

# WatchGuard<sup>®</sup> Command Line Interface Reference

---

Fireware XTM v11.0



---

## Notice to Users

---

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 revision: 08/10/2009

## Copyright, Trademark, and Patent Information

---

Copyright © 1998 - 2009 WatchGuard Technologies, Inc. All rights reserved. All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Complete copyright, trademark, patent, and licensing information can be found in the Copyright and Licensing Guide, available online:

<http://www.watchguard.com/help/documentation/>

---

### ADDRESS:

505 Fifth Avenue South  
Suite 500  
Seattle, WA 98104

### SUPPORT:

[www.watchguard.com/support](http://www.watchguard.com/support)  
U.S. and Canada +877.232.3531  
All Other Countries +1.206.613.0456

### SALES:

U.S. and Canada +1.800.734.9905  
All Other Countries +1.206.613.0895

### ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. All products are backed by LiveSecurity® Service, a ground-breaking support and maintenance program. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please call 206.613.6600 or visit [www.watchguard.com](http://www.watchguard.com).

# Contents

---

- Introduction to the CLI ..... 1**
  - About the CLI Reference Guide ..... 1
    - Command reference format ..... 1
    - Command reference notation ..... 1
    - Sample command references ..... 2
  - Start the Command Line Interface ..... 2
    - Connect with serial cable ..... 3
    - Connect with TCP/IP ..... 3
  - Enter Commands in the CLI ..... 4
    - Terminal commands ..... 4
  - Get Help ..... 5
    - help ..... 5
    - Syntax used for help command ..... 5
    - "?" command ..... 7
  - Error Handling in the CLI ..... 8
  - Import and Export Files ..... 8
  
- Command Modes Overview ..... 11**
  - Introduction to the CLI Command Modes ..... 11
    - Main command mode ..... 12
    - Configuration command mode ..... 12
    - Interface command mode ..... 12
    - Policy command mode ..... 12
    - Common commands ..... 13
  - Command Line Interface Prompt ..... 13
  
- Common Commands ..... 15**
  - List of Common Commands ..... 15

---

Common Command Reference .....	16
exit .....	16
help .....	16
history .....	17
show .....	17
show cluster .....	18
show ip .....	18
show log-setting .....	18
show proposal .....	18
show objects .....	19
show certificate .....	19
show ddns .....	19
show interface .....	20
show log-cache .....	20
show update-history .....	20
<b>Main Command Mode .....</b>	<b>21</b>
Access the Main Command Mode .....	22
List of Main Mode Commands .....	22
Main Command Mode Reference .....	23
arp flush .....	23
backup image .....	23
cert-request .....	23
checksum .....	24
clock .....	24
configure .....	24
debug-cli .....	24
diagnose .....	24
dnslookup .....	25
export .....	25
import .....	26
password .....	26
ping .....	26
reboot .....	27
restore .....	27
shutdown .....	27
sync .....	27
sysinfo .....	28
tcpdump .....	28
traceroute .....	28
upgrade .....	28
vpn-tunnel .....	28
who .....	29
<b>Configuration Command Mode .....</b>	<b>31</b>
Access the Configuration Command Mode .....	32

List of Configuration Mode Commands .....	32
Configuration Command Mode Reference .....	32
auth-setting .....	32
bridge .....	33
cluster .....	34
ddns .....	35
default-packet-handling .....	36
global-setting .....	37
interface .....	37
ip .....	38
log-setting .....	40
managed-client .....	40
modem .....	41
multi-wan .....	43
network-mode .....	44
ntp .....	45
policy .....	45
signature update .....	46
snmp .....	46
static-arp .....	47
system .....	47
vlan .....	47
vpn-setting .....	48
wireless .....	48
.....	50
<b>Interface Command Mode .....</b>	<b>51</b>
Access the Interface Command Mode .....	52
List of Interface Mode Commands .....	52
Interface Command Mode Reference .....	52
dhcp .....	52
dos-prevention .....	53
enable .....	53
ip .....	54
link-speed .....	54
mac-ip-binding .....	54
mtu .....	55
name .....	55
pppoe .....	55
qos .....	56
secondary .....	56
type .....	57
vpn-pmtu .....	57
<b>Policy Command Mode .....</b>	<b>59</b>
Access the Policy Command Mode .....	60

---

List of Policy Mode Commands .....	60
Policy Command Mode Reference .....	61
alias .....	61
apply .....	62
auth-server .....	63
auth-user-group .....	64
bovpn-gateway .....	64
bovpn-tunnel .....	66
dynamic-nat .....	69
mvpn-ipsec .....	69
mvpn-rule .....	72
one-to-one-nat .....	74
policy-type .....	74
pptp .....	75
proposal .....	75
rule .....	76
schedule .....	80
sslvpn .....	80
traffic-management .....	82
user-group .....	82
users .....	82
<b>Index .....</b>	<b>83</b>

# 1 Introduction to the CLI

---

WatchGuard® Firebox® e-Series and Firebox XTM 1050 devices with Firebox XTM v11.0 operating system include a Command Line Interface (CLI) installed on the hardware. You can connect to the device 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.

## About the CLI Reference Guide

---

This section provides guidance for how to use the command reference in this document.

### Command reference format

The syntax section for each command uses a table format:

This line shows a single syntax for a command using the notation described in the following section.
This line contains the guidance and comments for the command. 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 line contains the text "No options available."

### Command reference notation

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

Notation	Required	Optional	Meaning	Example
<b>text</b>	✓		Must be typed exactly as shown.	<b>show</b>
<b>text</b>	✓		The requested information is required. Examples include an account name, password, or IP address.	<b>accountname</b>
<i>string</i>	✓		When information must be selected from a series of options, these appear in the command guidance.	<i>blocked-site</i> or <i>allowed-site</i>
<u>text</u>		✓	An additional parameter that, when used, alters the behavior of the command.	<u>log</u>

Notation	Required	Optional	Meaning	Example
<i>text</i>		✓	Additional information that, when provided alters the behavior of the command.	<i>text</i>
<b>text</b> <i>string</i>		✓	An extension or option to expand the functionality of the original command. Both <b>text</b> and <i>string</i> are required to complete the additional parameter. <b>text</b> must be entered as is, and <i>string</i> is required information.	<b>count in</b>

## Sample command references

A command reference provides:

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

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

### history

**Description:** Display the command history list with line numbers.

**Syntax:**

<b>history</b>
No options available.

### export

**Description:** Export information to an external platform or file.

**Syntax:**

<b>export type to location</b>
<p><b>type</b> must be one of the following:</p> <ul style="list-style-type: none"> <li>- <i>blocked-site</i> - blocked IP address</li> <li>- <i>allowed-site</i> - allowed IP address</li> <li>- <i>config</i> - device configuration</li> <li>- <i>muvpn</i> - Mobile VPN with IPSec client configuration file</li> <li>- <i>support</i> - support log message file</li> </ul> <p><b>location</b> must be either an ftp or tftp address.</p>

**Example:**

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

## Start the Command Line Interface

You connect to the WatchGuard® CLI using a terminal client located in the same secure environment as the Firebox®. The terminal client must use SSH2 to connect to the WatchGuard device by serial cable. You can also connect to the Console port or via TCP/IP to a Trusted or Optional interface. You can man-

age the WatchGuard device via the CLI while it is in operation, though some configuration changes require a restart.

## Connect with serial cable

To manage a WatchGuard device via serial cable, the personal computer must have an available serial port as well as an installed terminal client application.

- 1 Connect a serial cable from your computer or laptop to the Console port on the WatchGuard device.
- 2 Open your terminal application. Open a new connection window.
- 3 Verify that the terminal is set to VT100. Verify that your connection parameters are set to:

Setting	Value
Port	The serial port on your management station, usually COM1
Baud Rate	115200
Data Bits	8
Stop Bits	1
Parity	No
Flow Control	None



*If the terminal is not set to VT100, some command and control key functions do not work. For example, Ctrl-C will not break, some special characters will not type, and ESC will not work.*

- 4 Press <ENTER>.
 

*The connection window displays a welcome message and the Firebox login prompt.*
- 5 Enter the administrator user name. Press <ENTER>.
 

*There are two default administrator accounts: admin and status. Use admin for read-write privileges. Use status for read-only privileges.*
- 6 Enter the administrator read-write password. Press <ENTER>.
 

*The default password for the admin account is readwrite. The default password for the status account is readonly. The WatchGuard CLI opens in the Main command mode with the prompt WG#.*

## Connect with TCP/IP

The default WatchGuard policy allows you to connect to and administer a WatchGuard device from any computer on a trusted or optional network on port 4118. For more information on how to modify the default policy to either restrict access to the CLI or enable access from an external network, see the *WatchGuard System Manager User Guide*.

To do this procedure, you must have a terminal client which 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 terminal is set to VT100. Verify that your connection parameters are set to:

Setting	Value
Host	The IP address of the Firebox trusted or optional interface.
TCP Port	4118

Setting	Value
Service	SSH (version SSH2)
Protocol	IPv4



If the terminal is not set to VT100, some command and control key functions do not work. For example, Ctrl-C will not break, some special characters will not type, and ESC will not work.

- 3 Press <ENTER>.  
*The connection window displays a welcome message and the Firebox login prompt.*
- 4 Enter the administrator user name and password.  
*There are two default administrator accounts: admin and status. Use admin for read-write privileges. Use status for read-only privileges. The default password for the admin account is readwrite. The WatchGuard CLI opens in the Main command mode with the prompt WG#. The default password for the status account is readonly. The WatchGuard CLI opens in the Main command mode with the prompt WG>.*

## Enter Commands in the CLI

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

### Terminal commands

The following table gives a series of commands to move around and to operate the in CLI.



Your terminal client can use different commands or operating system rules to do the procedures that are given 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 ←	Move the cursor to the left one character.
Ctrl F or Ctrl →	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 ↑	Recall commands in the history buffer.
Ctrl N or Ctrl ↓	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 get access to the help system, type **help** or **?** at the command line and press Enter.

### help

**Description:** Display a numbered list of the available command formats for the specific command.

**Syntax:**

help <i>command</i>
If no <b>command</b> provided, describes general features of the help system.
If <b>command</b> provided, returns a list of all the possible syntaxes for the specified command.
If <b>?</b> provided for command, returns a list of all commands for which help is available in current command mode.
<b>command</b> 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> to (<ftp>|<tftp>|console)
  [4] export support to (<ftp>|<tftp>)

help ping
  [1] ping <mstring>

help tcpdump
  [1] tcpdump [<mstring>]*
```

### Syntax used for help command

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

Element	Example	Usage
	<ftp> <tftp>	Indicates that the command will allow 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.

Element	Example	Usage
<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 a FTP address in the required format will be accepted by the command. See "Import and Export Files" on page 8 for the required format.
<tftp>	[to (<ftp> <tftp>)]	Indicates that a TFTP address in the required format will be accepted by the command. See the following 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 of nnn.nnn.nnn.nnn where nnn is from 0 to 255 is required. Used in conjunction with <ipmask>.
<ipmask>	(<ipaddr> <ipmask> <net>)	Indicates an Netmask in the form of mmm.mmm.mmm.mmm where mmm is from 0 to 255 is required. Used in conjunction 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 from 0 to 255 and dd is from 0 to 32.
<macaddr>	<macaddr>	Indicates a physical address of a device is required. Format must be 01:23:45:67:89:ab.

Element	Example	Usage
<cr>	<cr>	Indicates that the command line is complete and can be executed upon hitting the "Enter" key.
<mstring>	<pre>ping &lt;mstring&gt;   where &lt;mstring&gt;:   [-LRUbdnqrVvA] [-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 &lt;mstring&gt;   where &lt;mstring&gt;:   [-adhrvAMOO] [-w wait] [-S start_ttl]   [-m max_ttl]   [-p port#] [-q nqueries] [-g gateway]   [-t tos]   [-s src_addr] [-g router] [-l proto] host [data   size]    tcpdump &lt;mstring&gt;   where &lt;mstring&gt;:   [-adeflnOPqStuvxX] [-c count]   [-i interface] [-s snaplen]   [-T type][expression][</pre>	Indicates multiple string of optional and required attributes as an argument of a command.

## “?” 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. 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:**

```
show s?
```

```

schedule          Schedule for use in the application of policies
signature-update  Signature update configuration
snmp              Simple Network Management Protocol
sslvpn           Secure Sockets Layer Virtual Private Network
static-arp       Static ARP entries
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 displays:

- 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 account user1000**. Because there is no user1000, the command is inaccurate, and the CLI returns the message `% Error: Account 'user1000' not found`. Note that the error message assists the user to identify 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.

For example, in the Main command mode the user enters the command **re**. Because there are three commands which begin with 're', the CLI returns the message `%Ambiguous command input detected at '^' marker` where the ^ marker denotes the start of the ambiguous input.

---

## Import and Export Files

The WatchGuard® CLI allows files to be exported and imported between a WatchGuard device and a remote server using either FTP or TFTP. The address must include a file name and the complete URL path where appropriate. The FTP address must use the following syntax to identify the user, server, and filename:

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

### **Example:**

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

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

```
tftp://host/url-path
```

**Example:**

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



# 2 Command Modes Overview

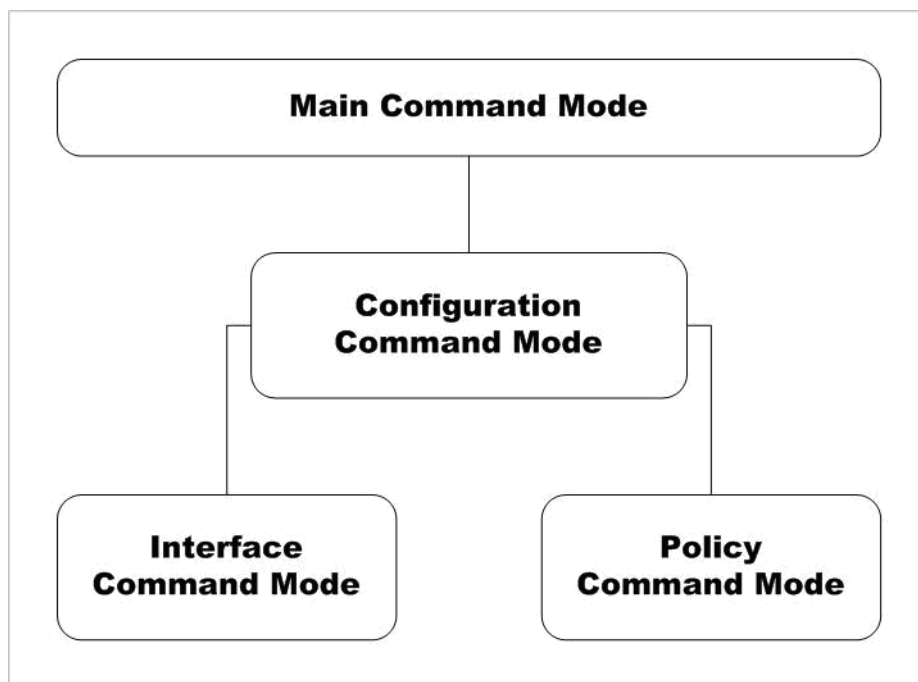
---

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

## Introduction to the CLI Command Modes

---

The command mode hierarchy shown below 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. Using the Main mode, a network administrator can perform these functions:

- Modify some higher level configuration settings
- See system logs
- Enter the Configuration command mode
- Restore or upgrade the software image
- Shutdown or reboot the WatchGuard device

## Configuration command mode

The Configuration command mode is used for system and network configuration of the WatchGuard device. To get access to the Configuration command mode, open the CLI in the Main command mode, then use the command **configure**. Using the Configuration mode, a network administrator can perform these functions:

- Manage the logging performed by the WatchGuard device
- Configure global network settings
- Enter the Policy and Interface command modes

## Interface command mode

The Interface command mode is used to configure the Ethernet interfaces of the WatchGuard device. To get access to the Interface command mode, open the CLI in the Configuration command mode, then use the command **interface**. Using the Interface command mode, a network administrator can 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

## Policy command mode

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

- Create and modify rules 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

## Common commands

Many commands are shared by all four command modes. These are known as “common commands.” In this reference guide, we break the common commands out into a separate chapter. You can use common commands in all four 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 reflect the working 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-eth0)#
Policy	Common and Policy commands	WG(config/policy)#



# 3 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

---

The following commands are available in all command modes:

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

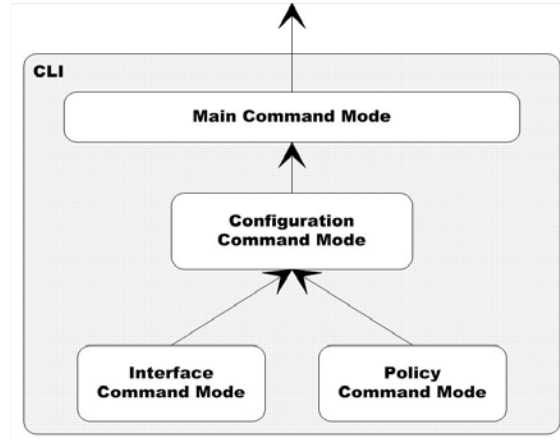
# Common Command Reference

## exit

**Description:** In the Main mode, exit the CLI. Otherwise, return to the previous mode.

**Syntax:**

<b>exit</b>
No options available.



## help

**Description:** See general information or possible syntax for specified command. For more information, see “Get Help” on page 5.

**Syntax:**

<b>help command</b>
If no <b>command</b> provided, describes general features of the help system. If <b>command</b> provided, returns a list of all the possible syntaxes for the specified command. If ? provided for command, returns a list of all commands for which help is available in current command mode. <b>command</b> 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<i dent>

help export
[1] export (blocked-site|allowed-site) to (<ftp>|<tftp>)
[2] export (config) to (<ftp>|<tftp>|console)
[3] export mvvpn <i dent> to (<ftp>|<tftp>|console)
[4] export support to (<ftp>|<tftp>)

help ping
[1] ping <mstring>

help tcpdump
[1] tcpdump [<mstring>]*
    
```

## history

**Description:** Display the command history list with line numbers.

**Syntax:**

<b>history</b>
Display commands entered into the CLI with line numbers.

**Example:**

