for Firebox authentication.

Syntax

users (*name*) (*passphrase*) (*session-timeout*) (*idle-timeout*) [**group** *groupname*] [**description** *desc*]

name is a string that uniquely identifies the user.

passphrase is the unencrypted client password.

session-timeout is the duration in hours before a session times out. It must be an integer. The default value is 8.

idle-timeout is the duration in minutes before an idle session times out. It must be an integer. The default value is 30.

groupname is a Firebox authentication user group.

desc is a brief description of the user.

Example

```
users jackp somethingeasy 24 60 group executives description Jack_Parase_CEO
```