```
history
```

## 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:**

<b>show <i>component</i></b>
<b><i>component</i></b> must be a valid command. If ? used for component, returns a list of all valid strings for <b><i>component</i></b> .

The following table is a list of ***component*** values for which no options are available.

<b>Component</b>	<b>Display</b>
<i>arp</i>	ARP table
<i>clock</i>	Manage the system clock
<i>default-packet-handling</i>	Default packet handling
<i>dynamic-nat</i>	Dynamic NAT
<i>factory-default</i>	Factory default configuration
<i>features</i>	Active licensed software features
<i>login-user</i>	List of management users logged on to the device
<i>managed-client</i>	Configuration this firebox as a managed client
<i>network-mode</i>	WatchGuard security appliance system mode
<i>multi-wan</i>	Multiple wide area network settings
<i>ntp</i>	Network Time Protocol
<i>one-to-one-nat</i>	1-to-1 NAT settings for the device
<i>pptp</i>	Point to Point Tunneling Protocol
<i>proxy-action</i>	Default proxy actions
<i>route</i>	Established static routes
<i>signature-update</i>	Signature update configuration settings
<i>snmp</i>	Simple Network Management Protocol (SNMP) settings
<i>sslvpn</i>	Secure Sockets Layer Virtual Private Network
<i>static-arp</i>	Static ARP entries added to the static ARP table
<i>status-report</i>	Display system status
<i>sysinfo</i>	Display system information
<i>upgrade</i>	The audit trail of software upgrade(s)

Component	Display
<i>vpn-setting</i>	Global settings for virtual private networking
<i>vpn-status bovpn</i>	Active branch office VPN tunnels
<i>vpn-status pptp</i>	Active Mobile VPN with PPTP users

## show cluster

**Description:** Display the names of FireCluster members or the status of the cluster.

**Syntax:**

<b>show cluster <i>component</i></b>	
<b><i>component</i></b> is one of the following:	
<i>member</i>	Shows the list of FireCluster members
<i>status</i>	Shows the current status of the FireCluster

## show ip

**Description:** Display the Internet Protocol settings for selected component.

**Syntax:**

<b>show ip <i>component</i></b>
<b><i>component</i></b> must be one of the following: <i>allowed-site, blocked-port, blocked-site, dns, dynamic-routing, route, or wins.</i>

## show log-setting

**Description:** Display the log settings for a specified component.

**Syntax:**

<b>show log-setting <i>component</i></b>	
<b><i>component</i></b> is one of the following:	
Component	Description
<i>log-level</i>	Diagnostic log level
<i>ike-packet-trace</i>	IKE packet trace
<i>linternal-storage</i>	Internal storage
<i>performance-statistics</i>	Performance statistics
<i>syslog-server</i>	Syslog server
<i>watchguard-log-server</i>	WatchGuard® Log Server

## show proposal

**Description:** Display the settings for the specified branch office VPN IPSec proposal.

**Syntax:**

<b>show proposal <i>proposal number</i></b>
<i>p1</i> - Phase 1 proposal
<i>p2</i> - Phase 2 proposal

## show objects

**Description:** Use to display all the settings associated with a named object.

**Syntax:**

<b>show object name</b>	
<i>name</i> is the name of the object If <i>name</i> is not specified, displays a list of all configured objects of the type <i>object</i> <i>object</i> is one of the following:	
<b>Object</b>	<b>Description</b>
<i>alias</i>	Alias
<i>auth-server</i>	Authentication server
<i>auth-setting</i>	Authentication settings
<i>auth-user-group</i>	Authorized user and group
<i>bovpn-gateway</i>	Branch office virtual private network gateways
<i>bovpn-tunnel</i>	Branch office virtual private network tunnels
<i>bridge</i>	Bridged interface on the WatchGuard device
<i>feature-key</i>	WatchGuard® feature key
<i>global-setting</i>	Global settings for the device
<i>mvpn-ipsec</i>	Mobile VPN with IPsec group configuration
<i>mvpn-rule</i>	Mobile VPN with IPsec policies
<i>policy-type</i>	Policy template
<i>rule</i>	Policy rule specification
<i>schedule</i>	Schedule to control traffic by time and day of week
<i>traffic-management</i>	Traffic management action
<i>user-group</i>	Firebox authentication user group
<i>users</i>	Firebox authentication user
<i>vlan</i>	Virtual local area network

## show certificate

**Description:** Display the certificates available in the WatchGuard device.

**Syntax:**

<b>show certificate component</b>	
<i>component</i> is one of the following:	
<b>Component</b>	<b>Description</b>
<cr>	Carriage return
<int>	Certificate ID <10000-99999>
<i>fingerprint</i>	Certificate fingerprint of a certificate on the device
<i>name</i>	Name of the entity
<i>type</i>	Show the certificates by type

## show ddns

**Description:** Display the dynamic DNS service configuration information.

**Syntax:**

<b>show ddns <i>type</i></b>
<i>type</i> is the dynamic DNS service type. The only valid string is <i>DynDNS</i> .

## show interface

**Description:** Display the physical interface configuration and status.

**Syntax:**

<b>show interface <i>number</i></b>
<i>number</i> is the network interface number. <i>number</i> must represent a valid number for the device. If <i>number</i> is provided, the device displays information for only the specified interface. Otherwise, it displays information for all interfaces.

## show log-cache

**Description:** Display the internal temporary log repository for traffic monitor.

**Syntax:**

<b>show log-cache <i>sequence startpoint count number</i></b>
Display log entries from a specified start point of the log repository. <i>startpoint</i> is the starting sequence number of the log entries to display. <i>number</i> is the maximum number of log entries to display. It must be an integer from 1 to 10000.
<b>show log-cache tail <i>count number</i></b>
Display log entries backward from the end of the internal log repository. <i>number</i> is the maximum number of log entries to display. It must be an integer from 1 to 10000.
<b>show log-cache <i>key</i></b>
Displays entries that contain the key value

## show update-history

**Description:** Display the historical update record.

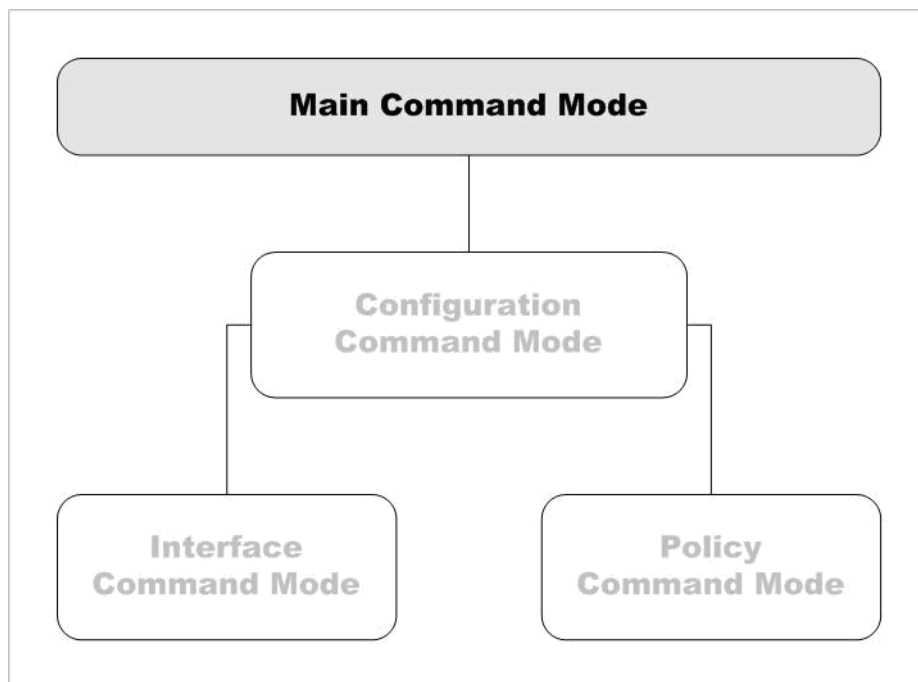
**Syntax:**

<b>show update-history <i>type</i></b>
<i>type</i> must be one of the following: <i>ips</i> , or <i>av-sig</i> .

# 4 Main Command Mode

---

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



Within the Main mode, the administrator can do these functions:

- Modify some higher level configuration settings
- Enter the Configuration command mode
- Restore or upgrade the software image
- Shutdown or reboot the WatchGuard device

---

## Access 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 whether you connected to the device using the read-write admin account (WG#) or the read-only status account (WG>).

---

## List of Main Mode Commands

---

You can use all common commands in the Main command mode. For more information, see “List of Common Commands” on page 15. In addition, the following commands are available only in the Main mode:

Command	Usage
<b>arp flush</b>	Clear the ARP cache of all entries.
<b>backup image</b>	Store a backup copy of the flask disk image.
<b>cert-request</b>	Use the WatchGuard device to create a security certificate.
<b>checksum</b>	Generate and display the MD5 checksum of all the packages installed.
<b>clock</b>	Manage and change the system clock.
<b>configure</b>	Enter the Configuration command mode.
<b>debug-cli</b>	Configure debugging options.
<b>diagnose</b>	Display internal diagnostic information.
<b>dnslookup</b>	Domain name resolution
<b>export</b>	Export information to an external platform or file.
<b>import</b>	Import information from an external platform or file.
<b>password</b>	Change the administrator read-write or read-only password.
<b>ping</b>	Send a ping request to the specified IP address.
<b>reboot</b>	Halt all processing and do a cold restart of the device.
<b>restore</b>	Restore the device to a backup image or default configuration.
<b>shutdown</b>	Shut down the WatchGuard device.
<b>sync</b>	Synchronize the licenses and RSS feed between two WatchGuard devices.
<b>sysinfo</b>	Display the WatchGuard device system information.
<b>tcpdump</b>	Dump traffic on the network.
<b>traceroute</b>	Examine and display the route to a specified destination.
<b>upgrade</b>	Upgrade the operating system.
<b>vpn-tunnel</b>	Force the rekey of a BOVPN gateway.
<b>who</b>	Display a list of administrator users logged in to the WatchGuard device.

## Main Command Mode Reference

### arp flush

**Description:** Clear the ARP cache of all entries.

**Syntax:**

<b>arp flush</b>
No options available.

### backup image

**Description:** Store a backup copy of the flask disk image.

**Syntax:**

<b>backup image <i>password to location</i></b>
<i>password</i> is the backup password for the device. <i>location</i> must be a valid FTP or TFTP address.

**Example:**

```
backup image readwritefoo to ftp://joez:passwd1@100.100.100.3/myback.sysa-dl
```

### cert-request

**Description:** Use the WatchGuard device to create a security certificate.

**Syntax:**

<p><b>cert-request <i>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</i></b></p> <p><i>purpose</i> must be one of the following: https-proxy-authority, https-proxy-server, ipsec-web-server-other.  <i>commonname</i> is the certificate common name.  <i>companyname</i> is a string that identifies the issuer of the certificate. This should be your company name.  <i>dnsname</i> is the fully qualified domain name.  <i>countryname</i> is a string that identifies the originating country, C. The default is US.  <i>statename</i> is a string that identifies the originating state or province, ST.  <i>cityname</i> is a string that identifies the originating city or location, L.  <i>deptname</i> is a string that identifies the originating department within a larger organization, OU.  <i>deviceaddress</i> is an IP address identifying the originating device.  <i>domain</i> is the domain name of the originating company.  <i>key-type</i> must be one of the following: <i>dsa</i> or <i>rsa</i>. The default is RSA.  <i>key-length</i> must be one of the following: <i>length-1024</i> or <i>length-2048</i>  <i>key-usage</i> is optional for ipsec-web-server-other only. If using DSA encryption, the value must be <i>signature</i>. If RSA encryption, the value must be one of the following: <i>encryption</i>, <i>signature</i>, or <i>both</i>.</p>
--

**Example:**

```
cert-request https-proxy-authority BigCompanyAcct BigCompany www.bigcompany.com country US
cert-request https-proxy-server BigCompanyAcct BigCompany www.bigcompany.com
country US state Maine department Accounting address 200.202.12.3 domain
www.bigcompany.com algorithm dsa length 1024
```

## checksum

**Description:** Generate and display the checksum of all the packages installed on the device.

**Syntax:**

<b>checksum</b>
No options available.

**Example:**

```
checksum
```

## clock

**Description:** Manage and change the system clock.

**Syntax:**

<b>clock time HH:MM:SS <u>date</u> MM/DD/YYYY</b>
<i>time</i> is in the format: HH:MM:SS. The selection of AM or PM is not supported, thus the hours must be entered in the range 0 to 23.
<i>date</i> is in the format MM/DD/YYYY. Leading zeroes are not required in the month and day fields.

**Example:**

```
clock time 11:30:56 date 12/1/2004
```

## configure

**Description:** Enter the Configuration command mode.

**Syntax:**

<b>configure</b>
No options available.

## debug-cli

**Description:** Configure debugging options.

**Syntax:**

<b>debug-cli <i>level</i></b>
<i>level</i> must be one of the following: <i>critical</i> , <i>error</i> , <i>warning</i> , <i>info</i> , <i>debug</i> , or <i>dump</i>

**Example:**

```
debug-cli critical
```

## diagnose

**Description:** Display internal diagnostic information.

**Syntax:**

<b>diagnose <u>to</u> <i>location</i></b>
View diagnostic information for a single device. <i>location</i> must be either an FTP or TFTP address.
<b>diagnose cluster <u>to</u> <i>location</i></b>

See diagnostic information for a cluster of WatchGuard devices.

*location* must be either an FTP or TFTP address.

#### diagnose vpn "*ident*"

See diagnostic information for VPN Debug.

*ident* must be one of the following:

- /ike/tracelevel/set *n1*
- /ike/pkttrace/set *n2*
- /ike/counters
- /ike/restart
- /ike/gateway/list
- /ike/gateway/info
- /ike/policy/list
- /ike/policy/info
- /ike/policy/conn
- /ike/policy/counters
- /ike/sa/list
- /ike/sa/list/policy
- /ike/sa/counters
- /ipsec/policy/list
- /ipsec/policy/info
- /ipsec/policy/rinfo
- /ipsec/sa/list
- /ipsec/sa/ikepcy/list
- /ipsec/sa/ipsecpcy/list
- /ipsec/sp/list
- /ipsec/sp/info
- /ipsec/counters
- /ipsec/spi/hashtable
- /ipsec/cluster/topology
- /ipsec/bovpn/rekey

***n1*** must be one of the following, 0:restore, 1:err, 2:warn, 3:info, 4:debug

***n2*** must be one of the following, 0:off, 1:start and overwrite, 2:rotate, 3:append, 4:reset

#### Example:

```
diagnose cluster
diagnose to tftp://bigcoftp/files/upload/memory.dot
diagnose vpn "/ike/sa/list"
diagnose vpn "/ike/tracelevel/set 2"
```

## dnslookup

**Description:** Look up domain name.

**Syntax:**

**dnslookup *domainname***

Resolve a domain name.

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

#### Example:

```
dnslookup www.companyname.com
```

## export

**Description:** Export information to an external platform or file.

**Syntax:**

<b>export type to location</b>
<i>type</i> must be one of the following: <i>blocked site</i> or <i>allowed-site</i> <i>location</i> must be either an FTP or TFTP address.
<b>export config to location</b>
<i>location</i> must be either an FTP, TFTP address or console.
<b>export muvpn <i>muvpnid</i> to location</b>
<i>muvpnid</i> must be an existing Mobile VPN with IPsec ID. <i>location</i> must be either an FTP, TFTP address or console.
<b>export support to location</b>
<i>location</i> must be either an FTP or TFTP address.

**Example:**

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

## import

**Description:** Import information from an external platform or file.

**Syntax:**

<b>import type action option from location</b>
<i>type</i> must be one of the following: <i>blocked-site</i> or <i>allowed-site</i> . <i>option</i> must be one of the following: <i>override</i> or <i>merge</i> . <i>location</i> must be either an FTP or TFTP address.
<b>import type from location</b>
<i>type</i> must be one of the following: <i>bulk-license</i> , <i>certificate</i> , <i>crl</i> , <i>config</i> or <i>feature-key</i> . <i>location</i> must be either an FTP or TFTP address.
<b>import route-config type from location</b>
<i>type</i> must be one of the following: <i>bgp</i> , <i>rip</i> , or <i>ospf</i> . <i>location</i> must be either an FTP or TFTP address or <i>console</i> .

**Example:**

```
import blocked-site action merge from tftp://myftpsite/files/upload/site.dot
import certificate from tftp://myftpsite/files/upload/cert.dot
import bulk-license from tftp://myftpsite/files/upload/keys.dot
import route-config ospf from console
```

## password

**Description:** Change the administrator read-write or read-only password.

**Syntax:**

<b>password</b>
No options available.

## ping

**Description:** Send a ping request to the specified IP address.

**Syntax:**

<b>ping</b> <i>&lt;mstring&gt;</i> <i>host</i>
--

<i>host</i> is the host name or IP address in the format of A.B.C.D.
--

**Example:**

```
ping 74.125.19.147
ping -c 5 74.125.19.147
```

**reboot****Description:** Halt all processing and do a cold restart of the device.**Syntax:**

<b>reboot</b>
---------------

No options available.
-----------------------

**restore****Description:** Restore the device to a backup image or default configuration.**Syntax:**

<b>restore factory-default</b>
--------------------------------

Restores the device to its factory default configuration. No options available.
---

<b>restore image <i>password</i> from <i>location</i></b>
---

<i>password</i> is the restore password of the device. <i>location</i> is a valid FTP or TFTP address.
---

**Example:**

```
restore image configpasswordfoo from tftp://myftpsite/files/upload/april.fxi
```

**shutdown****Description:** Shut down the WatchGuard device.**Syntax:**

<b>shutdown</b>
-----------------

No options available.
-----------------------

**sync****Description:** Synchronize the licenses and RSS feed between two WatchGuard devices. The RSS feed is available from the LiveSecurity® Service.**Syntax:**

<b>sync feature -key <i>apply</i></b>
---------------------------------------

<i>apply</i> is a string that identifies the WatchGuard device to which the licenses should be applied.
---

<b>sync rss-feed</b>
----------------------

No options available.
-----------------------

**Example:**

```
sync feature-key
```

## sysinfo

**Description:** Displays the WatchGuard device system information.

**Syntax:**

<b>sysinfo</b>
No options available.

## tcpdump

**Description:** Dump traffic on the network.

**Syntax:**

<b>tcpdump</b> <u>&lt;mstring&gt;</u>
No options available.

**Example:**

```
tcpdump -d -q
```

## traceroute

**Description:** Examine and display the route to a specified destination.

**Syntax:**

<b>traceroute</b> <u>&lt;mstring&gt;</u> <i>host</i>
<i>host</i> is a valid IP address.

**Example:**

```
traceroute -d 74.125.19.147
```

## upgrade

**Description:** Upgrade the operating system.

**Syntax:**

<b>upgrade system from</b> <i>location</i> <u>force</u>
<i>location</i> must be either an FTP or TFTP address. <u>force</u> must be one of the following: <i>yes</i> or <i>no</i> . This forces the system upgrade.

**Example:**

```
upgrade system ftp://test:testing@1.2.3.4/upg.wgu yes
```

## vpn-tunnel

**Description:** Force the rekey of a BOVPN gateway.

**Syntax:**

<b>vpn-tunnel rekey</b> <i>gateway</i>
<i>gateway</i> identifies a BOVPN gateway.

**Example:**

```
vpn-tunnel rekey ChicagoSeattle
```

## who

**Description:** Display a list of administrator users logged in to the WatchGuard device.

**Syntax:**

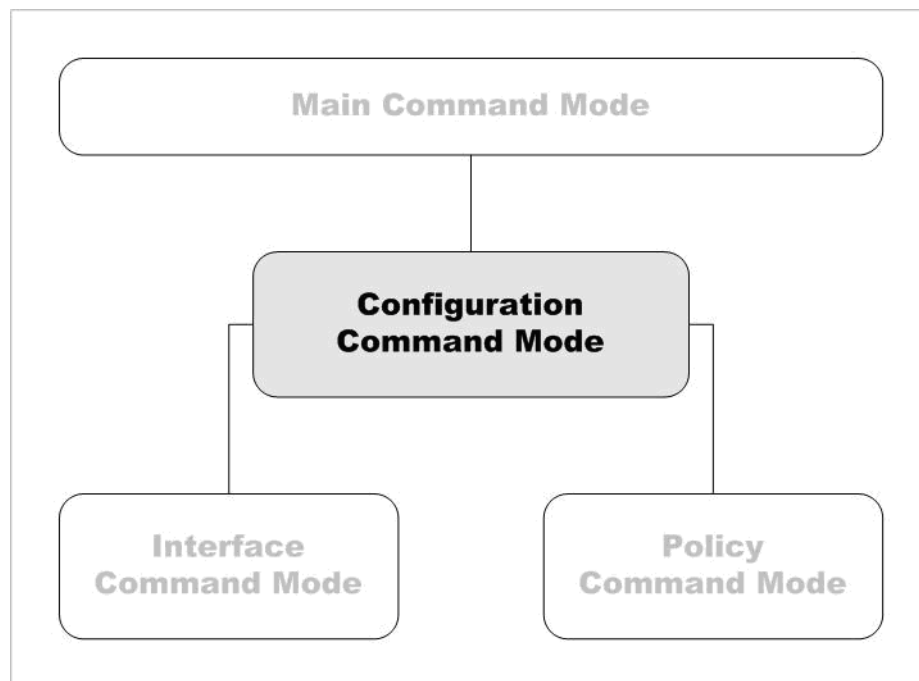
<b>who</b>
No options available.



# 5 Configuration Command Mode

---

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



In the Configuration mode, the administrator can do these functions:

- Manage user accounts
- Manage the logging performed by the WatchGuard device
- Configure global network settings
- Control branch office VPN gateways and tunnels
- Enter the Policy and Interface command modes

---

## Access 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 or Interface 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. For more information, see “List of Common Commands” on page 15. In addition, the following commands are available only in the Configuration mode:

Command	Usage
<b>auth-setting</b>	Configure settings for authentication.
<b>bridge</b>	Assign a name to a VLAN bridge.
<b>cluster</b>	Configure settings for FireCluster.
<b>ddns</b>	Configure settings for dynamic DNS.
<b>default-packet-handling</b>	Configure the default packet handling settings.
<b>global-setting</b>	Configure the global settings of a device.
<b>interface</b>	Enter the Interface command mode for the specified interface.
<b>ip</b>	Configure IP settings for firewall features such as block sites and ports.
<b>ldap</b>	Configure the device to use an LDAP authentication server.
<b>log-setting</b>	Define how and where the device sends log messages.
<b>managed-client</b>	Configure the device to be a managed client of another device.
<b>multi-wan</b>	Configure the device with multiple external interfaces.
<b>network-mode</b>	Change the system configuration mode to either Mixed Routed, Drop-in, or Bridge.
<b>ntp</b>	Configure the device to use an NTP server.
<b>policy</b>	Enter the Policy command mode.
<b>signature update</b>	Configure updates to IPS and GAV signatures files and engine.
<b>snmp</b>	Configure the device to interoperate with SNMP tools.
<b>static-arp</b>	Hard code a static-arp binding.
<b>system</b>	Set the system properties.
<b>vlan</b>	Create VLAN interface on the device.
<b>vpn-setting</b>	Configure global VPN settings

---

## Configuration Command Mode Reference

---

### auth-setting

**Description:** Configure the authentication service of the device.

**Syntax:**

<b>auth-setting timeout-type day <i>days</i> hour <i>hours</i> minute <i>minutes</i> second <i>seconds</i></b>
Configure the timeout setting options of authentication. <b>timeout-type</b> is the authentication option that must be set for timeout. It must be one of the following: <i>auth-user-idle-timeout</i> , <i>auth-user-session-timeout</i> , <i>mgmt-user-idle-timeout</i> , or <i>mgmt-user-session-timeout</i> . <i>days</i> is the duration in days. It must be an integer from 0 to 365. <i>hours</i> is the duration in hours. It must be an integer from 0 to 23. <i>minutes</i> is the duration in minutes. It must be an integer from 0 to 59. <i>seconds</i> is the duration in seconds. It must be an integer from 0 to 59.
<b>auth-setting auto-redirect enable</b>
Automatically redirect user to authentication page for authentication.
<b>auth-setting auto-redirect url <i>url-path</i></b>
Send a redirect to a particular web site to the browser after successful authentication. <b>url-path</b> is the web site to redirect after authentication.
<b>auth-setting same-user-multi-login <i>setting</i></b>
Set authentication to allow or disallow multiple logins from a user at the same time. <b>setting</b> must be one of the following: <i>enable</i> or <i>disable</i> . Enabled by default.
<b>auth-setting single-sign-on enable</b>
Enable Single Sign-On (SSO) on the device. Use <b>no ip auth-setting single-sign-on enable</b> to disable SSO.
<b>auth-setting single-sign-on agent address cache -timeout</b>
Specify Single Sign-On (SSO) Agent on the network. <b>address</b> is the IP address of SSO Agent. <b>cache-timeout</b> is the amount of time in seconds the SSO information is stored.
<b>auth-setting single-sign-on except-ip <i>ip-address ip-address</i></b>
Add SSO exception list. <b>ip-address</b> is the IP address of the computer to exempt from SSO. You can specify multiple IP addresses in the command.

**Example:**

```

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 disable
auth-setting single-sign-on enable
auth-setting single-sign-on agent 10.0.1.253
auth-setting single-sign-on except-ip 10.0.1.33 10.0.1.55

```

**bridge**

**Description:** Create or edit a Bridge virtual interface on the device.

**Syntax:**

<b>bridge <i>bridgename</i></b>
<b>bridgename</b> is a string that uniquely identifies the bridge. Use <b>no bridge <i>bridgename</i></b> to delete the bridge virtual interface.

After you enter the command **bridge *bridgename*** the configuration continues to the Bridge details command. The prompt changes to "WG(config/bridge-*bridgename*)#".

<b>security-zone <i>zone ip-address member if-number if-number if-number</i></b>
<b><i>zone</i></b> is the security zone. It must be either of the following: trusted, or optional. <b><i>ip-address</i></b> is the IP Address assigned to the virtual 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. <b><i>if-number</i></b> is the interface index that is assigned as a member of the Bridge. You can specify more than two member interfaces of the Bridge.

**Example:**

```
bridge Bridgel0
security-zone trusted 10.10.1.1/24 member 3 4 5
```

## cluster

**Description:** Configure the FireCluster settings. This command does not apply to Firebox X Edge devices.

**Syntax:**

<b>cluster enable</b>
Enable FireCluster feature of a device.
<b>cluster id <i>c-id</i></b>
Set the Identification number of a FireCluster. <i>c-id</i> is an Identification number between 1 to 255.
<b>cluster interface <i>if-type if-number</i></b>
Identifies the type and its corresponding interface of a FireCluster. <i>if-type</i> must be one of the following: <i>management, primary, secondary</i> . <i>if-number</i> is the interface number assigned to the specified type.
<b>cluster mode <i>c-mode</i></b>
Selects the FireCluster mode. <i>c-mode</i> must be one of the following: <i>active-active</i> or <i>active-passive</i> .
<b>cluster load-balance <i>type</i></b>
Specify the load balancing algorithm of an Active/Active FireCluster. <i>type</i> must be one of the following: <i>Least-Connections, Round-Robin</i> .
<b>cluster member <i>option member-name serial-no primary-ip mgt-ip secondary-ip from source</i></b>
Add a new FireCluster member or edit an existing FireCluster member. <i>option</i> must be one of the following: <i>add</i> or <i>edit</i> . <i>member-name</i> is a string that is the name of the FireCluster member device. <i>serial-no</i> is the serial number of the device. <i>primary-ip</i> is the IP address of the primary FireCluster interface. <i>mgt-ip</i> is the management IP address of the FireCluster. <i>secondary-ip</i> is the IP address of the optional secondary FireCluster interface. <i>source</i> FireCluster member license file take from one of the following: <i>FTP, TFTP</i> or <i>console</i> .
<b>cluster notification snmp-trap enable</b>
Activate and send SNMP traps for FireCluster.

<b>cluster notification notification enable action-type <i>a-type</i> launch-interval <i>int</i> repeat-count <i>count</i></b>
--

Activate email or pop-up window notifications for FireCluster.

**a-type** must be one of the following: *email* or *pop-window*. The default is email.

*int* is the launch interval between 1 to 65535. The default is 15.

*count* is the launch interval between 1 to 256. The default is 10.

### 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 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
```

## ddns

**Description:** Configure the device to use a dynamic domain name service provider.

### Syntax:

<b>ddns DynDNS interface username password domainname type options interval</b>
---

**interface** is the name of the interface configured to use DynDNS.

**username** is a string that represents the DynDNS user name.

**password** is the DynDNS password.

**domainname** is a string that is the domain name used for your DynDNS account.

**type** is the DynDNS service type. It must be one of the following: *dyndns*, *statdns*, or *custom*.

**options** is a string composed of one or more DynDNS options:

- You must type an "&" 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

*interval* is the frequency in days that the device forces an update. This must be an integer.

### Example:

```
ddns DynDNS interface 0 watchguard strongpass2 watchguard.com statdns
&backmx=NO&wildcard=ON& 28
```

## default-packet-handling

**Description:** Configure default packet handling settings.

**Syntax:**

<p><b>default-packet-handling logging type</b> <i>action logging-action</i> <i>launch-interval int</i> <i>repeat-count count</i></p>
<p>Configure log settings for default packet handling options.</p> <p><b>type</b> is the type of log message to enable. It must be one of the following: <i>ip-spoofing, arp, port, address, ip-src, ping, ipsec, ike, syn, icmp, udp, ddos-des, ddos-src, incoming, outgoing, internal, or external</i>.</p> <p>Use <b>no default-packet-handling logging category type</b> to disable the logging of packets of the specified category.</p> <p><b>type</b> is the form of notification. It must be one of the following:</p> <ul style="list-style-type: none"> <li>- 1 is Send Log Message.</li> <li>- 2 is Send SNMP trap</li> <li>- 3 is Send Notification.</li> </ul> <p>If the <b>type</b> selected is 3, then you also have the following options:</p> <ul style="list-style-type: none"> <li>- <i>int</i> is the minimum time in minutes between notifications. It must be an integer from 1 to 65525.</li> <li>- <i>count</i> is the number of times an event must occur before a repeat notification is sent. It must be an integer from 1 to 256.</li> </ul>
<p><b>default-packet-handling unhandled option enable</b></p>
<p>Set action taken for packets that do not match any default packet handling rule.</p> <p><b>option</b> is the action taken when the device receives a packet that does not match any rule. It must be one of the following: <i>auto-block</i> or <i>send-message</i>.</p> <p>Use <b>no default-packet-handling unhandled</b> to disable all actions for unhandled packets.</p>
<p><b>default-packet-handling dangerous-active activity enable threshold</b></p>
<p>Enable default packet handling rules for certain types of dangerous activity.</p> <p><b>activity</b> is the form of dangerous activity. It must be one of the following: <i>icmp-flood enable, syn-flood enable, udp-flood enable, ipsec-flood enable, ike-flood enable, ip-scan enable, port-scan enable, spoofing-attack enable, or source-route enable</i>.</p> <p><b>threshold</b> is the threshold value. It is an integer as follows:</p> <ul style="list-style-type: none"> <li>- Ports 10 to 65535 for <i>icmp-flood</i> or <i>syn-flood</i>.</li> <li>- Packets per second 1 to 65535 for <i>udp-flood, ipsec-flood, ike-flood, ip-scan, or port-scan</i>.</li> <li>- Leave blank for <i>spoofing-attack</i> or <i>source-route enable</i>.</li> </ul>
<p><b>default-packet-handling ddos side enable quota</b></p>
<p>Configure evaluation of traffic for DDoS.</p> <p><b>side</b> is whether to monitor based on the source or destination. It must be one of the following: <i>server-ddos</i> or <i>client-ddos</i>.</p> <p><b>quota</b> is the number of connections per second. It must be an integer from 10 to 65535.</p>

**Example:**

```
default-packet-handling logging ike 3 action 3 launch-interval 50 repeat-
count 10
default-packet-handling unhandled auto-block enable
default-packet-handling dangerous-activity ike-flood enable 1000
default-packet-handling ddos server-ddos enable 1500
```

## global-setting

**Description:** Define the global settings of the device.

**Syntax:**

<b>global-setting auto-reboot enable</b>
Enable the auto-reboot feature of the device. Use <b>no global-setting auto-reboot enable</b> to disable auto-reboot function.
<b>global-setting auto-reboot hour <i>hr</i> minute <i>min</i></b>
Defines the auto-reboot timer of the device. <b><i>hr</i></b> is the number of hours from 0 to 23. <b><i>min</i></b> is the optional number of minutes from 0 to 59.
<b>global-setting icmp-message <i>message</i></b>
Define the ICMP error message of the device. Use <b>no global-setting icmp-message <i>message</i></b> to disable icmp-message function. <b><i>message</i></b> is the ICMP message returned to the source. It must be one of the following: <i>allow-all</i> , <i>deny-all</i> , <i>fragmentation-required</i> , <i>host-unreachable</i> , <i>network-unreachable</i> , <i>port-unreachable</i> , <i>protocol-unreachable</i> , <i>time-exceeded</i> . If the <b><i>message</i></b> selected is <i>fragmentation-required</i> , then DF bit is set to 1.
<b>global-setting tcp-mss-adjustment <i>option</i></b>
Set the maximum segment size adjustment. <b><i>option</i></b> must be one of the following: <i>automatic</i> or <b>limit-to <i>size</i></b> - <b><i>size</i></b> is the specified size in bits. It must be an integer from 40 to 1460.
<b>global-setting tcp-syn-checking enable</b>
Enable the TCP/syn of the device. Use <b>no global-setting tcp-syn-checking enable</b> to disable TCP/syn checking function.
<b>global-setting traffic-management enable</b>
Enable the traffic management feature of the device. Use <b>no global-setting traffic-management enable</b> to disable traffic management feature of the device.
<b>global-setting webui-port <i>port</i></b>
Set the Web User Interface port of the device. <b><i>port</i></b> is the port number from 1 to 65535.

**Example:**

```
global-setting auto-reboot enable
global-setting auto-reboot hour 2 30
global-setting icmp-message deny-all
global-setting tcp-syn-checking enable
global-setting tcp-mss-adjustment automatic
global-setting tcp-mss-adjustment limit-to 100
global-setting traffic-management enable
global-setting webui-port 3128
```

## interface

**Description:** Enter the Interface command mode for the specified interface.

**Syntax:**

<b>interface FastEthernet <i>number</i></b>
<i>number</i> must be an integer from 0 to max number of port minus one depending on the platform and model.

**Example:**

```
interface FastEthernet 0
WG(config/i fe-eth0)#
```

**ip**

**Description:** Configure Internet Protocol settings for firewall features such as block sites and ports.

**Syntax:**

<b>ip allowed-site <i>address</i></b>
Adds or removes an address from the allowed IP address list. <i>address</i> must be one of the following: <i>host ip</i> , <i>subnet net</i> , or <i>range startip endip</i> . - <i>ip</i> , <i>startip</i> , and <i>endip</i> must be an IP address in the format of A.B.C.D. - <i>net</i> must be an IP subnet in the format of A.B.C.D/# where # must be in the range of 0 to 32. Use <b>no ip allowed-site</b> to clear all entries on the allowed IP address list.
<b>ip blocked portblocked-port <i>port</i> log <i>logstate</i> auto-blocked <i>autostate</i> alarm <i>alarmsetting</i> <i>alarmoption</i></b>
Blocks all traffic to specified port or ports. <i>port</i> is an integer from 1 to 65535. You can configure more than one. <i>logstate</i> enables or disables log messages when packets are addressed to the specified port. The value must be: <i>enable</i> or <i>disable</i> . <i>autostate</i> 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: <i>enable</i> or <i>disable</i> . <i>alarmsetting</i> selects the notification alarm parameter. <i>alarmoption</i> configures the parameter. The values must be one of the following: - <i>blocked-ip-enable</i> — <i>enable</i> or <i>disable</i> - <i>remote-enable</i> — <i>enable</i> or <i>disable</i> - <i>trap-enable</i> — <i>enable</i> or <i>disable</i> - <i>launch-interval</i> — an integer from 60 to 3932100 - <i>repeat-count</i> — an integer from 1 to 256 - <i>action-type</i> — <i>email</i> or <i>popup</i> You can configure more than one alarm setting.
<b>ip blocked-site duration <i>minutes</i></b>
Configure the duration that a site remains on the blocked sites list after being automatically added due to packet handling rules. <i>minutes</i> is an integer from 1 to 99999.
<b>ip blocked-site dynamic <i>ip-address</i> expire-after <i>day dd hour hh minute min second sec</i></b>
Blocks all traffic from specified IP addresses for the specified time. <i>ip-address</i> is the host to be temporarily blocked. <i>dd</i> is the number of days from 0 to 365. <i>hh</i> is the number of hours from 0 to 23. <i>min</i> is the number of minutes from 0 to 59. <i>sec</i> is the number of seconds from 0 to 59.
<b>ip blocked-site dynamic flush</b>
Flushes all the status of the dynamically blocked sites.
<b>ip blocked-site <i>address</i> alarm <i>alarmsetting</i> <i>alarmoption</i></b>

<p>Blocks all traffic from specified host, subnet or range of IP addresses.</p> <p><b>address</b> must be one of the following: <i>host ip</i>, <i>subnet net</i>, or <i>range startip endip</i>.</p> <ul style="list-style-type: none"> <li>- <i>ip</i>, <i>startip</i>, and <i>endip</i> must be an IP address in the format of A.B.C.D.</li> <li>- <i>net</i> must be an IP subnet in the format of A.B.C.D/# where # must be in the range of 0 to 32.</li> </ul> <p><i>alarmsetting</i> selects the notification alarm parameter. <i>alarmoption</i> configures the parameter. The values must be one of the following:</p> <ul style="list-style-type: none"> <li>- <i>blocked-ip-enable</i> — <i>enable</i> or <i>disable</i></li> <li>- <i>remote-enable</i> — <i>enable</i> or <i>disable</i></li> <li>- <i>trap-enable</i> — <i>enable</i> or <i>disable</i></li> <li>- <i>launch-interval</i> — an integer from 60 to 3932100</li> <li>- <i>repeat-count</i> — an integer from 1 to 256</li> <li>- <i>action-type</i> — <i>email</i> or <i>popup</i></li> </ul> <p>You can configure more than one alarm setting.</p>
<p><b>ip dns domain-name domain</b></p> <p>Provide a domain name to complete unqualified host names.</p> <p><b>domain</b> is the provided domain name.</p>
<p><b>ip dns servers address</b></p> <p>Adds or removes a DNS server(s).</p> <p><b>address</b> is the IP address of a DNS server. You can configure a maximum of three IP addresses. Use <b>no ip dns servers</b> to remove all DNS server entries.</p>
<p><b>ip dynamic-routing type</b></p> <p>Set routing protocol.</p> <p><b>type</b> must be one of the following: <i>bgp</i>, <i>ospf</i>, or <i>rip</i>.</p>
<p><b>ip route option fwdaddr metric metricvalue</b></p> <p>Create a static network route.</p> <p><b>option</b> must be one of the following: <i>address</i> or <i>net</i>.</p> <ul style="list-style-type: none"> <li>- <i>address</i> is the IP address for the destination in the format of A.B.C.D.</li> <li>- <i>net</i> 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.</li> </ul> <p><b>fwdaddr</b> is the forwarding router's address in the format of A.B.C.D.</p> <p><b>metricvalue</b> is the route metric. It must be an integer from 1 to 1024.</p>
<p><b>ip wins servers address</b></p> <p>Configure WINS servers used by the WatchGuard device for services such as MVPN and DHCP.</p> <p><b>address</b> must be an IP address in the format of A.B.C.D.</p> <p>You can configure a maximum of three IP addresses.</p> <p>Use <b>no ip wins servers</b> to clear all WINS server addresses out of the configuration.</p>
<p><b>ip blocked-site duration minutes</b></p> <p>Configure the duration that a site remains on the blocked sites list after being automatically added due to packet handling rules.</p> <p><b>minutes</b> is an integer from 1 to 99999.</p>
<p><b>ip blocked-site dynamic ip-address expire-after day dd hour hh minute min second sec</b></p> <p>Blocks all traffic from specified IP addresses for the specified time.</p> <p><b>ip-address</b> is the host to be temporarily blocked.</p> <p><b>dd</b> is the number of days from 0 to 365.</p> <p><b>hh</b> is the number of hours from 0 to 23.</p> <p><b>min</b> is the number of minutes from 0 to 59.</p> <p><b>sec</b> is the number of seconds from 0 to 59.</p>

**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 200.23.103.0/24
ip blocked-site duration 15
ip dns domain-name watchguard.com
ip dns servers 192.168.1.1 192.168.1.2
ip dynamic-routing bgp
ip route 100.100.101.3 200
ip wins servers 192.168.1.1 192.168.1.2
    
```

## log-setting

**Description:** Enable message logging facilities.

**Syntax:**

<b>log-setting log-level <i>type level</i></b>
Control debug log messages of the type and level specified. <b>type</b> must be one of the following: <i>Authentication, FireCluster-2, Cluster-Management-3, Cluster-Operation-4, Cluster-Event-Monitoring-5, Cluster-Transport-6, Firewall-7, Management-8, Networking-9, DHCP-client-10, DHCP-server-11, PPP-12, PPPoE-13, Proxy-14, Connection-Framework-Manager-15, Session-Manager-16, DNS-17, FTP-18, H323-19, HTTP-20, HTTPS-21, POP3-22, SMTP-23, SIP-24, TCP-UDP-25, TFTP-26, Security-Subscriptions-27, Gateway-Antivirus-28, spamBlocker-29, WebBlocker-30, VPN-31, IKE-32, PPTP-33, or SSLVPN-34.</i> <b>level</b> must be one of the following: <i>Off, Error, Warning, Information, or Debug.</i>
<b>log-setting syslog-server enable <i>address option</i></b>
Send log messages to a remote syslog server. <i>address</i> is the IP address of a remote syslog server. It must be in the format of A.B.C.D. <b>option</b> must be one of the following: <i>default</i> or <b>type <i>setting1 setting2</i></b> . <ul style="list-style-type: none"> <li>- <b>type</b> must be one of the following: <i>alarm, event, traffic, debug, or support.</i></li> <li>- <b>setting1</b> must be one of the following: <i>auth, priv-auth, cron, daemon, ftp, kern, lpr, mail, news, syslog, user, uucp, local0, local1, local2, local3, local4, local5, local6, or local7.</i></li> <li>- <b>setting2</b> must be one of the following: <i>original, debug, info, notice, warning, err, crit, alert, or emerg.</i></li> </ul>
<b>log-setting <i>type</i> enable</b>
Enable the collection of a specified category of log messages. <b>type</b> must be one of the following: <i>ike-packet-trace, internal-storage, or performance-statistics.</i> Use <b>no log-settings <i>type</i></b> to disable the category of log messages.
<b>log-setting watchguard-log-server enable <i>ip-address key</i></b>
Define the WatchGuard Log Server to be used by the device to send logs. <b>ip-address</b> is the IP address of the WatchGuard Log Server. <b>key</b> is the encryption key used to send information between the device and the 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
    
```

## managed-client

**Description:** Configure the device as a managed client of another WatchGuard device.

**Syntax:**

<b>managed-client device-name <i>name</i></b>
Add the name used to identify the managed client on the Management Server and in reports. <i>name</i> is a unique alphanumeric name which identifies the device.
<b>managed-client enable</b>
Enable the device as a managed client of another WatchGuard device. No options available Use <u>no</u> <b>managed-client</b> to disable the administration of the device as a managed client.
<b>managed-client certificate from <i>location</i></b>
Import a Management Server CA certificate. <i>location</i> must be either a valid FTP or TFTP address or the string <i>console</i> .
<b>managed-client primary <i>address password</i></b>
Set primary Management Server. <i>address</i> is the IP address of the primary Management Server. It must be in the form of A.B.C.D. <i>password</i> is the unencrypted client shared secret.
<b>managed-client secondary <i>address password</i></b>
Set one or more secondary Management Servers. <i>address</i> is the IP address of a secondary Management Server. It must be in the form of A.B.C.D. <i>password</i> is the unencrypted client shared secret. You can configure up to three secondary Management Servers.

**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
```

## modem

**Description:** Configure modem settings for dial-up serial modem failover. For Firebox X Edge e-Series platform only.

**Syntax:**

<b>modem <i>param</i> enable</b>
Enable a modem parameter ( <i>param</i> ). Where <i>param</i> is one of the following: <b>&lt;null&gt;</b> - Enable modem for dial-up failover when all external interfaces are down. <b>manually-dns</b> - Manually configure DNS IP Address. <b>debug-trace</b> - Enables the modem and Point-to-Point Protocol (PPP) debug trace. Use <u>no</u> <b>modem <i>param</i> enable</b> to disable the above modem commands options.
<b>modem telephone <i>tel-no name domain-name passwd dns1 dns2</i></b>
Configure the account settings of the dial-up fail-over. <b>tel-no</b> is the Internet Service Provider's remote access dial-in phone number. <b>name</b> is the user name for PPP authentication. <b>domain-name</b> is the optional domain name for PPP authentication. <b>passwd</b> is the password. <b>dns1</b> is the primary DNS IP Address. <b>dns2</b> is the optional secondary DNS IP Address.

<b>modem account-name <i>name domain-name passwd dns1 dns2</i></b>
Configure or change the account settings of the dial-up failover modem without changing the phone number.
<b>modem alternate-telephone <i>tel-no</i></b>
Add an alternate phone number for the dial-up modem. <b>tel-no</b> is the Internet Service Provider's remote access dial-in alternate phone number.
<b>modem param <i>value</i></b>
Configure modem options for the dial-up failover. <b>param</b> is one of the following: <ul style="list-style-type: none"> <li><b>dial-timeout</b> is the dial-up timeout of the PPP negotiation if the modem does not connect. <ul style="list-style-type: none"> <li>- <b>value</b> is time in seconds from 60 to 300, default is 120.</li> </ul> </li> <li><b>redial-attempts</b> is the number of dial-up attempts before it gives up the PPP negotiation. <ul style="list-style-type: none"> <li>- <b>value</b> is number of redials from 0 to 5 default is 3.</li> </ul> </li> <li><b>inactive-timeout</b> is the inactive session timeout of the PPP connection. <ul style="list-style-type: none"> <li>- <b>value</b> is time in minutes from 0 to 30, default is 0.</li> </ul> </li> <li><b>mtu</b> is Maximum Transmission Unit of the PPP connection. <ul style="list-style-type: none"> <li>- <b>value</b> is in bytes is from 256 to 1500, default is 1500.</li> </ul> </li> <li><b>primary-dns</b> specifies the primary DNS in the DNS settings. <ul style="list-style-type: none"> <li>- <b>value</b> is the IP Address of the primary DNS.</li> </ul> </li> <li><b>secondary-dns</b> specifies the secondary DNS in the DNS settings. <ul style="list-style-type: none"> <li>- <b>value</b> is the IP Address of the secondary DNS.</li> </ul> </li> <li><b>volume</b> specifies the loudness of the modem's volume. <ul style="list-style-type: none"> <li>- <b>value</b> must be one of the following: <i>Off, Low, Medium, or High</i>.</li> </ul> </li> </ul>
<b>modem link-monitor <i>ext-if lm-param option</i></b>
Defines the Link Monitor configuration for Edge devices using a dial-up backup. <b>ext-if</b> is the External Interface being monitored to trigger a failover. <b>lm-param</b> is the Link Monitor parameter. <b>lm-param</b> must be one of the following together with its <b>option</b> . <ul style="list-style-type: none"> <li><b>ping</b> - Enable Ping to probe the remote side of the external link. <ul style="list-style-type: none"> <li>- <b>option</b> is <b>host</b>, the remote host to ping. This can be an IP address or a hostname.</li> <li>- Use <b>no modem link-monitor ext-if ping enable</b> to disable Ping probing.</li> </ul> </li> <li><b>tcp</b> - Enable TCP to probe the remote side of the external link. <ul style="list-style-type: none"> <li>- <b>option</b> is <b>host port</b> where: <b>host</b> is the remote host to negotiate TCP session. This can be an IP address or a host name. The <b>port</b> 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.</li> <li>- Use <b>no modem link-monitor ext-if tcp enable</b> to disable TCP probing.</li> </ul> </li> <li><b>both</b> - 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. <ul style="list-style-type: none"> <li>- <b>option</b> is <b>enable</b>, both the Ping and TCP probe are required for link monitoring.</li> <li>- Use <b>no modem link-monitor ext-if both enable</b> to require either Ping or TCP probe only.</li> </ul> </li> <li><b>probe-interval</b> - The time space between each link monitoring probe. <ul style="list-style-type: none"> <li>- <b>option</b> is <b>sec</b>, the time in seconds from 1 to 1200 and is 15 seconds by default.</li> </ul> </li> <li><b>deactivate-count</b> - The number of consecutive link monitoring failures before it deactivates the external interface. <ul style="list-style-type: none"> <li>- <b>option</b> is <b>number</b>, the number of probes from 1 to 10 and is 3 by default.</li> </ul> </li> <li><b>reactivate-count</b> - The number of consecutive link monitoring successes before it reactivates the external interface. <ul style="list-style-type: none"> <li>- <b>option</b> is <b>number</b>, the number of probes from 1 to 10 and is 3 by default.</li> </ul> </li> </ul>

**Example:**

```
modem enable
modem account-name user1 domain.com mypa55w0rd 202.50.129.53 202.50.130.53
modem telephone 2061234 user1 mypa55w0rd 202.50.129.53
modem alternate-telephone 2064321
```

```
modem dial-timeout 90
modem primary-dns 202.50.129.53
modem link-monitor 0 ping 196.24.1.1
```

## multi-wan

**Description:** Configure the external interfaces to use multi-WAN features.

**Syntax:**

<b>multi-wan type <i>interface</i></b>
Configure the selected interface to use a type of multi-WAN. <i>type</i> must be one of the following: <i>tcp-sticky-timer</i> , <i>udp-sticky-timer</i> , or <i>others-sticky-timer</i> . <i>interface</i> must be an integer from 0 to the maximum interface value on the device.
<b>multi-wan failback-option <i>option</i></b>
Set the action taken when the original address becomes available again. <i>option</i> must be one of the following: <i>gradual</i> or <i>immediate</i> .
<b>multi-wan load-balance failover <i>interface1 interface2</i></b>
Set the failover sequence for interfaces in a multi-WAN failover configuration. <i>interface1</i> is the identifying name of the first interface to which traffic will fail over. <i>interface2</i> is the identifying name of the second interface to which traffic will fail over. You can enter as many interface names as you have interfaces configured for multi-WAN failover. There must be a minimum of two.
<b>multi-wan load-balance interface-overflow <i>interface1 threshold1 interface2 threshold2</i></b>
Set the load balance overflow sequence in a multi-WAN interface overflow configuration. <i>interface1</i> is the identifying name of the first interface to which traffic will distribute traffic. <i>threshold1</i> is the threshold value in 100 Kbps increments. It must be an integer from 0 to 10000. <i>interface2</i> is the identifying name of the second interface to which traffic will distribute traffic. <i>threshold2</i> 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.
<b>multi-wan load-balance round-robin <i>interface1 weight1 interface2 weight2</i></b>
Set the round-robin sequence in a multi-WAN round-robin configuration. <i>interface1</i> is the identifying name of the first interface to which traffic will distribute traffic. <i>weight1</i> is the round-robin weight. It must be an integer from 0 to 65535. <i>interface2</i> is the identifying name of the second interface to which traffic will distribute traffic. <i>weight2</i> 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.
<b>multi-wan load-balance routing-table <i>interface1 interface2</i></b>
Set the interface sequence in a multi-WAN routing table configuration. <i>interface1</i> is the identifying name of the first interface to which traffic will distribute traffic. <i>interface2</i> is the identifying name of the second interface to which traffic will distribute traffic. You can enter as many interface names as you have interfaces configured for multi-WAN routing table. There must be a minimum of two.

<p><b>multi-wan link-monitor <i>interface interval frequency deactivate-count dcount reactivate-count rcount operation andor ICMP icmpaddress TCP tcpaddress</i></b></p> <p>Set the method to use to check the status of an interface configured for multi-WAN.</p> <p><b><i>interface</i></b> is the number of the external interface. It must be an integer from 0 to 7.</p> <p><b><i>frequency</i></b> is interval in seconds between probes. It must be an integer from 1 to 1200. The default value is 15.</p> <p><b><i>dcount</i></b> is the number of failures that must occur for the device to deactivate the interface. The default value is 3.</p> <p><b><i>rcount</i></b> is the number of successes that must occur for the device to reactivate the interface. The default value is 3.</p> <p><b><i>andor</i></b> sets whether the probe uses both TCP and PING to check status or only one. It must be either: <i>AND</i> or <i>OR</i>. The default value is <i>OR</i>.</p> <p><b><i>icmpaddress</i></b> is the IP address of destination host which the device can ping to check status. It must be an address in the format A.B.C.D.</p> <p><b><i>tcpaddress</i></b> is the IP address and port of a destination host which the device can 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.</p>
---

**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
```

## network-mode

**Description:** Set system mode.

**Syntax:**

<p><b>network-mode <i>option</i></b></p> <p><b><i>option</i></b> must be one of the following: <i>routed</i>, <b>drop-in</b> <i>address gateway</i>, or <b>bridge</b> <i>address gateway</i>.</p> <ul style="list-style-type: none"> <li>- <i>address</i> is the IP address used as the primary address for all interfaces on the device. 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.</li> <li>- <i>gateway</i> is the IP address of default gateway. It must be in the form A.B.C.D.</li> </ul>
<p><b>network-mode auto-host-mapping <i>if-number setting if-number setting</i></b></p> <p>Specify the interface that needs automatic host mapping.</p> <p><b><i>if-number</i></b> is the interface index number.</p> <p><b><i>setting</i></b> must be either of the following: <i>enable</i> or <i>disable</i>. You may specify more than one interface with their respective settings.</p>
<p><b>network-mode dhcp relay <i>serverip</i></b></p> <p>Configure to relay DHCP requests to the specified server.</p> <p><b><i>serverip</i></b> is the IP address of the DHCP server being used for computers on the interface. Use <b>no dhcp enable</b> to disable DHCP relay on the interface.</p>
<p><b>network-mode dhcp server start-addr <i>startip endip leasetime dns-server dns* domain domainname reservation resvname macaddress ipaddress wins wins*</i></b></p>

<p>Configure as a DHCP server for computers connected to the device.</p> <p><b>start-addr</b> defines a DHCP address pool. In the same line, you can use the start-addr command multiple times with the following parameters:</p> <ul style="list-style-type: none"> <li>- <b>startip</b> is the first IP address in the DHCP address pool.</li> <li>- <b>endip</b> is the last IP address in the DHSCP address pool.</li> </ul> <p><b>leasetime</b> is the duration in hours that addresses are leased to devices on the network. The value must be an integer.</p> <p><b>dns*</b> is the IP address of one or more valid DNS servers.</p> <p><b>domainname</b> is the domain name of used by devices on the network.</p> <p><b>reservation</b> 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 the following parameters:</p> <ul style="list-style-type: none"> <li>- <b>resvname</b> is a string to identify a reserved address.</li> <li>- <b>macaddress</b> is the MAC address of the device using a reserved address.</li> <li>- <b>ipaddress</b> is the IP address assigned to the reserved address.</li> </ul> <p>Use <b>no dhcp enable</b> to disable DHCP server on the interface.</p>
<p><b>network-mode related-host ip-address if-number</b></p>
<p><b>ip-address</b> is the IP address being related to the interface.</p> <p><b>if-number</b> is the interface index being related to the IP address.</p>

**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
```

## ntp

**Description:** Configure the device to get timestamps from an NTP server.

**Syntax:**

<p><b>ntp enable</b></p> <p>No options available. Use <b>no ntp</b> to disable use of an NTP server.</p>
<p><b>ntp server ip address</b></p> <p>Add an NTP server using an IP Address. <b>address</b> is the IP address of an NTP server in the format A.B.C.D. Use <b>no ntp server ip address</b> to remove an NTP server from the configuration.</p>
<p><b>ntp server domain hostname</b></p> <p>Add an NTP server using a domain name. <b>hostname</b> is the hostname (FQDN) of an NTP server. Use <b>no ntp server domain hostname</b> to remove an NTP server from the configuration.</p>

**Example:**

```
ntp server ip 200.220.100.12
ntp server domain ntp.foo.org
no ntp server ip 203.201.39.1
```

## policy

**Description:** Enter the Policy command mode.

**Syntax:**

<b>policy</b>
No options available.

**Example:**

```
interface policy
WG(config/policy)#
```

## signature update

**Description:** Configure device to get updated signature files for IPS and Gateway Antivirus.

**Syntax:**

<b>signature-update <i>component action</i></b>
<b>component</b> must be one of the following: <i>IPS</i> or <i>GAV</i> . <b>action</b> must be either: <i>interval</i> , or <b>server-url</b> <i>url</i> . - <i>interval</i> is the frequency between updates measured in hours. - <i>url</i> is the URL of the update server.

**Example:**

```
signature-update gav enable
```

## snmp

**Description:** Configure the device to integrate with SNMP tools.

**Syntax:**

<b>snmp servers <i>address</i></b>
Configure SNMP management stations. <b>address</b> is an IP address in the format A.B.C.D. You can configure up to three SNMP management stations. Use <u>no</u> <b>snmp server address</b> to remove an SNMP management station from the configuration.
<b>snmp version v1_2 <i>community string</i></b>
Configure the device to use SNMP version 1 or 2 polling. <b>string</b> is the value of the community string.
<b>snmp snmp-version v3 <i>username authprotocol authpassword privacytype</i></b>
Configure the device to use SNMP version 3 polling. <b>username</b> is a string for the SNMP user name. <b>authprotocol</b> is the authentication protocol. It must be one of the following: <i>MD5</i> or <i>SHA1</i> <b>authpassword</b> is the user password on the SNMP management station. <b>privacytype</b> is the privacy protocol. It must be either: <b>DES</b> <i>despassword</i> or <i>None</i> . - <i>despassword</i> is the password used to encrypt DES on the SNMP management station.
<b>snmp traps enable <i>type</i></b>
Enable SNMP traps for the device. <b>type</b> must be one of the following: <i>trap v1</i> , <i>trap v2c</i> , <i>trap v3</i> , <i>inform v2</i> , or <i>inform v3</i> .

**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:** Creates an IP address to MAC address binding.

**Syntax:**

<b>static-arp name ip-address mac-address</b>
<i>name</i> the name of the interface.
<i>ip-address</i> the IP address of the computer.
<i>mac-address</i> 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:**

<b>system contact string</b>
<i>string</i> is the name of the system administrator.
<b>system location string</b>
<i>string</i> is the geographic location of the device.
<b>system name string</b>
<i>string</i> is the friendly name of the device as it appears in reports and graphic displays.
<b>system timezone zone</b>
<i>zone</i> is the timezone of the device. It must be a two digit integer from 00 to 62. To get a list of <i>zone</i> values, type <b>help system timezone ?</b>

**Example:**

```
system contact Joe Parchese
system name BigCoHeadquarters
system location Seattle
system timezone 04
```

## vlan

**Description:** Create or edit a VLAN virtual interface on the device.

**Syntax:**

<b>vlan vlannname</b>
<i>vlannname</i> is a string that uniquely identifies the VLAN. Use <u>no</u> <b>vlan vlannname</b> to delete the VLAN virtual interface.

After entering the command **vlan vlanname** the configuration continues to the VLAN details command. The prompt changes to "WG(config/vlan-vlanname)#".

<b>vlan-id id security-zone zone address member if-number option if-number option</b>
<p><b>id</b> is the VLAN unique identifier numbers from 1 to 4094.</p> <p><b>zone</b> is the security zone. It must be one of the following: external, trusted, or optional.</p> <p><b>address</b> is the IP address assigned to the virtual interface.</p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- For External Zone it can be one of the following <i>static-ip</i>, <i>dhcp</i> or <i>pppoe</i>.</li> </ul> <p><b>if-number</b> is the interface index that is assigned as a member of the VLAN.</p> <p><b>option</b> must be one of the following: <i>tagged</i>, or <i>untagged</i>.</p> <p>You can specify more than one member interface of the VLAN.</p>

**Example:**

```
vlan VLAN10
vlan-id 10 security-zone trusted 10.10.1.1/24 member 3 tagged 4 tagged
```

## vpn-setting

**Description:** Enable global VPN settings.

**Syntax:**

<b>vpn-setting setting enable</b>
<p><b>setting</b> must be either: <i>pass-through</i>, or <i>tos-tunnel-flag</i></p> <p>Use <u>no</u> <b>vpn-setting setting enable</b> to disable a global VPN setting.</p>

**Example:**

```
vpn-setting passthrough
vpn-setting tos-tunnel-flag
```

## wireless

**Description:** Configure Wi-Fi settings. For Firebox X Edge e-Series devices only.

**Syntax:**

<b>wireless client status</b>
<p>Enable wireless client as an external interface.</p> <p><b>status</b> must be either <i>enable</i> or <i>disable</i>.</p>
<b>wireless client dhcp-client client clientname host-name hostname l-time ip-address</b>
<p>Configure wireless client settings when negotiating with DHCP server.</p> <p><b>clientname</b> is a string for the optional client name.</p> <p><b>hostname</b> is a string for the optional hostname.</p> <p><b>l-time</b> is a string for the optional lease time from 1 to 2147483647.</p> <p><b>ip-address</b> is a string for the optional preferred IP Address.</p>
<b>wireless client manual-conf ip-address mask gateway</b>
<p>Manually configure wireless client's IP address.</p> <p><b>ip-address</b> is the wireless client's IP address.</p> <p><b>mask</b> is the subnet mask in dotted decimal notation.</p> <p><b>gateway</b> is the default gateway of the wireless External interface.</p>
<b>wireless client pppoe-client username passwd ip-address ac-name acname service svc-name auth-retry num-try dial-on-demand dod-setting idle idle-time retry-delay rd-time retry-enable rd-setting retry-interval r-int retry-num r-num unique u-setting</b>

<p>Configure wireless client's Point-to-Point Protocol over Ethernet settings.</p> <p><b>username</b> is a string for the PPP over Ethernet username.</p> <p><b>passwd</b> is the PPPoE password.</p> <p><b>acname</b> is the access concentrator name</p> <p><b>svc-name</b> is a string for the PPPoE service name.</p> <p><b>num-try</b> is the number of authentication tries allowed. An integer from 0 to 20.</p> <p><b>dod-setting</b> is the dial-on-demand setting. It must be either enable or disable</p> <p><b>idle-time</b> is the idle timeout in minutes. An integer from 0 to 60.</p> <p><b>rd-time</b> is the PPPoE initialization retry delay. An Integer from 0 to 3600.</p> <p><b>re-setting</b> indicates whether to use LCP echo requests to detect lost PPPoE connections. It must be either enable or disable.</p> <p><b>r-int</b> is the retry interval in seconds. An integer from 1 to 1200.</p> <p><b>r-num</b> is the number of times allowed to retry. An integer from 1 to 60.</p> <p><b>u-setting</b> indicates whether to use host-unique tag in PPPoE discovery packets. It must be either enable or disable.</p>
<p><b>wireless wireless-option wireless ssid auth enc enc-option</b></p> <p>Configure wireless authentication and encryption settings.</p> <p><b>wireless-option</b> is the Wi-Fi option. Must be one of the following: <i>client, access-point1, access-point1</i> or <i>guest</i>.</p> <p><b>ssid</b> is a string for the network name.</p> <p><b>auth</b> is the authentication options. It must be one of the following: <i>open-system, shared-key, wpa-only, wpa-wpa2, wpa2-only</i>.</p> <p><b>enc</b> is the encryption options. Depending on the authentication option selected, encryption is based on the following:</p> <ul style="list-style-type: none"> <li>- for <i>open-system</i>, <b>enc</b> must be one of the following: <i>disable, wep-128-ascii, wep-128-hex, wep-40-ascii, wep-64-hex</i>.</li> <li>- for <i>shared-key</i>, <b>enc</b> must be one of the following: <i>wep-128-ascii, wep-128-hex, wep-40-ascii, wep-64-hex</i>.</li> <li>- for <i>wpa-only, wpa-wpa2 and wpa2-only</i>, <b>enc</b> must be one of the following: <i>aes, auto</i> or <i>tkip</i>.</li> </ul> <p><b>enc-option</b> is the option needed to complete the encapsulation. This is depending on the selected encapsulation and is as follows:</p> <ul style="list-style-type: none"> <li>- for <i>disable</i>, <b>enc-option</b> is Null.</li> <li>- for <i>wep-128-ascii, wep-128-hex, wep-40-ascii, and wep-64-hex</i>, <b>enc-option</b> must be a combination of <i>key-index</i> which is an integer from 1 to 4 and <i>key</i> whose length and type is defined on the selected encapsulation.</li> <li>- for <i>aes, auto</i> and <i>tkip</i>, <b>enc-option</b> is the passphrase.</li> </ul>
<p><b>wireless apname param</b></p> <p>Configure the access point and its parameters.</p> <p><b>apname</b> must be one of the following: <i>access-point1, access-point2, or guest</i>.</p> <p><b>param</b> is the access point parameters with its corresponding values.</p> <ul style="list-style-type: none"> <li>- <b>setting</b> is the access point setting. It must be either <i>enable</i> or <i>disable</i>.</li> <li>- <b>broadcast setting</b> is the SSID broadcast setting. <i>setting</i> must be either <i>enable</i> or <i>disable</i>.</li> <li>- <b>interface zone</b> is to bridge the wire to either Trusted or Optional interface. <i>zone</i> must be either <i>trusted</i> or <i>optional</i>.</li> <li>- <b>log-auth setting</b> is to log all authentication events. <i>setting</i> must be either <i>enable</i> or <i>disable</i>.</li> <li>- <b>mac-acl mac-address setting</b> is to restrict access by MAC Address. <i>mac-address</i> is the physical address of the machine being allowed. <i>setting</i> must be either <i>enable</i> or <i>disable</i>.</li> <li>- <b>requirevpn setting</b> is to indicate whether to require encrypted Mobile VPN with IPSec connections. <i>setting</i> must be either <i>enable</i> or <i>disable</i>.</li> <li>- <b>frag-threshold f-threshold</b> is the fragmentation threshold. <i>f-threshold</i> must be an integer from 256 to 2346.</li> <li>- <b>rts-threshold r-threshold</b> is the request to send threshold. <i>r-threshold</i> must be an integer from 256 to 2346.</li> </ul>

**wireless radio-settings *option***

Configure wireless radio settings.

***option*** must be one of the following:

- *channel* is the channel from 0 to 14 with 0 meaning auto.
- *mode* is the radio mode either *IEEE-802dot11g*, *IEEE-802dot11b*, or *both*.
- **region** *op-region* is the operation region.

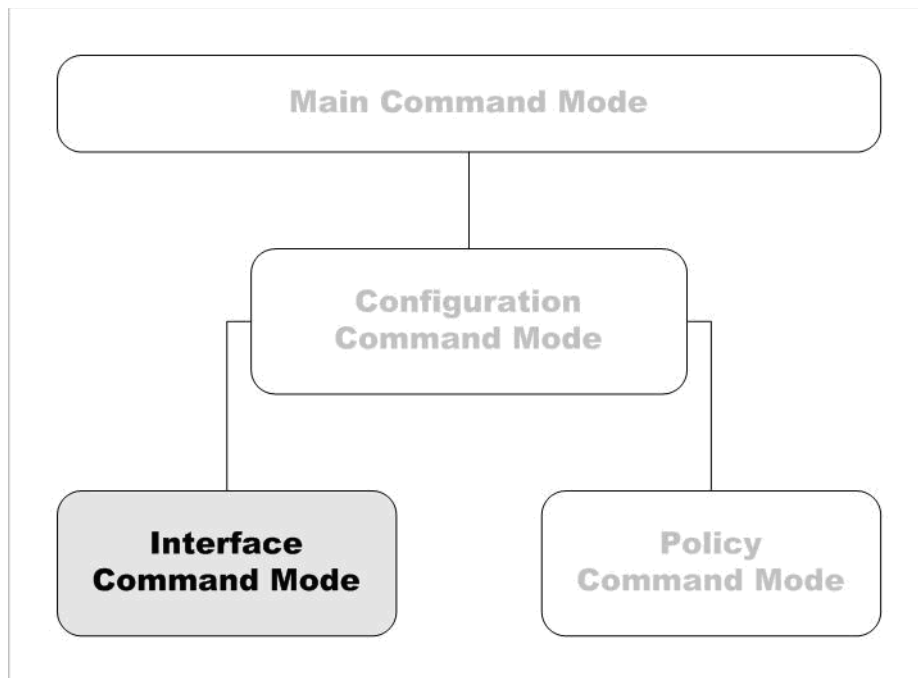
**Example:**

```
wireless client enable
wireless radio-settings region Americas
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 access-point1 enable
wireless access-point1 wireless AP01 shared-key wep-64-hex 1 ab00ab00ab
wireless access-point1 broadcast enable
wireless radio-settings 6
wireless radio-settings both
```

# 6 Interface Command Mode

---

The WatchGuard® Command Line Interface (CLI) Interface command mode is used to configure the separate Ethernet interfaces available on the WatchGuard device.



In the Interface mode, the administrator can do these functions:

- 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

## Access the Interface Command Mode

To get access to the Interface command mode, open the CLI in the Configuration command mode, then use the **interface *string*** command. The CLI prompt changes to `WG(config g/string)#` where *string* 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. For more information, see “List of Common Commands” on page 15. In addition, the following commands are available only in the Interface mode:

Command	Usage
<b>dhcp</b>	Enable the interface as either a DHCP server or relay.
<b>dos-prevention</b>	Enable per interface Denial of Service hacker prevention
<b>enable</b>	Enable or disable the physical interface.
<b>ip</b>	Configure the IP address and addressing options for the interface.
<b>link-speed</b>	Set the link speed and duplex for the interface.
<b>mac-ip-binding</b>	Bind the Ethernet MAC address to a particular IP address.
<b>mtu</b>	Control the interface MTU settings.
<b>name</b>	Set the name for the interface as it appears in reports and the user interface.
<b>pppoe</b>	Configure Point to Point over Ethernet Protocol for the external interface.
<b>qos</b>	Enable QoS Marking for traffic that goes out of the interface.
<b>secondary</b>	Configure secondary IP addresses for use by the interface to route traffic.
<b>type</b>	Set the interface type.
<b>vpn-pmtu</b>	Configure 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 obtain and IP address from an external DHCP server.

**Syntax:**

<b>dhcp relay <i>serverip</i></b>
Configure a trusted or optional interface to relay DHCP requests to the specified server. <i>serverip</i> is the IP address of the DHCP server being used for computers on the interface. Use <u>no</u> <b>dhcp enable</b> to disable DHCP relay on the interface.
<b>dhcp server start-addr <i>startip endip leasetime dns-server dns* domain domainname reservation resvname macaddress ipaddress wins wins*</i></b>

<p>Configure the trusted or optional interface as a DHCP server for computers on that interface.</p> <p><b>start-addr</b> defines a DHCP address pool. In the same line, you can use the start-addr command multiple times with the following parameters:</p> <ul style="list-style-type: none"> <li>- <b>startip</b> is the first IP address in the DHCP address pool.</li> <li>- <b>endip</b> is the last IP address in the DHCP address pool.</li> </ul> <p><b>leasetime</b> is the duration in hours that addresses are leased to devices on the network. The value must be an integer.</p> <p><b>dns*</b> is the IP address of one or more valid DNS servers.</p> <p><b>domainname</b> is the domain name of used by devices on the network.</p> <p><b>reservation</b> 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 the following parameters:</p> <ul style="list-style-type: none"> <li>- <b>resvname</b> is a string to identify a reserved address.</li> <li>- <b>macaddress</b> is the MAC address of the device using a reserved address.</li> <li>- <b>ipaddress</b> is the IP address assigned to the reserved address.</li> </ul> <p>Use <b>no dhcp enable</b> to disable DHCP server on the interface.</p>
<p><b>dhcp any leasetime</b></p>
<p>Configure the external interface to obtain a DHCP-assigned IP address from the ISP.</p> <p><b>leasetime</b> is the duration in hours that addresses are leased to devices on the network. The value must be an integer.</p> <p>Use <b>no dhcp</b> to disable DHCP client on the interface.</p>
<p><b>dhcp host-id hostid host-name hostname ipaddress leasetime</b></p>
<p>Configure a detailed DHCP client on the External interface.</p> <p><b>hostid</b> is the Host ID to use in negotiating IP address from the DHCP server.</p> <p><b>hostname</b> is the Host Name to use in negotiating IP address from the DHCP server.</p> <p><b>ipaddress</b> is to force the DHCP server to lease a specific IP address.</p> <p><b>leasetime</b> is the duration in hours that addresses are leased to devices on the network. The value must be an integer.</p> <p>Use <b>no dhcp host-name host-id lease-time</b> to disable detailed DHCP client on the interface.</p>

**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 watchguard.com reservation ceo 00:44:FF:33:00:AC
10.0.1.35 wins 10.0.1.100
dhcp server wins 10.0.1.100
```

## dos-prevention

**Description:** Configure Denial of Service (DOS) hacker prevention settings.

**Syntax:**

<b>dos-prevention enable</b>
No options available.
Use <b>no enable</b> to disable the interface.

**Example:**

```
dos-prevention enable
```

## enable

**Description:** Enable or disable the physical interface.

**Syntax:****enable**

No options available.

Use no **enable** to disable the interface.

**ip**

**Description:** Configure the IP address and addressing options for the interface.

**Syntax:****ip address option**

Set the IP address of an interface.

**option** must be one of the following: *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 df flag**

Configure Don't Fragment bit on the external interface.

- **flag** must be one of the following: *clear*, *set*, or *copy*.

**Example:**

```
ip address 192.168.116.1 255.255.255.0
ip address 192.168.116.1/24
ip df set
```

**link-speed**

**Description:** Set the interface link speed and duplex.

**Syntax:****link-speed option**

**option** must be one of the following: *auto-negotiate*, *100-full*, *100-half*, or *10-half*.

**Example:**

```
link-speed 100-full
```

**mac-ip-binding**

**Description:** Control access to a WatchGuard device interface 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.

**Example:**

```
mtu 1024
```

**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 username password ipaddress connection option type time retries lcptimeout re-authentication re-auth ac-name acname service-name serv**

Configure an always-on PPPoE client of an external interface.

**username** is the string PPPoE user name.

**password** is the PPPoE password.

**ipaddress** force PPPoE to use this IP address.

**option** must be either: *enable*, or *disable*.

**type** must be either: *always-on*, or *dial-on-demand*.

**time** must be either:

- if **type** is *always-on*, auto-reconnect time in seconds from 0 to 3600.
- if **type** is *dial-on-demand*, inactivity timeout in minutes from 0 to 60.

**retries** number of retries allowed from 1 to 60.

**lcptimeout** is the LCP echo timeout in seconds from 1 to 1200.

**re-auth** is the allowed re-authentication tries from 0 to 20.

**acname** is the Access Concentrator Name.

**serv** is the PPPoE Service Name.

no pppoe unnumbered
Configure PPPoE not to obtain IP address via PPP/IPCP. No options available.

**Example:**

```
pppoe myuser mypasswd 100.100.100.10 connection enable always-on 30 3 10 re-
authentication 5 ac-name concetrator1 service-name serviceA
pppoe myusername mypasswd connection enable dial-on-demand 10 60 100
no pppoe unnumbered
```

## qos

**Description:** Configure Quality of Service settings for the interface.

**Syntax:**

<b>qos marking dscp state priority-method <i>method</i></b>
<i>state</i> is the DSCP state and must be one of the following values: <i>assign type</i> , <i>clear</i> , or <i>preserve</i> . <ul style="list-style-type: none"> <li>- If <i>state</i> is <i>assign</i>, you must add a string for <i>type</i>.</li> <li>- <i>type</i> is the DSCP assign method and must be one of the following values: <i>Best-effort</i>, <i>CS1-Scavenger</i>, <i>AF11</i>, <i>AF12</i>, <i>AF13</i>, <i>CS2</i>, <i>AF21</i>, <i>AF22</i>, <i>AF23</i>, <i>CS3</i>, <i>AF31</i>, <i>AF32</i>, <i>AF33</i>, <i>CS4</i>, <i>AF41</i>, <i>AF42</i>, <i>AF43</i>, <i>CS5</i>, <i>EF</i>, <i>Control-CS6</i>, or <i>Control-CS7</i>.</li> </ul> <i>method</i> is the method used to assign priority and must be one of the following values: <i>No_Priority</i> , <i>Customer</i> , or <i>Mapped-from-Marking</i> .
<b>qos marking precedence state priority-method <i>method</i></b>
<i>state</i> is the precedence state and must be one of the following values: <i>assign value</i> , <i>clear</i> , or <i>preserve</i> . <ul style="list-style-type: none"> <li>- If <i>state</i> is <i>assign</i>, you must add a string for <i>value</i>.</li> <li>- <i>value</i> is the precedence value. It must be an integer from 0 to 7.</li> </ul> <i>method</i> is the method used to assign priority and must be one of the following values: <i>No_Priority</i> , <i>Customer</i> , or <i>Mapped-from-Marking</i> .
<b>qos max-link-bandwidth <i>value</i></b>
<i>value</i> 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:**

<b>secondary <i>address</i></b>
<i>address</i> must be one of the following: <i>addr mask</i> or <i>net</i> <ul style="list-style-type: none"> <li>- <i>addr</i> is an IP address, and must be in the format of A.B.C.D.</li> <li>- <i>mask</i> is an IP subnet mask, and must be in the format of A.B.C.D.</li> <li>- <i>net</i> 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.</li> </ul> This command can take multiple address entries. Use <u>no</u> <b>secondary</b> 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
```

## type

**Description:** Set the interface type.

**Syntax:**

<b>type option</b>
<p><b>option</b> must be one of the following: <i>trusted, optional, external</i> <u>addressmethod</u></p> <p>If <b>option</b> value is <i>external</i>, you must add the parameter <u>addressmethod</u> whose value is: <i>default-gw gateway, dhcp, or pppoe</i>.</p> <ul style="list-style-type: none"> <li>- If <u>addressmethod</u> is <i>default-gw</i>, you must add the parameter <u>gateway</u>.</li> <li>- <u>gateway</u> is IP address and subnet prefix of the default gateway in the format of A.B.C.D/# where # must be in the range of 0 to 32.</li> </ul>

**Example:**

```
type trusted
type external default-gw 100.100.101.0/24
```

## vpn-pmtu

**Description:** Configure PMTU settings for IPSec for an external interface.

**Syntax:**

<b>vpn-pmtu <u>minimum-size size life-time time</u></b>
<p><u>size</u> is the minimum MTU in bytes from 68 to 1550, default is 512.</p> <p><u>time</u> is the aging time of learned PMTU in seconds from 60 to 2147483647, default is 600.</p>

**Example:**

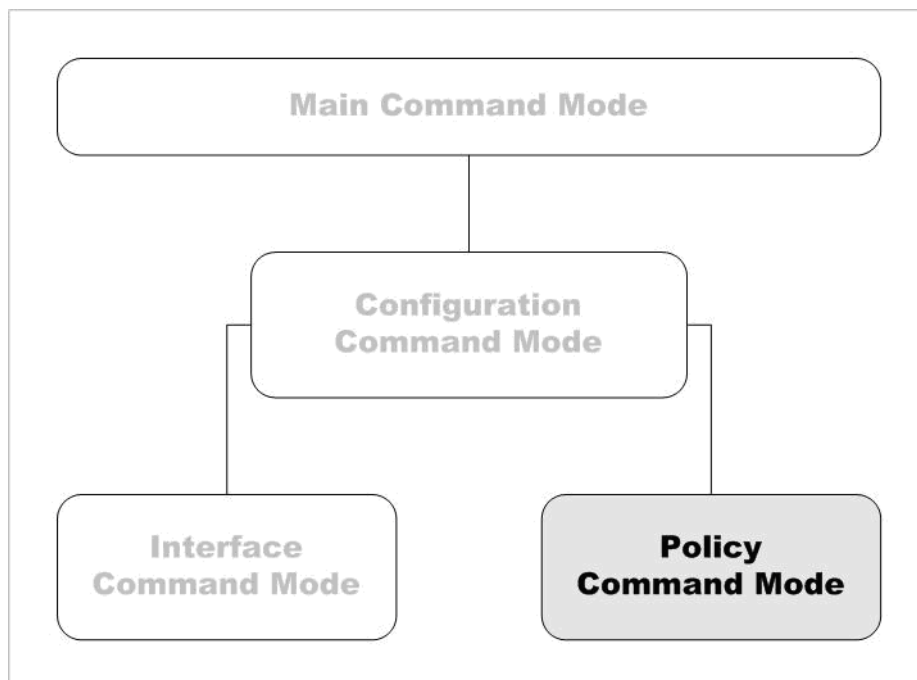
```
vpn-pmtu minimum-size 768 life-time 1200
```



# 7 Policy Command Mode

---

The WatchGuard® Command Line Interface (CLI) Policy command mode is used to configure the fire-wall policies.



In the Policy mode, the administrator can do these functions:

- Create and modify rules 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

## Access the Policy Command Mode

To get access to the Policy command mode, open the CLI in the Configuration command mode, then use the **policy** command. The CLI prompt changes to `WG(confi g/pol i cy)#`.

## List of Policy Mode Commands

You can use all common commands in the Policy command mode. For more information, see “List of Common Commands” on page 15. In addition, the following commands are available only in the Policy mode:

Command	Usage
<b>alias</b>	Create aliases for a group of hosts, networks or interfaces.
<b>apply</b>	Save newly added or edited configuration.
<b>auth-server</b>	Configure authentication server settings.
<b>auth-user-group</b>	Define user groups for authentication.
<b>bovpn-gateway</b>	Configure a BOVPN gateway policy.
<b>bovpn-tunnel</b>	Configure a BOVPN tunnel policy.
<b>dynamic-nat</b>	Enable the a dynamic NAT policy for traffic through the specific interfaces.
<b>mvpn-ipsec</b>	Configure Mobile VPN with IPsec groups.
<b>mvpn-rule</b>	Configure Mobile VPN with IPsec policy rules.
<b>one-to-one-nat</b>	Enable the global use of 1-to-1 NAT to route traffic.
<b>policy-type</b>	Display a list of configured policies or the details of a specific policy
<b>pptp</b>	Configure a Mobile VPN with PPTP policy.
<b>proposal</b>	Configure IPsec Phase 2 proposals.
<b>rule</b>	Configure security policy rules.
<b>schedule</b>	Create and modify a schedule for use in policies.
<b>sslvpn</b>	Configure the device to allow Mobile VPN with SSL.
<b>traffic-management</b>	Define traffic management actions for use in policies.
<b>user-group</b>	Create a user group for use in policies.
<b>users</b>	Add individual users for use in policy rules.

# Policy Command Mode Reference

## alias

**Description:** Create shortcuts to identify a group of hosts, networks, or interfaces.

**Syntax:**

<b>alias name description desc option</b>
<p>Configure an alias for a single device, network, or IP address range.</p> <p><b>name</b> is the unique string that identifies the alias. You cannot use spaces.</p> <p><b>desc</b> is a string that describes the use of the alias. You cannot use spaces.</p> <p><b>option</b> must be one of the following: <b>address</b>, <b>network-ip net</b>, or <b>host-range startip endip</b>.</p> <ul style="list-style-type: none"> <li>- <b>address</b> is the IP address of a device on the network. It must be in the format A.B.C.D.</li> <li>- <b>net</b> is the IP address of a device on the network. It must be in the format A.B.C.D/# where # is a number between 0 and 32.</li> <li>- <b>startip</b> is the first IP address in the range. It must be in the format A.B.C.D.</li> <li>- <b>endip</b> is the last IP address in the range. It must be in the format A.B.C.D.</li> </ul>
<b>alias name description desc tunnel-address tunnel tunnelname address address user-group userdefinition</b>
<p>Configure an alias for a tunnel to define the user or group, address, and tunnel name.</p> <p><b>name</b> is the unique string that identifies the alias. You cannot use spaces.</p> <p><b>desc</b> is a string that describes the use of the alias. You cannot use spaces.</p> <p><b>tunnelname</b> is a string that identifies the tunnel.</p> <p><b>address</b> must be one of the following: <b>address</b>, <b>network-ip net</b>, or <b>host-range startip endip</b>.</p> <ul style="list-style-type: none"> <li>- <b>address</b> is the IP address of a device on the network. It must be in the format A.B.C.D.</li> <li>- <b>net</b> is the IP address of a device on the network. It must be in the format A.B.C.D/# where # is a number between 0 and 32.</li> <li>- <b>startip</b> is the first IP address in the range. It must be in the format A.B.C.D.</li> <li>- <b>endip</b> is the last IP address in the range. It must be in the format A.B.C.D.</li> </ul> <p><b>userdefinition</b> defines a user or group for the tunnel. It is composed of <b>usergroup groupname authmethod</b> where:</p> <ul style="list-style-type: none"> <li>- <b>usergroup</b> is either: <i>user</i> or <i>group</i>.</li> <li>- <b>groupname</b> is a string for a user or group as already defined on the device.</li> <li>- <b>authmethod</b> is one of the following: <i>Firebox-DB</i>, <i>RADIUS</i>, <i>LDAP</i>, <i>SecurID</i>, or <i>Active-Directory</i>.</li> </ul>
<b>alias name description desc custom-address interface if-name address tunneladdress user-group userdefinition</b>
<p>Configure an alias to define the user or group, address, and an interface on the device.</p> <p><b>name</b> is the unique string that identifies the alias. You cannot use spaces.</p> <p><b>desc</b> is a string that describes the use of the alias. You cannot use spaces.</p> <p><b>if-name</b> is the name of the device interface.</p> <p><b>address</b> must be one of the following: <b>address</b>, <b>network-ip net</b>, or <b>host-range startip endip</b>.</p> <ul style="list-style-type: none"> <li>- <b>address</b> is the IP address of a device on the network. It must be in the format A.B.C.D.</li> <li>- <b>net</b> is the IP address of a device on the network. It must be in the format A.B.C.D/# where # is a number between 0 and 32.</li> <li>- <b>startip</b> is the first IP address in the range. It must be in the format A.B.C.D.</li> <li>- <b>endip</b> is the last IP address in the range. It must be in the format A.B.C.D.</li> </ul> <p><b>userdefinition</b> defines a user or group for the tunnel. It is composed of <b>usergroup groupname authmethod</b> where:</p> <ul style="list-style-type: none"> <li>- <b>usergroup</b> is either: <i>user</i> or <i>group</i>.</li> <li>- <b>groupname</b> is a string for a user or group as already defined on the device.</li> <li>- <b>authmethod</b> is one of the following: <i>Firebox-DB</i>, <i>RADIUS</i>, <i>LDAP</i>, <i>SecurID</i>, or <i>Active-Directory</i>.</li> </ul>
<b>alias name description desc alias aliasname</b>

<p>Configure an alias to another alias.</p> <p><b>name</b> is the unique string that identifies the alias. You cannot use spaces.</p> <p><b>desc</b> is a string that describes the use of the alias. You cannot use spaces.</p> <p><b>aliasname</b> is an alias already configured on the device.</p>
<p><b>alias name description desc user-group userdefinition</b></p>
<p>Configure an alias to an authentication user or group.</p> <p><b>name</b> is the unique string that identifies the alias. You cannot use spaces.</p> <p><b>desc</b> is a string that describes the use of the alias. You cannot use spaces.</p> <p><b>userdefinition</b> defines a user or group for the tunnel. It is composed of <b>usergroup groupname authmethod</b> where:</p> <ul style="list-style-type: none"> <li>- <b>usergroup</b> is either: <i>user</i> or <i>group</i>.</li> <li>- <b>groupname</b> is a string for a user or group as already defined on the device.</li> <li>- <b>authmethod</b> is one of the following: <i>Firebox-DB, RADIUS, LDAP, SecurID, or Active-Directory</i>.</li> </ul>

**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
```

## apply

**Description:** Apply configuration changes to the device.

**Syntax:**

<b>apply</b>
No options available.

## auth-server

**Description:** Configure the device to use an authentication server.

**Syntax:**

```
auth-server type primary enable primaryIP secondary enable secondaryIP search-base
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 device to use an LDAP or Active-Directory authentication server.

**type** must be one of the following: *LDAP* or *Active-Directory*.

**primaryIP** is the IP address of the primary authentication server. It must be in the format A.B.C.D.

**secondaryIP** is the IP address of the secondary authentication server. It must be in the format A.B.C.D.

**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 and you want to limit the search in this OU only 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 10.

**dnsstring** is the distinguished name of a search operation. The maximum characters allowed is 255.

**groupstring** is an attribute on an LDAP server that holds user group information. The maximum characters allowed is 31.

**idletimeout** is the duration allowed 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 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.

```
auth-server type primary enable primaryIP secret1 secret1 secondary enable secondary IP secret2
deadtime deadtimevalue group groupnumber port portnumber retry retries timeout
timeoutvalue
```

Configure the device to use a RADIUS or SecurID authentication server.

**type** must be one of the following: *RADIUS* or *SecurID*.

**primaryIP** is the IP address of the primary authentication server. It must be in the format A.B.C.D.

**secondaryIP** is the IP address of the secondary authentication server. It must be in the format A.B.C.D.

**secret1** is the shared secret between the device and the primary authentication server.

**secret2** is the shared secret between the device and the secondary authentication server.

**deadtimevalue** is the duration in minutes before a dead server is marked as active again. It must be an integer from 0 to 86400. The default value is 10.

**groupnumber** is 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.

**Example:**

```
auth-server Active-Directory primary enable 192.168.110.5 secondary enable
192.168.110.6
```

```
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-user-group

**Description:** Create authentication users and groups in the WatchGuard device internal database.

**Syntax:**

<b>auth-user-group <i>name type server desc</i></b>
Define an authentication group or single user. <b><i>name</i></b> is a string to uniquely identify the authentication group or user. <b><i>type</i></b> must be either: <i>user</i> , or <i>group</i> . <b><i>server</i></b> must be one of the following: <i>Firebox-DB</i> , <i>LDAP</i> , <i>RADIUS</i> , <i>Active-Directory</i> , or <i>SecurID</i> . - <b><i>desc</i></b> is a string to describe the authentication group or user.

**Example:**

```
auth-user-group jackp user Chief_Executive_Officer
auth-user-group executives group VIPs
```

## bovpn-gateway

**Description:** Configure a branch office virtual private network (BOVPN) gateway.

**Syntax:**

<b>bovpn-gateway <i>name</i></b>
Assign a unique name to a BOVPN gateway. <b><i>name</i></b> is a string that uniquely identifies the BOVPN gateway.

After entering the command **bovpn-gateway name** the configuration continues to the BOVPN Gateway details command. The prompt changes to "WG(confi g/pol i cy/bovpngateway-name) #".

<b>endpoint rgateway rgatewayid lgatewayid interface authentication</b>
<p>Configure the general settings for a BOVPN gateway. At first, this is the only command available when you define a BOVPN Gateway. After you enter the endpoint command, other BOVPN Gateway commands become available.</p> <p><b>name</b> is the gateway name. The maximum character length is 124.</p> <p><b>rgateway</b> must be either: <i>dynamic</i> or <b>rem-ip-address</b></p> <ul style="list-style-type: none"> <li>- <b>rem-ip-address</b> is an IP address for the remote gateway in the format A.B.C.D.</li> </ul> <p><b>rgatewayid</b> must be either: <b>rem-ip-address</b> or <i>by-domain method domainname</i></p> <ul style="list-style-type: none"> <li>- <b>rem-ip-address</b> is an IP address for the remote gateway in the format A.B.C.D.</li> <li>- <b>method</b> is one of the following: <i>domain-name</i>, <i>user-domain</i>, or <i>x500</i>.</li> <li>- <b>domainname</b> is the string that represents the domain name.</li> </ul> <p><b>lgatewayid</b> must be either: <b>loc-ip-address</b> or <i>by-domain method domainname</i></p> <ul style="list-style-type: none"> <li>- <b>loc-ip-address</b> is an IP address for the local gateway in the format A.B.C.D.</li> <li>- <b>method</b> is one of the following: <i>domain-name</i> or <i>user-domain</i>.</li> <li>- <b>domainname</b> is the string that represents the domain name.</li> </ul> <p><b>interface</b> is the alias of the external interface used for the local gateway.</p> <p><b>authentication</b> is the method used to secure the tunnel. It must be either: <b>certificate</b> or <b>preshared</b></p> <ul style="list-style-type: none"> <li>- <b>certificate</b> is in the form of: <b>certificate id type algorithm name</b> where: <ul style="list-style-type: none"> <li>* <b>id</b> is the certificate identification number</li> <li>* <b>type</b> must be one of the following: <i>none</i>, <i>ip-address</i>, <i>domain</i>, <i>user-domain</i>, or <i>x500</i></li> <li>* <b>algorithm</b> is either: <i>rsa</i> or <i>dsa</i></li> <li>* <b>name</b> is the certificate name</li> </ul> </li> <li>- <b>presharedkey</b> is in the form of: <b>pre-shared secret</b> where: <ul style="list-style-type: none"> <li>* <b>secret</b> is the shared secret used to negotiate the tunnel</li> </ul> </li> </ul>
auto-start enable
<p>Configure the BOVPN tunnel to start negotiation as soon as the device restarts.</p> <p>No options available.</p>
<b>certificate id type algorithm name</b>
<b>Edit device IPsec certificate used in BOVPN.</b>
<p><b>id</b> is the certificate identification number</p> <p><b>type</b> must be one of the following: <i>none</i>, <i>ip-address</i>, <i>domain</i>, <i>user-domain</i>, or <i>x500</i></p> <p><b>algorithm</b> is either: <i>rsa</i> or <i>dsa</i></p> <p><b>name</b> is the certificate name</p>
phase1 attribute

<p>Add or edit phase 1 configurations of BOVPN.</p> <p><b>attribute</b> is one of the following:</p> <ul style="list-style-type: none"> <li>- <b>p1-attrib enable</b> <ul style="list-style-type: none"> <li>* <b>p1-attrib</b> is one of the following: <i>dead-peer-detection</i>, <i>ike-keep-alive</i>, or <i>nat-traversal</i></li> </ul> </li> <li>- <b>dpd-max-retries tries traffic-idle-timeout time</b> <ul style="list-style-type: none"> <li>* <b>tries</b> is an integer from 1 to 30.</li> <li>* <b>time</b> is an integer from 10 to 300.</li> </ul> </li> <li>- <b>keep-alive-interval k-time</b> <ul style="list-style-type: none"> <li>* <b>k-time</b> is an integer from 1 to 65535. The IKE keep-alive interval for NAT traversal.</li> </ul> </li> <li>- <b>max-failures count</b> <ul style="list-style-type: none"> <li>* <b>count</b> is an integer from 1 to 30. The maximum number of failures before BOVPN stops sending IKE keep-alive.</li> </ul> </li> <li>- <b>message-interval mi-time</b> <ul style="list-style-type: none"> <li>* <b>mi-time</b> is an integer from 0 to 300. The message interval for IKE keep-alive.</li> </ul> </li> <li>- <b>mode gw-mode</b> <ul style="list-style-type: none"> <li>* <b>gw-mode</b> is the gateway mode. It must be one of the following: <i>Main</i>, <i>Aggressive</i>, or <i>Main-Fallback-Aggressive</i></li> </ul> </li> <li>- <b>transform index method encrypt life group</b> <ul style="list-style-type: none"> <li>* <b>index</b> is the transform index to edit the previously configured transform settings.</li> <li>* <b>method</b> is either: <i>MD5</i>, or <i>SHA1</i></li> <li>* <b>encrypt</b> is one of the following: <ul style="list-style-type: none"> <li>* <i>DES life unit t-unit</i></li> <li>* <i>DES-3 life unit t-unit</i></li> <li>* <i>AES life encrypt-key-length length unit t-unit</i></li> </ul> </li> <li>where: <ul style="list-style-type: none"> <li>* <b>life</b> is the SA life</li> <li>* <b>length</b> is the AES encryption key length</li> <li>* <b>t-unit</b> is either: <i>minute</i>, or <i>hour</i></li> </ul> </li> <li>* <b>group</b> is one of the following: <i>Diffie-Hellman-Group1</i>, <i>Diffie-Hellman-Group2</i>, or <i>Diffie-Hellman-Group5</i></li> </ul> </li> </ul>
<p><b>pre-shared secret</b></p>
<p>Edit the pre-shared secret key of the BOVPN.</p> <p><b>secret</b> is the shared secret used to negotiate the tunnel.</p>

**Example:**

```
bovpn-gateway Headquarters
endpoint 202.58.165.10 202.58.165.10 216.129.32.20 External pre-shared
n0s3cr3+!
phase1 transform MD5 DES 120 encrypt-key-length 16 unit hour Diffie-Hellman-
Group1
pre-shared mys3cr3tk3y
```

## bovpn-tunnel

**Description:** Create or modify a tunnel for a branch office virtual private network.

**Syntax:**

<p><b>bovpn-tunnel name</b></p>
<p>Assign a unique name to a BOVPN tunnel.</p> <p><b>name</b> is a string that uniquely identifies the BOVPN tunnel.</p>

After you enter the command **bovpn-gateway name** the configuration continues to the BOVPN Tunnel details command. The prompt changes to “WG(confi g/pol i cy/bovpntunnel -name)#”.

<b>gateway gateway localaddress remoteaddress direction enable-broadcast</b>
<p>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, <b>localaddress</b> and <b>remoteaddress</b> are required fields but during tunnel edits these fields are no longer required.</p> <p><b>gateway</b> is the gateway name.</p> <p><b>localaddress</b> must use one of the following formats:</p> <ul style="list-style-type: none"> <li>- <b>host ipaddress</b> where <b>ipaddress</b> is an IP address for the local end point in the format A.B.C.D.</li> <li>- <b>range start-ip startip end-ip endip</b> where: <ul style="list-style-type: none"> <li>* <b>startip</b> is the first IP address of a range in the format A.B.C.D.</li> <li>* <b>endip</b> is the last IP address of a range in the format A.B.C.D.</li> </ul> </li> <li>- <b>subnet net</b> where <b>net</b> is a network address and mask in the format A.B.C.D./#</li> </ul> <p><b>remoteaddress</b> must use one of the following formats:</p> <ul style="list-style-type: none"> <li>- <b>host ipaddress</b> where <b>ipaddress</b> is an IP address for the local end point in the format A.B.C.D.</li> <li>- <b>range start-ip startip end-ip endip</b> where: <ul style="list-style-type: none"> <li>* <b>startip</b> is the first IP address of a range in the format A.B.C.D.</li> <li>* <b>endip</b> is the last IP address of a range in the format A.B.C.D.</li> </ul> </li> <li>- <b>subnet net</b> where <b>net</b> is a network address and mask in the format A.B.C.D./#</li> </ul> <p><b>direction</b> sets the direction of the traffic through the tunnel. You must use one of the following:</p> <ul style="list-style-type: none"> <li>- <i>bi-direction</i> <b>nat-type</b> — traffic routed both ways through the tunnel (default)</li> <li>- <i>inbound</i> <b>nat-type</b> — traffic routed from the remote address to the local address</li> <li>- <i>outbound</i> <b>nat-type</b> — traffic routed from the local address to the remote address</li> </ul> <p>* <b>nat-type</b> must be <b>type ip-address</b> where:</p> <ul style="list-style-type: none"> <li>* <b>type</b> is one of the following: <ul style="list-style-type: none"> <li>* <i>dnat</i> — Dynamic NAT IP address for either inbound or outbound only.</li> <li>* <i>host-ip</i> — 1-to-1 NAT host IP address.</li> <li>* <i>network-ip</i> — 1-to-1 NAT network IP address.</li> <li>* <i>range-ip</i> — 1-to-1 range IP address.</li> </ul> </li> <li>* <b>ip-address</b> is in the format A.B.C.D. or A.B.C.D/(0 to 32) whichever is applicable.</li> </ul> <p><b>enable-broadcast</b> must be <b>broadcast-over-tunnel enable</b> to enable Broadcast over BOVPN</p>
add-to-policy enable
Add the tunnel to the BOVPN-Allow policies. No options available.
<b>address-pair index localaddress remoteaddress direction enable-broadcast</b>

<p>Add or edit an address pair of the tunnel.</p> <p><b><i>index</i></b> is the index of the address pair to be edited.</p> <p><b><i>localaddress</i></b> must use one of the following formats:</p> <ul style="list-style-type: none"> <li>- <b>host <i>ipaddress</i></b> where <b><i>ipaddress</i></b> is an IP address for the local end point in the format A.B.C.D.</li> <li>- <b>range <i>start-ip startip end-ip endip</i></b> where: <ul style="list-style-type: none"> <li>* <b><i>startip</i></b> is the first IP address of a range in the format A.B.C.D.</li> <li>* <b><i>endip</i></b> is the last IP address of a range in the format A.B.C.D.</li> </ul> </li> <li>- <b>subnet <i>net</i></b> where <b><i>net</i></b> is a network address and mask in the format A.B.C.D./#</li> </ul> <p><b><i>remoteaddress</i></b> must use one of the following formats:</p> <ul style="list-style-type: none"> <li>- <b>host <i>ipaddress</i></b> where <b><i>ipaddress</i></b> is an IP address for the local end point in the format A.B.C.D.</li> <li>- <b>range <i>start-ip startip end-ip endip</i></b> where: <ul style="list-style-type: none"> <li>* <b><i>startip</i></b> is the first IP address of a range in the format A.B.C.D.</li> <li>* <b><i>endip</i></b> is the last IP address of a range in the format A.B.C.D.</li> </ul> </li> <li>- <b>subnet <i>net</i></b> where <b><i>net</i></b> is a network address and mask in the format A.B.C.D./#</li> </ul> <p><b><i>direction</i></b> sets the direction of the traffic through the tunnel. You must use one of the following:</p> <ul style="list-style-type: none"> <li>- <b><i>bi-direction nat-type</i></b> — traffic routed both ways through the tunnel (default)</li> <li>- <b><i>inbound nat-type</i></b> — traffic routed from the remote address to the local address</li> <li>- <b><i>outbound nat-type</i></b> — traffic routed from the local address to the remote address</li> </ul> <p>* <b><i>nat-type</i></b> must be <b><i>type ip-address</i></b> where:</p> <ul style="list-style-type: none"> <li>* <b><i>type</i></b> is one of the following: <ul style="list-style-type: none"> <li>* <b><i>dnat</i></b> — Dynamic NAT IP address for either inbound or outbound only.</li> <li>* <b><i>host-ip</i></b> — 1-to-1 NAT host IP address.</li> <li>* <b><i>network-ip</i></b> — 1-to-1 NAT network IP address.</li> <li>* <b><i>range-ip</i></b> — 1-to-1 NAT range IP address.</li> </ul> </li> <li>* <b><i>ip-address</i></b> is in the format A.B.C.D. or A.B.C.D/(0 to 32) whichever is applicable.</li> </ul> <p><b><i>enable-broadcast</i></b> must be <b>broadcast-over-tunnel enable</b> to enable Broadcast over BOVPN</p>
<p><b>move where</b></p> <p>Move the tunnel either up, down or at a certain indexed location.</p> <p><b><i>where</i></b> must be one of the following:</p> <ul style="list-style-type: none"> <li>- <b><i>up index1</i></b></li> <li>- <b><i>down index1</i></b></li> <li>- <b><i>to index2</i></b></li> <li>* <b><i>index1</i></b> or <b><i>index2</i></b> is the arbitrary location where the tunnel will move to. If <b><i>index1</i></b> is omitted it is understood to be a value of 1.</li> </ul>
<p><b>multicast-settings enable origin-ip group-ip direction</b></p> <p>Configure the tunnel to allow multicast packets.</p> <p><b><i>origin-ip</i></b> is the origination IP address of the multicast.</p> <p><b><i>group-ip</i></b> is the multicast address of the receiving hosts.</p> <p><b><i>direction</i></b> is either of the two:</p> <ul style="list-style-type: none"> <li>- <b><i>input if-index</i></b> — where <b><i>if-index</i></b> is the interface index of one of the trusted or optional interfaces where the multicast origin host is connected.</li> <li>- <b><i>input if-index if-index</i></b> — where <b><i>if-index</i></b> is the interface index or indices of the Trusted or Optional interfaces where the receiving hosts are connected.</li> </ul> <p>When Multicast is enabled the command <code>tunnel -endpoints</code> must be used to define the route for encapsulation.</p>
<p><b>phase2 pfs enable group</b></p> <p>Enable Perfect Forwarding Secrecy of the tunnel.</p> <p><b><i>group</i></b> is the IKE Diffie-Hellman group. Must be one of the following: <i>dh-group1</i>, <i>dh-group2</i>, or <i>dh-group5</i></p>
<p><b>phase2 proposals p2name</b></p> <p>Assign a Phase 2 Proposal to the tunnel.</p> <p><b><i>p2name</i></b> is an existing phase 2 proposal on the device.</p>

**tunnel-endpoints *local-ip remote-ip***

Define the route for encapsulation of broadcast and multicast traffic.

Used only when either or both Broadcast or Multicast is enabled.

***local-ip*** is the unused IP address on the local network of the tunnel address pair.

***remote-ip*** is the unused 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
```

## dynamic-nat

**Description:** Configure the device to use dynamic network address translation.

**Syntax:****dynamic-nat from *local* to *remote***

***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 the protected network.

**Example:**

```
dynamic-nat from webservers to Any-External
```

## mvpn-ipsec

**Description:** Configure device to use Mobile User VPN with IPsec

**Syntax:****mvpn-ipsec *name***

***name*** is the group name of an existing Mobile VPN with IPsec configuration.

Use **no mvpn-ipsec *name*** to disable

After entering the command **mvpn-ipsec name** the CLI continues to the initial Mobile VPN with IPsec configuration command. The prompt changes to “WG(confi g/pol i cy/muvpn-*name*)#”:

<p><b>auth-server auth-svr authmethod is-force-all ip-pool</b></p> <p>Set initial configuration of Mobile VPN with IPsec.</p> <p><b>auth-svr</b> is the authentication server used for Mobile VPN with IPsec. Must be one of the following: <i>Firebox-DB, RADIUS, LDAP, Active-Directory, or SecurID</i>.</p> <p><b>authmethod</b> is the method used to authenticate the tunnel. Must be either of the two:</p> <ul style="list-style-type: none"> <li>- <b>rsa-svr-IP admin-passphrase</b> <ul style="list-style-type: none"> <li>* <b>rsa-svr-IP</b> is the RSA certificate server IP address.</li> <li>* <b>admin-passphrase</b> is the administrator passphrase of the RSA server.</li> </ul> </li> <li>- <b>tunnel-passphrase</b> is the tunnel encryption passphrase.</li> </ul> <p><b>is-force-all</b> is a boolean to denote if it is a Captive Tunnel or Split Tunnel. Must be either of the two: <b>no tunnel-resource</b> or <b>yes</b></p> <ul style="list-style-type: none"> <li>- <b>tunnel-resource</b> is the address of the allowed resource in the format: <b>hostip</b> or <b>network-ip</b> <ul style="list-style-type: none"> <li>* <b>hostip</b> is an IP address in the format A.B.C.D.</li> <li>* <b>network-ip</b> is a network address and mask in the format A.B.C.D./# where # is a number from 0 to 32.</li> </ul> </li> </ul> <p><b>ip-pool</b> is the address to be assigned to mobile computers that connect with Mobile VPN with IPsec in the format: <b>host-ip hostip</b> or <b>range-ip start-ip end-ip</b></p> <ul style="list-style-type: none"> <li>- <b>hostip</b> is an IP address in the format A.B.C.D.</li> <li>- <b>start-ip</b> is the start of range IP address in the format A.B.C.D.</li> <li>- <b>end-ip</b> is the end of range IP address in the format A.B.C.D.</li> </ul>
---

After you enter the command **auth-server auth-svr auth-method is-force-all ip-pool** the CLI continues to the detailed Mobile VPN with IPsec configuration command. This is essentially to edit the initial configuration if you do not want the default values. You must use the **Apply** command before your changes become active.

<p><b>all-traffic-allow enable</b></p> <p>Force all traffic to through the tunnel.</p> <p>Use <b>no all-traffic-allow tunnel-resource</b> to negate this command</p> <ul style="list-style-type: none"> <li>- <b>tunnel-resource</b> is the address of the allowed resource in the format: <b>hostip</b> or <b>network-ip</b> <ul style="list-style-type: none"> <li>* <b>hostip</b> is an IP address in the format A.B.C.D.</li> <li>* <b>network-ip</b> is a network address and mask in the format A.B.C.D./# where # is a number from 0 to 32.</li> </ul> </li> </ul>
<p><b>auth-method authmethod</b></p> <p>Configure or edit the authentication method.</p> <p><b>authmethod</b> is the method used to authenticate the tunnel. Must be either of the two:</p> <ul style="list-style-type: none"> <li>- <b>rsa-svr-IP admin-passphrase</b> <ul style="list-style-type: none"> <li>* <b>rsa-svr-IP</b> is the RSA certificate server IP address.</li> <li>* <b>admin-passphrase</b> is the administrator passphrase of the RSA server.</li> </ul> </li> <li>- <b>tunnel-passphrase</b> is the tunnel encryption passphrase.</li> </ul>
<p><b>auth-server auth-svr</b></p> <p>Set or replace the authentication server.</p> <p><b>auth-svr</b> is the authentication server used for Mobile VPN with IPsec. Must be one of the following: <i>Firebox-DB, RADIUS, LDAP, Active-Directory, or SecurID</i>.</p>
<p><b>firebox-ip primary primary-ip backup backup-ip</b></p> <p>Set the primary and backup IP address of the Firebox or remove the backup IP address used in Mobile VPN with IPsec.</p> <p><b>primary-ip</b> is primary external interface IP address.</p> <p><b>backup-ip</b> is secondary external interface IP address.</p> <p>You may delete only the backup Firebox IP address using the command: <b>no firebox-ip backup</b></p>
<p><b>line-management mode timeout</b></p>

<p>Set line management, for users with Mobile VPN with IPSec v10 client software or later.</p> <p><b><i>mode</i></b> is any of the following: <i>manual</i>, <i>automatic</i>, or <i>variable</i>.</p> <p><b><i>timeout</i></b> is an integer from 0 to 65535.</p>
<p><b>phase1 setting</b></p>
<p>Set or modify the Phase 1 settings.</p> <p><b><i>setting</i></b> is one of the following:</p> <ul style="list-style-type: none"> <li>- <b>authentication <i>authmethod</i></b> where <b><i>authmethod</i></b> must be either: <i>MD5</i> or <i>SHA</i></li> <li>- <b>encryption <i>encrypmethod</i></b> where <b><i>encrypmethod</i></b> must be: <i>DES</i>, <i>TRIPLE-DES</i>, <i>AES-124</i>, <i>AES-192</i>, or <i>AES-256</i></li> <li>- <b>sa-life <i>duration unit unittype</i></b> <ul style="list-style-type: none"> <li>* <b><i>duration</i></b> is an integer from 0 to 2147483647</li> <li>* <b><i>unittype</i></b> is either: <i>hour</i> or <i>minute</i></li> </ul> </li> <li>- <b>key-group <i>grouptype</i></b> where <b><i>grouptype</i></b> must be: <i>dh-group1</i>, <i>dh-group2</i>, or <i>dh-group5</i></li> <li>- <b>nat-traversal enable <i>interval</i></b> where <b><i>interval</i></b> is an integer from 0 to 2147483647</li> <li>- <b>ike-keep-alive enable <i>interval max-failures</i></b> <ul style="list-style-type: none"> <li>* <b><i>interval</i></b> is an integer from 0 to 300</li> <li>* <b><i>max-failures</i></b> is an integer from 1 to 30</li> </ul> </li> <li>- <b>dpd enable <i>timeout max-retries</i></b> <ul style="list-style-type: none"> <li>* <b><i>timeout</i></b> is an integer from 10 to 300</li> <li>* <b><i>max-retries</i></b> is an integer from 1 to 30</li> </ul> </li> </ul>
<p><b>phase2 setting</b></p>
<p>Set or modify a Phase 2 settings.</p> <p><b><i>setting</i></b> is one of the following:</p> <ul style="list-style-type: none"> <li>- <b>authentication <i>authmethod</i></b> where <b><i>authmethod</i></b> must be either: <i>MD5</i> or <i>SHA</i></li> <li>- <b>encryption <i>encrypmethod</i></b> where <b><i>encrypmethod</i></b> must be: <i>DES</i>, <i>TRIPLE-DES</i>, <i>AES-124</i>, <i>AES-192</i>, or <i>AES-256</i></li> <li>- <b>key-expiration-time enable <i>lifetime kbytes unittype</i></b> <ul style="list-style-type: none"> <li>* <b><i>lifetime</i></b> is an integer from 0 to 2147483647, the default is 8.</li> <li>* <b><i>kbytes</i></b> is an integer from 1 to 2147483647</li> <li>* <b><i>unittype</i></b> is either: <i>hour</i> or <i>minute</i></li> </ul> </li> <li>- <b>pfs enable <i>group</i></b> <ul style="list-style-type: none"> <li>* <b><i>group</i></b> is one of the following: <i>dh-group1</i>, <i>dh-group2</i>, or <i>dh-group5</i></li> </ul> </li> </ul>
<p><b>resource-addr tunnel-resource</b></p>
<p>Specify the allowed resources when using Mobile VPN with IPSec.</p> <p><b><i>tunnel-resource</i></b> is the address of the allowed resource in the format: <b><i>hostip</i></b> or <b><i>network-ip</i></b></p> <ul style="list-style-type: none"> <li>- <b><i>hostip</i></b> is an IP address in the format A.B.C.D.</li> <li>- <b><i>network-ip</i></b> is a network address and mask in the format A.B.C.D./# where # is a number from 0 to 32.</li> </ul>
<p><b>timeout option time</b></p>
<p>Set the session and idle time-outs. If the authentication server is also configured with these time-outs they take precedence over these settings</p> <p><b><i>option</i></b> is either of the two: <i>idle</i>, or <i>session</i>.</p> <p><b><i>timeout</i></b> is an integer from 0 to 43200.</p>
<p><b>virtual-addr ip-pool</b></p>
<p>Set the IP address pool to be assigned to mobile computers that connect with Mobile VPN with IPSec.</p> <p><b><i>ip-pool</i></b> is the pool of IP address in the format: <b><i>host-ip hostip</i></b> or <b><i>range-ip start-ip end-ip</i></b></p> <ul style="list-style-type: none"> <li>- <b><i>hostip</i></b> is an IP address in the format A.B.C.D.</li> <li>- <b><i>start-ip</i></b> is the start of range IP address in the format A.B.C.D.</li> <li>- <b><i>end-ip</i></b> is the end of range IP address in the format A.B.C.D.</li> </ul>

**Example:**

```

mvpn-ipsec MVPNIPSecUsers
auth-server Firebox-DB myp@ssphr@s3 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:**

<b>mvpn-rule name</b>
<b>name</b> is the rule name to be assigned to the MVPN IPsec policy rules. Use <code>no mvpn-rule name</code> to delete rule.

After you enter 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(confi g/pol i cy/mvpngrul e-name)#".

<b>mvpn-ipsec name policy-type</b>
Select the Policy Type to be applied to the Mobile VPN with IPsec group. <b>name</b> is the existing Mobile VPN with IPsec group name where the rule is to be applied. <b>policy-type</b> is the pre-define Policy Types assigned to the rule.

After you enter the command **mvpn-ipsec name policy-type**, a range of new commands is available to configure the rule details. You must use the **Apply** command before your changes become active.

<b>option enable</b>
Enable Mobile VPN with IPsec rule options. <b>option</b> must be one of the following: <ul style="list-style-type: none"> <li>- <i>auto-block</i> — auto block external sites that attempt to connect.</li> <li>- <i>icmp-message allow-all</i> — permit all icmp error messages.</li> <li>- <i>icmp-message fragmentation-required</i> — fragmentation required but DF bit is set.</li> <li>- <i>icmp-message host-unreachable</i> — send host unreachable.</li> <li>- <i>icmp-message network-unreachable</i> — send network unreachable.</li> <li>- <i>icmp-message port-unreachable</i> — send port unreachable.</li> <li>- <i>icmp-message protocol-unreachable</i> — send protocol unreachable.</li> <li>- <i>icmp-message time-exceeded</i> — time to live exceeded in transit.</li> <li>- <i>icmp-message use-global</i> — use global settings in the response.</li> </ul>
<b>firewall action</b>
<b>action</b> must be one of the following: <i>allowed, denied, or reject</i> <b>option</b> <ul style="list-style-type: none"> <li>- if action selected is <i>reject</i>, <b>option</b> must be added as one of the following: <i>ICMP_HOST, ICMP_NETWORK, ICMP_PORT, ICMP_PROTOCOL, or TCP_RST</i></li> </ul>
<b>idle-time</b>
Specify custom idle timeout for the rule. <b>time</b> timeout in seconds, an integer from 0 to 2147483647. A 0 value means disable this function.
<b>logging option</b>

<p>Configure logging settings specific to the rule.</p> <p><b>option</b> must be one of the following:</p> <ul style="list-style-type: none"> <li>- <i>log-message</i> <b>enable</b> — send log message.</li> <li>- <i>snmp-trap</i> <b>enable</b> — send SNMP trap.</li> <li>- <i>notification</i> <b>enable action-type type launch-interval interval repeat-count count</b> — send notification, where: <ul style="list-style-type: none"> <li>* <b>type</b> is either <i>email</i> or <i>pop-window</i>. The default is <i>email</i>.</li> <li>* <b>interval</b> is the launch interval in minutes from 1 to 65535. The default value is 15.</li> <li>* <b>count</b> is the repeat count, an integer from 1 to 256. The default value is 10.</li> </ul> </li> </ul>
<p><b>proxy-action action</b></p>
<p>Apply the matching default proxy actions on the rule.</p> <p><b>action</b> must be one of the following: <i>DNS-Outgoing</i>, <i>DNS-Incoming</i>, <i>FTP-Client</i>, <i>FTP-Server</i>, <i>HTTP-Client</i>, <i>HTTP-Server</i>, <i>POP3-Client</i>, <i>POP3-Server</i>, <i>SMTP-Outgoing</i>, <i>SMTP-Incoming</i>, <i>TCP-UDP-proxy</i>, <i>H.323-Client</i>, <i>SIP-Client</i>, <i>DNS-Incoming</i>, <i>HTTPS-Client</i>, or <i>HTTPS-Server</i>.</p>
<p><b>qos enable</b></p>
<p>Override per-interface QoS settings if Traffic Management and QoS are enabled.</p> <p>No available options.</p>
<p><b>qos marking type method priority-method p-method</b></p>
<p><b>type</b> must be either <i>dscp</i>, or <i>precedence</i>.</p> <p><b>method</b> must be either <i>assign m-value</i>, or <i>preserve</i>.</p> <ul style="list-style-type: none"> <li>- if <b>type</b> is <i>dscp</i>, <b>m-value</b> is one of the following: <i>Best-effort</i>, <i>CS1-Scavenger</i>, <i>AF11</i>, <i>AF12</i>, <i>AF13</i>, <i>CS2</i>, <i>AF21</i>, <i>AF22</i>, <i>AF23</i>, <i>CS3</i>, <i>AF31</i>, <i>AF32</i>, <i>AF33</i>, <i>CS4</i>, <i>AF41</i>, <i>AF42</i>, <i>AF43</i>, <i>CS5</i>, <i>EF</i>, <i>Control-CS6</i>, or <i>Control-CS7</i></li> <li>- if <b>type</b> is <i>precedence</i>, <b>m-value</b> is an integer from 0 (normal) to 7 (highest).</li> </ul> <p><b>p-method</b> is a string, must be one of the following: <i>No_Priority</i>, <i>Customized c-value</i>, <i>Mapped-from-Marking</i>.</p> <p><b>c-value</b> is an integer from 0 (normal) to 7 (highest).</p>
<p><b>schedule sked-name</b></p>
<p>Assign an existing schedule to the policy.</p> <p><b>sked-name</b> is the pre-created schedule.</p>
<p><b>specify-user name auth-svr</b></p>
<p>Assign a specific user to the policy.</p> <p><b>name</b> is existing user name.</p> <p><b>auth-svr</b> must be one of the following: <i>Firebox-DB</i>, <i>RADIUS</i>, <i>LDAP</i>, <i>SecurID</i>, or <i>Active-Directory</i>.</p>
<p><b>traffic-mgmt tm-name</b></p>
<p>Assign an existing traffic management action to the policy.</p> <p><b>tm-name</b> is the pre-created traffic management rule.</p>

**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 the following: *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-type

**Description:** Create a custom policy template.

**Syntax:**

**policy-type name timeout group servicegroup servicegroup**

Create a custom policy group 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 2147483647. The default value is 180.

**servicegroup** is the service group assigned to the template. Multiple service groups can be assigned to the template.

**policy-type name timeout protocol prot**

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 value is 180.

All ports are integers from 1 to 65535. **prot** must be in the format of the following options:

- **tcp port-range firstport lastport**
- **tcp port**
- **udp port-range firstport lastport**
- **udp port**
- **gre**
- **ah**
- **esp**
- **any**
- **icmp type code**

\* **type** must be: *Echo\_Reply*, *Destination\_Unreachable*, *Source\_Quench*, *Redirect*, *Echo\_Request*, *Time\_Exceeded*, *Parameter\_Problem*, *Timestamp\_Request*, *Timestamp\_Reply*, *Information\_Request*, *Information\_Reply*, *Address\_Mask\_Request*, *Address\_Mask\_Reply*, or *Any*

\* **code** must be an integer from 0 to 255

**Example:**

```
policy-type funkydb.1 protocol udp 60002
```

## pptp

**Description:** Configure the firewall to allow Mobile VPN with PPTP.

**Syntax:**

<b>pptp enable</b>
No options available. Use <b>no pptp enable</b> to disable Mobile VPN with PPTP.
<b>pptp setting value</b>
Set maximums in bytes. <b>setting</b> must be either: <i>pptp-mtu</i> or <i>pptp-mru</i> <b>value</b> must be an integer from 500 to 1500. The default value is 1400.
<b>pptp pptp-address address</b>
Define the PPTP address pool. <b>address</b> must be either: <b>host ipaddress</b> or <b>range firstip lastip ipaddress</b> , <b>firstip</b> , and <b>lastip</b> are all IP addresses with the format A.B.C.D.
<b>pptp option</b>
Enable PPTP options. <b>option</b> must be one of the following: <b>auth-domain domain</b> where <b>domain</b> is the authentication domain name <b>auth-session-timeout session</b> where <b>session</b> is an integer from 0 to 43200. The default value is 12. <b>auth-idle-timeout idle</b> where <b>idle</b> is an integer from 0 to 43200. The default value is 15. <b>mppe method</b> where <b>method</b> must be: <i>encryption-128-bits</i> , <i>enable-fallback-to-40-bits</i> , or <i>no encryption</i>

**Example:**

```
pptp pptp-mtu 1500
pptp pptp-address range 192.168.110.100 192.168.110.140
pptp auth-session 20
```

## proposal

**Description:** Create Phase 2 Proposals for IPSec VPN.

**Syntax:**

<b>proposal p2 p2name p2type transform life-time life-size encryption authentication</b>
Configures the Phase 2 Proposal details. <b>p2name</b> is a unique string to identify the IPSec Phase 2 Proposal. <b>p2type</b> is the Phase 2 Proposal type. It must be either: <i>ah</i> , or <i>esp</i> . <b>life-time</b> is the SA life time in minutes from 1 to 2147483647. <b>life-size</b> is the SA life size in kilobytes from 1 to 2147483647. <b>encryption</b> 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 the following: <i>none</i> , <i>des</i> , <i>3des</i> , <i>aes128</i> , <i>aes192</i> , or <i>aes256</i> . <b>authentication</b> is the authentication algorithm. For AH proposal type <b>authentication</b> is either <i>md5</i> or <i>sha1</i> . For ESP, it must be one of the following: <i>none</i> , <i>md5</i> , or <i>sha1</i> .
<b>proposal p2 p2name replay-detection size</b>
Set the anti-replay window size. <b>p2name</b> is a unique string to identify the IPSec Phase 2 Proposal. <b>size</b> is the window size of the replay detection. It must be one of the following: <i>disable</i> , <i>window-32</i> , or <i>window-64</i> .

**Example:**

```
proposal p2 p2esp esp transform 480 1024 aes256 md5
proposal p2 p2ah ah transform 1440 2048 sha1
proposal p2 p2ah replay-detection window-32
```

## rule

**Description:** Configure the rules of the security policy.

**Syntax:**

<b>rule name</b>
<i>name</i> is the policy name on the firewall. Use <code>no rule name</code> to delete rule.

After you enter the command **rule name** the CLI continues to the policy type assignment of the rule.

The prompt changes to "WG(confi g/pol i cy/rul e-*name*)#".

<b>policy-type p-type from source to destination</b>
Select the Policy Type to be applied to the rule. <b>p-type</b> is the policy type. To see the list of policy types you can execute the command <code>show policy-type</code> . <b>source</b> is any or a combination of the following: <ul style="list-style-type: none"> <li>- <i>alias if-alias</i> — <i>if-alias</i> is the interface alias. Must be one of the following: <i>Trusted, Optional, External, Any-Trusted, Any-Optional, or Any-External</i>.</li> <li>- <i>custom-address if-alias address address-format group-user type name authsvr</i>  <ul style="list-style-type: none"> <li>* <b>address-format</b> must be one of the following:  <ul style="list-style-type: none"> <li>* <i>host-ip A.B.C.D</i></li> <li>* <i>host-range A.B.C.D W.X.Y.Z</i></li> <li>* <i>network-ip A.B.C.D/M</i></li> </ul> </li> <li>* <b>type</b> is either: <i>user</i>, or <i>group</i></li> <li>* <b>name</b> is the user name or group name</li> <li>* <b>authsvr</b> is one of the following: <i>Firebox-DB, RADIUS, LDAP, SecurID, or Active-Directory</i></li> </ul> </li> <li>- <i>tunnel-address bovpn</i> — <i>bovpn</i> is the BOVPN name</li> <li>- <i>user-group type name authsvr</i></li> </ul> <b>destination</b> is any or a combination of the following: <ul style="list-style-type: none"> <li>- <i>alias if-alias</i> — <i>if-alias</i> is the interface alias. Must be one of the following: <i>Trusted, Optional, External, Any-Trusted, Any-Optional, or Any-External</i>.</li> <li>- <i>custom-address if-alias address address-format group-user type name authsvr</i>  <ul style="list-style-type: none"> <li>* <b>address-format</b> must be one of the following:  <ul style="list-style-type: none"> <li>* <i>host-ip A.B.C.D</i></li> <li>* <i>host-range A.B.C.D W.X.Y.Z</i></li> <li>* <i>network-ip A.B.C.D/M</i></li> </ul> </li> <li>* <b>type</b> is either: <i>user</i>, or <i>group</i></li> <li>* <b>name</b> is the user name or group name</li> <li>* <b>authsvr</b> is one of the following: <i>Firebox-DB, RADIUS, LDAP, SecurID, or Active-Directory</i></li> </ul> </li> <li>- <i>tunnel-address bovpn</i> — <i>bovpn</i> is the BOVPN name</li> <li>- <i>user-group type name authsvr</i></li> </ul> <b>is-enable</b> denotes if the rule is active or not. Must be either: <i>enable</i> , or <i>disable</i> .

After you enter the command **policy-type p-type from source to destination is-enable** a new range of commands is available to configure the rule details. You must use the **Apply** command before your changes become active.

<b>alarm alarmid trap remote action launch-interval repeat-count block</b>
<p>Configure an alarm for the specified rule.</p> <p><b>name</b> is the name of the rule.</p> <p><b>alarmid</b> is an alarm identification.</p> <p><b>trap</b> enables SNMP trap. The value must be either: <i>0</i> or <i>1</i>.</p> <p><b>remote</b> enable notification. The value must be either: <i>0</i> or <i>1</i>.</p> <p><b>action</b> sets the notification type. It must be either: <i>email</i> or <i>popup</i>.</p> <p><b>launch-interval</b> is the minimum time in minutes between different notifications. It must be an integer from 60 to 3932100.</p> <p><b>repeat-count</b> is the number of times an event can reoccur before an additional alarm is sent. It must be an integer from 1 to 256.</p> <p><b>block</b> enables the automatic addition of the source IP to the blocked site. The value must be either: <i>0</i> or <i>1</i>.</p>
<b>dynamic-nat switch</b>
<p>Enable dynamic NAT for traffic controlled by the specified rule.</p> <p><b>switch</b> must be either:</p> <ul style="list-style-type: none"> <li>- <i>disable</i></li> <li>- <b>enable function</b> — where <b>function</b> is either: <ul style="list-style-type: none"> <li>* <i>network-nat-setting</i></li> <li>* <i>all-traffic-in-policy ip-address</i> — where <b>ip-address</b> is in the format A.B.C.D.</li> </ul> </li> </ul>
<b>firewall action</b>
<p>Set the firewall action for the specified rule.</p> <p><b>action</b> must be one of the following: <i>Allow</i>, <i>Block</i> <b>switch</b>, or <i>Reject</i> <b>rejectaction switch</b></p> <ul style="list-style-type: none"> <li>- <b>switch</b> is either: <i>enable</i>, or <i>disable</i>.</li> <li>- <b>rejectaction</b> must be one of the following: <i>Disabled</i>, <i>ICMP_HOST</i>, <i>ICMP_NETWORK</i>, <i>ICMP_PORT</i>, <i>ICMP_PROTOCOL</i>, or <i>TCP_RST</i></li> </ul>
<b>from source</b>
<p>Edit the source field of an existing policy.</p> <p><b>source</b> is any or a combination of the following:</p> <ul style="list-style-type: none"> <li>- <i>alias if-alias</i> — <b>if-alias</b> is the interface alias. Must be one of the following: <i>Trusted</i>, <i>Optional</i>, <i>External</i>, <i>Any-Trusted</i>, <i>Any-Optional</i>, or <i>Any-External</i>.</li> <li>- <i>custom-address if-alias address address-format group-user type name authsvr</i></li> <li>* <b>address-format</b> must be one of the following: <ul style="list-style-type: none"> <li>* <i>host-ip A.B.C.D</i></li> <li>* <i>host-range A.B.C.D W.X.Y.Z</i></li> <li>* <i>network-ip A.B.C.D/M</i></li> </ul> </li> <li>* <b>type</b> is either: <i>user</i>, or <i>group</i></li> <li>* <b>name</b> is the user name or group name</li> <li>* <b>authsvr</b> is one of the following: <i>Firebox-DB</i>, <i>RADIUS</i>, <i>LDAP</i>, <i>SecurID</i>, or <i>Active-Directory</i></li> <li>- <i>tunnel-address bovpn</i> — <b>bovpn</b> is the BOVPN name</li> <li>- <i>user-group type name authsvr</i></li> </ul>
<b>icmp-message action</b>
<p>Set the traffic action for ICMP messages.</p> <p><b>action</b> must be one of the following: <i>use-global</i>, <i>allow-all</i>, <i>deny-all</i>, or <i>option</i></p> <ul style="list-style-type: none"> <li>- <b>option</b> can be any combination of the following: <i>fragmentation-required</i>, <i>time-exceeded</i>, <i>network-unreachable</i>, <i>host-unreachable</i>, <i>protocol-unreachable</i>, and <i>port-unreachable</i></li> </ul>
<b>idle-timeout length</b>
<p>Set the idle timeout in seconds.</p> <p><b>length</b> is the idle timeout in seconds. It must be an integer from 0 to 2147483647.</p>

<b>ips-monitor</b>
<p>Enable or disable the IPS-Monitor feature of the specified rule.</p> <p><i>No options available.</i></p> <p>Use <code>no ips-monitor</code> to disable the feature.</p>
<b>logging</b>
<p>Enable or disable logging for the specified rule.</p> <p><i>No options available.</i></p> <p>Use <code>no logging</code> to disable the feature.</p>
<b>move location</b>
<p>Move the policy to a numbered location.</p> <p><b>location</b> is the desired location of the policy.</p>
<b>one-to-one-nat switch</b>
<p>Use or not use 1-to-1 NAT on the policy. Default is to use 1-to-1 NAT</p> <p><b>switch</b> is either: <i>0</i> (disable) or <i>1</i> (enable)</p>
<b>policy-routing backup primary-ext failover backup-ext backup-ext</b>
<p>Configure policy-based routing.</p> <p><b>primary-ext</b> is the alias of the primary external interface for the policy.</p> <p><b>backup-ext</b> is the alias of the backup external interface for the policy. More than one backup external interface can be assigned to a policy.</p>
<b>proxy-action action</b>
<p>Assigned a default proxy action to a policy.</p> <p><b>action</b> is the default proxy action on the device. To see the list of proxy actions, you can execute the command <code>show proxy-action</code>.</p>
<b>qos enable</b>
<p>Enable or disable override per interface QoS feature of the specified rule.</p> <p><i>No options available.</i></p> <p>Use <code>no qos enable</code> to disable the feature.</p>
<b>qos marking dscp state priority-method method</b>
<p>Override per interface QoS settings for the traffic controlled by the specified rule.</p> <p><b>state</b> is the DSCP state and must be one of the following values: <b>assign type</b> or <i>preserve</i>.</p> <ul style="list-style-type: none"> <li>- <b>type</b> is the DSCP assign method and must be one of the following values: <i>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.</i></li> </ul> <p><b>method</b> is the method used to assign priority and must be one of the following values: <i>No_Priority, Customer, or Mapped-from-Marking.</i></p>
<b>rule name qos marking precedence state priority-method method</b>
<p>Override per interface QoS precedence for the traffic controlled by the specified rule.</p> <p><b>state</b> is the precedence state and must be one of the following values: <b>assign value</b> or <i>preserve</i>.</p> <ul style="list-style-type: none"> <li>- <b>value</b> is the precedence value. It must be an integer from 0 to 7.</li> </ul> <p><b>method</b> is the method used to assign priority and must be one of the following values: <i>No_Priority, Customer, or Mapped-from-Marking.</i></p>
<b>schedule sked-name</b>
<p>Assign an existing schedule to the policy.</p> <p><b>sked-name</b> is the pre-created schedule.</p>
<b>server-load-balance external method sticky internal-ip weight port</b>

<p>Configure policy-based server load balancing.</p> <p><b>external</b> must be either:</p> <ul style="list-style-type: none"> <li>- <b>ip ipaddr</b> where <b>ipaddress</b> is in the format of A.B.C.D.</li> <li>- <b>address nameexternal</b> where <b>nameexternal</b> is an alias for an external interface</li> </ul> <p><b>method</b> must be either: <i>round-robin</i> or <i>least-connection</i></p> <p><b>sticky</b> is measured in minutes and must be an integer from 0 to 2147483647, 0 means disabled. You can add from 2 to 10 internal servers to a policy. For each, you must configure the following:</p> <ul style="list-style-type: none"> <li>- <b>internal-ip</b> must be an address on the trusted or option network in the format A.B.C.D.</li> <li>- <b>weight</b> is the priority assigned to the specified internalip relative to other servers configured</li> <li>- <b>port</b> is the port number and must be an integer from 0 to 65535</li> </ul>
<p><b>snmp</b></p> <p>Enable or disable sending SNMP trap feature of the specified rule.</p> <p><i>No options available.</i></p> <p>Use <b>no snmp</b> to disable the feature.</p>
<p><b>static-nat external internal port</b></p> <p>Configure the policy to use static NAT.</p> <p><b>external</b> is either:</p> <ul style="list-style-type: none"> <li>- <b>ext-ip address</b> where <b>address</b> is an IP address on the external network in the format A.B.C.D.</li> <li>- <b>ext-addr alias</b> where <b>alias</b> is a name or alias for an external network address</li> </ul> <p><b>internal</b> is an IP address on the internal network in the format A.B.C.D.</p> <p><b>port</b> is the port used to connect and must be an integer from 0 to 65535</p>
<p><b>to destination</b></p> <p>Edit the destination field of an existing policy.</p> <p><b>destination</b> is any or a combination of the following:</p> <ul style="list-style-type: none"> <li>- <i>alias if-alias</i> — <b>if-alias</b> is the interface alias. Must be one of the following: <i>Trusted, Optional, External, Any-Trusted, Any-Optional, or Any-External.</i></li> <li>- <i>custom-address if-alias address address-format group-user type name authsvr</i></li> </ul> <p>* <b>address-format</b> must be one of the following:</p> <ul style="list-style-type: none"> <li>* <i>host-ip</i> <b>A.B.C.D</b></li> <li>* <i>host-range</i> <b>A.B.C.D W.X.Y.Z</b></li> <li>* <i>network-ip</i> <b>A.B.C.D/M</b></li> </ul> <p>* <b>type</b> is either: <i>user</i>, or <i>group</i></p> <p>* <b>name</b> is the user name or group name</p> <p>* <b>authsvr</b> is one of the following: <i>Firebox-DB, RADIUS, LDAP, SecurID, or Active-Directory</i></p> <ul style="list-style-type: none"> <li>- <i>tunnel-address bovpn</i> — <b>bovpn</b> is the BOVPN name</li> <li>- <i>user-group type name authsvr</i></li> </ul>
<p><b>traffic-mgmt tmname</b></p> <p>Assign traffic management to a policy.</p> <p><b>tmname</b> pre-defined traffic management configuration.</p>

**Example:**

```
rule HTTP-proxy-Out
policy-type HTTP-proxy from alias Any-Trusted to alias Any-External enable
logging
schedule releaseweek
snmp
policy-routing backup External-1 failover External-2
```

## schedule

**Description:** Build a schedule for use in policies.

**Syntax:**

**schedule *name* time-block *entry***

***name*** is the name of the schedule.

***entry*** must be entered as follows: ***period starthour startmin endhour endmin***

- ***period*** must be one of the following: *daily, mon, tue, wed, thu, fri, sat, or sun*
- ***starthour*** is the period starting hour, and must be in the range of 0 to 23.
- ***startmin*** is the period starting minute, and must be in the range of 0 to 60.
- ***endhour*** is the period ending hour, and must be in the range of 0 to 23.
- ***endmin*** is the period ending minute, and must be in the range of 0 to 60.

Additional ***entry*** entries can be provided at the end of this command.

**Example:**

```
schedule releaseweek time-block mon 5 30 19 30 tue 5 30 19 30
```

## sslvpn

**Description:** Configure device to allow 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.

**sslvpn external address**

Configure Mobile VPN with SSL to use an external address or domain.

**external** is either: *primary* or *backup*

**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 specified DNS or WINS servers.

**type** is either: *dns* or *wins*

**address** is an IP address in the format A.B.C.D. You can enter up to 2 servers.

Use **no sslvpn type servers address** to remove a DNS or WINS server from the configuration.

**sslvpn dns domain-name domain**

Define the domain name used for SSL VPN.

**domain** is a qualified domain name.

Use **no sslvpn dns domain-name domain** to remove the domain name from the configuration.

**sslvpn resource method**

Define what resources are available to Mobile VPN with SSL users.

**method** must be one of the following:

- **user-route net** where **net** is a subnet address in the format A.B.C.D./#
- *appliance-route* — allow access to 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 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.

<b>sslvpn algorithm <i>type method</i></b>
Select the authentication and encryption methods used to secure SSL VPN connections. <b>type</b> must be either: <i>authentication</i> or <i>encryption</i> If <b>type</b> is <i>authentication</i> , <b>method</b> must be one of the following: <i>MD5</i> , <i>SHA-old</i> , <i>SHA-1</i> , <i>SHA256</i> , or <i>SHA512</i> . The default method is MD5. If <b>type</b> is <i>encryption</i> , <b>method</b> must be one of the following: <i>Blowfish</i> , <i>DES</i> , <i>3DES</i> , <i>AES-128</i> , <i>AES-192</i> , or <i>AES-256</i> . The default method is Blowfish.
<b>sslvpn auth-server <i>authentication</i></b>
Select a method to authenticate Mobile VPN with SSL users. The authentication method selected must already be configured for the device. <b>authentication</b> must be one of the following: <i>Firebox-DB</i> , <i>RADIUS</i> , <i>SecurID</i> , <i>LDAP</i> , or <i>Active-Directory</i> If <b>authentication</b> is either <i>RADIUS</i> or <i>SecurID</i> you can use the optional command <i>force</i> to force users to reauthenticate after a connection is lost.
<b>sslvpn keepalive <i>setting value</i></b>
Configure SSL VPN keep-alive settings. <b>setting</b> must be either: <i>interval</i> or <i>timeout</i> <b>value</b> is measured in seconds and must be an integer <ul style="list-style-type: none"> <li>- The default value for the keep-alive interval is 10.</li> <li>- The default value for the keep-alive timeout is 60.</li> </ul>
<b>sslvpn protocol <i>prot port</i></b>
Change the protocol and port used for Mobile VPN with SSL. <b>prot</b> must be either: <i>TCP</i> or <i>UDP</i> . The default is TCP. <b>port</b> must be an integer from 0 to 65535. The default is 443.
<b>sslvpn renegotiate <i>interval</i></b>
Set the amount of time measured in minutes for an active connection before the device forces a renegotiation of the tunnel. <b>interval</b> must be an integer greater than 60. The default value is 60.

**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 keepalive timeout 30
sslvpn renegotiate 90
```

## traffic-management

**Description:** Configure a traffic management action for use with policies.

**Syntax:**

<b>traffic-management <i>name configuration</i></b>
<p><b><i>name</i></b> is a string uniquely identifying the traffic action.  <b><i>configuration</i></b> is in the format: <b><i>interface minimum maximum</i></b></p> <ul style="list-style-type: none"> <li>- <b><i>interface</i></b> is an integer from 0 to 7</li> <li>- <b><i>minimum</i></b> is measured in Kbps and must be an integer from 0 to 1000000</li> <li>- <b><i>maximum</i></b> is measured in Kbps and must be an integer from 0 to 1000000</li> </ul> <p>You can enter <b><i>configuration</i></b> for up to the number interfaces on the device.</p>

## user-group

**Description:** Define a user group for Firebox authentication.

**Syntax:**

<b>user-group <i>name description desc membership user</i></b>
<p><b><i>name</i></b> is the name of the user group  <b><i>desc</i></b> is a short description of the purpose of the group  <b><i>user</i></b> is a user name already configured on the device???</p> <ul style="list-style-type: none"> <li>- You can add more than one user</li> </ul>

**Example:**

```
user-group accounting description Finance_and_Accounting_Dept membership
jackn gloriap cindyk karentc
```

## users

**Description:** Define a user for Firebox authentication.

**Syntax:**

<b>users <i>name passphrase session-timeout idle-timeout group groupname description desc</i></b>
<p><b><i>name</i></b> is a string that uniquely identifies the user  <b><i>passphrase</i></b> is the unencrypted client password  <b><i>session-timeout</i></b> is the duration in hours before a session times out. It must be an integer. The default value is 8.  <b><i>idle-timeout</i></b> is the duration in minutes before an idle session times out. It must be an integer. The default value is 30.  <b><i>groupname</i></b> is a Firebox authentication user group  <b><i>desc</i></b> is a brief description of the user</p>

**Example:**

```
users jackp somethingeasy 24 60 group executives description Jack_Parase_CEO
```

# Index

---

## Symbols

? 5, 7, 16, 17

## A

Active Directory  
  configure server 63  
  groups used as alias 61  
address pool  
  used for DHCP 45, 53  
  used for PPTP 75  
  used for SSL VPN 80  
admin  
  connecting to the device as 4  
  prompt 13  
administrator accounts 4  
adware 47  
alarm  
  configure for rule 77  
  send to remote log server 40  
  traffic from blocked site 39  
  traffic to blocked port 38  
alias  
  **alias** 19, 61, 62  
  assign to interface 55  
  create and modify 61  
  show interface aliases 19  
  use for authentication 62  
allowed site  
  add or remove address 38  
  import list 26  
  show IP settings for 18  
ambiguous command 8  
antivirus 46  
**apply** 62  
ARP  
  **arp flush** 23  
  flush table 23  
  show table 17

authentication  
  **auth-server** 63  
  **auth-user-group** 64  
  configure aliases for 62  
  configure server 63  
  configure user groups 64  
  Firebox users *See* users  
  show global settings 19  
  used for SSL VPN 81  
  user groups *See* user groups

## B

**backup image** 23  
blocked port  
  log messages 38  
  show IP settings for 18  
  specify port(s) 38  
blocked site  
  configure 38, 39  
  export to file 2  
  import list 26  
  set duration 38, 39  
  show settings 18  
BOVPN  
  gateway  
    **bovpn-gateway** 64  
    force rekey 28  
    show settings 19  
  tunnel  
    **bovpn-tunnel** 66  
    create alias 61  
    create or modify 66  
    show settings  
**bovpn-tunnel** *See* BOVPN  
branch office *See* BOVPN  
bridge  
  assign name 33, 47  
  **bridge** 19  
  enable mode  
  show settings 19

bulk license 26

## C

certificates

- cert-request** 23
- import from file 26
- import from Management Server 41
- issue certificate 23
- show available 19
- use device to issue 23

change passwords 26

**checksum** 24

CLI

- debugging 24
- entering commands 4
- exiting 16
- getting help 5
- prompt 13
- starting 2

clock

- change time 24
- clock** 17, 24
- show settings 17

cluster 24, 25

command mode 11

Common commands

- introduction 13, 15
- list of commands 15
- reference 16

configuration

- import from file 26
- restore from prior 27
- update 62

Configuration command mode

- accessing 32
- introduction 12, 31
- list of commands 32
- reference 32

connect 2

Console port 2

contact 47

## D

dangerous activity 33, 34, 36

DDNS *See* dynamic DNS

DDoS 36

debugging

- CLI 24
- configure type and level 40
- debug-cli** 24
- send messages to remote server 40

default packet handling

- configure 36, 53
- configure logging 33, 36
- dangerous activity 33, 34, 36
- DDoS 36
- default-packet-handling** 17, 36, 53
- show settings 17
- unhandled 33, 34, 36

default password 4

device name 47

DHCP

- dchp** 52
- enable as relay 44, 52
- enable as server 44, 52

**diagnose** 24, 25

diagnostic information 24, 25

dialer 47

Diffie-Helman 64

DNS

- add or remove server 33, 34, 35, 39
- set domain name 39
- used for authentication server 63
- used for DHCP server 44, 52
- used for SSL VPN 80

DNS lookup 22

domain name

- used for BOVPN 65
- used for certificate request 23
- used for dynamicDNS 35
- used for SSL VPN 80

downloader 47

drop-in mode

duplex 54

dynamic DNS

- configure device for 35
- show settings 19

dynamic NAT

- configure 69
- dynamic-nat** 69
- enable in rule 77

dynamic routing

- set protocol 39
- show settings 17, 18

## E

engine 46

enter commands 4

error messages 8

e-Series 1

event messages

- enable logging 40
- send to remote server 40

execution error 8

**exit** 16

export

- export** 2, 25
- files from device 8

External interface 57

## F

factory default

- restore to 27
- show 17

FastEthernet 38

feature keys

- features** 17

- import from file 26
- show 19
- show active features 17
- synchronize between devices

fingerprint 19

Firebox authentication 64

firewall action 77

flash disk *See* backup image

friendly name 47

FTP files 8

## G

gateway *See* BOVPN

GAV signatures 17

global settings

- device properties 47
- disable for specified rule 76
- enable VPN 48
- override QoS by rule 78
- show authentication 19
- show for device 19
- show VPN 18

groups *See* user groups

## H

**help** 5, 16

- ? 7
- syntax 5

hijacker 47

**history** 2, 17

## I

ICMP

- icmp** 77
- set traffic action 77
- show settings 18

idle timeout

- set for rule 77

IKE gateway 66

IKE packet trace

- show log settings 18

import

- bulk license 26
- files to device 8
- import** 26
- route configuration 26

incomplete command 8

interface

- configure address 54
- configure options 54
- configure secondary network 56
- configure speed and duplex 54
- create alias 61
- interface** 37
- MAC address binding 54
- multi-WAN probe 44
- name** 55

- set multi-WAN sequence 43

Interface command mode

- accessing 37, 52
- interface** 37
- introduction 12, 51, 59
- list of commands 52
- reference 52

Internet Protocol settings 18, 38

intrusion prevention 17, 36, 53

**ip** 38, 54

IPS signatures 17, 46

IPSec pass through 48

## K

keep alive

- for SSL VPN 81

## L

LDAP

- configure server 63

licenses *See* feature keys

**link-speed** 54

load balancing

- by policy 79
- sequence for multi-WAN 43
- set sequence for multi-WAN 43

local gateway 64

location 47

log messages

- blocked ports 38
- default packet handling 33, 36
- enable by category 40
- send to remote server 40

log server

- configure 40
- show settings 18

log settings

- internal storage 18
- log-cache** 18
- log-settings** 18, 40, 41, 48
- show settings 18

logged in users 17, 29

logging *See* log settings

## M

MAC address binding

- configure 54
- mac-ip-binding** 54
- show settings 17

Main command mode

- accessing 22
- introduction 12, 21
- list of commands 22
- reference 23

managed client

- configure secondary server 41
- enable device 41

- import certificate 41
- managed-client 17
- set primary server 41
- show settings 17
- Management Server 41
- mode *See network mode.*
- mtu** 55
- multi-WAN
  - load balance failover 43
  - method to check status 44
  - show settings 17
- MVPN
  - configure with IPSec 69, 72
  - mvpn-ipsec** 69, 72
  - show group IPSec group configuration 19

## N

- name** *See interface* 55
- NAT
  - one to one 74
  - static NAT 79
- network
  - configure secondary 56
  - create alias 61
- network mode
  - mode**
  - network-mode** 17
  - show settings 17
- notation 1
- NTP
  - configure 45
  - ntp** 45
  - show settings 17

## O

- one-to-one-nat** 74
- operating system 28
- Optional interface 2, 57

## P

- password** 26
- performance statistics
  - enable collection 40
  - show settings 18
- ping** 26
- policy** 45
- Policy command mode
  - accessing 45, 60
  - introduction 12
  - list of commands 60
  - policy** 45
  - reference 61
- policy *See rule* 76
- policy template
  - create custom 74, 75
  - policy-type** 74, 75
  - show settings 19

- policy-type** *See policy template*
- PPTP
  - configure address pool 75
  - configure firewall to allow 75
  - pptp** 75
  - show settings 17
- prompt 13
  - (WG(config)/ife-eth0)# 13
  - WG# 4, 13, 22
  - WG(Config)# 13
  - WG(config/policy)# 13
  - WG> 4, 22

## Q

- QoS
  - configure 56
  - override for rule 78
  - override marking by rule 78
  - qos** 56
- quit 16

## R

- RADIUS
  - configure primary server 63
  - use for tunnel authentication 61
- read only 4, 13, 22
- read write 4, 13, 22
- read-only password 26
- read-write password 26
- reboot** 27
- reference
  - common commands 16
  - Configuration command mode 32
  - Interface command mode 52
  - Main command mode 23
  - Policy command mode 61
- rekey BOVPN gateway 28
- remote gateway 64
- restart *See reboot*
- restore** 27
- round robin 43
- route
  - create static 39
  - import from file 26
  - show settings 17, 18
  - traceroute 28
- routed mode
- rule
  - configure 76
  - configure alarm 77
  - configure firewall action 77
  - enable 76
  - enable dynamic NAT 77
  - enable features 78, 79
  - override QoS by rule 78
  - rule** 19, 76
  - set idle timeout 77
  - show specification 19
  - use policy-based load balancing 79

use static NAT 79

## S

saving changes 62

schedule

configure 80

**schedule** 19, 80

show settings 19

secondary network

configure 56

**secondary** 56

SecurID

configure primary server 63

serial cable 2

server load balancing *See* load balancing

set network mode

**show**

**alias** 19

**arp** 17

**auth-setting** 19

**bovpn-gateway** 19

**bridge** 19

**certificate** 19

**certificate fingerprint** 19

**clock** 17

component 17

**ddns**

**default-packet-handling** 17

**factory-default** 17

**feature-key** 19

**features** 17

**global-settings** 19

**ip** 18

**login-user** 17

**log-settings** 18

**managed-client** 17

**multi-wan** 17

**mvpn-ipsec** 19

**network-mode** 17

**ntp** 17

**policy-type** 19

**pptp** 17

**route** 17

**rule** 19

**schedule** 19

**signature-update** 17

**snmp** 17

**sslvpn** 17

**status-report** 17

**sysinfo** 17

**traffic-management** 19

**update-history** 20

**upgrade** 17

**user-group**

**users**

**shutdown** 27

signature update

configure 46

show last date 17

**signature update** 46

**signature-update** 17

single sign on

show settings 19

SNMP

configure device for 46

enable trap for rule 77

show settings 17

**snmp** 17, 46

speed 54

spyware

configure 47

**spyware** 47

SSL VPN

configure 80

show settings 17

**sslvpn** 80

start CLI 2

static NAT 79

status

connecting to the device as 4

prompt 13

status report 17

support messages

enable collection of 40

send to remote server 40

**sync**

syntax 1

error 8

help command 5

reference format 1

reference notation 1

sys-b 28

system

display network mode 17

set network mode

**system** 47

system information

configure properties 47

show settings 17, 28

**sysinfo** 17, 28

## T

TCP

show settings 18

**tcpdump** 28

TCP/IP 2

terminal client 4

terminal commands 4

TFTP files 8

time *See* clock

timestamp 45

timezone

configure 47

**traceroute** 28

trackware 47

traffic management

configure action 82

show action 19

**traffic-management** 19, 82

traffic messages

send to remote server 40

show log settings 18

transform 64

Trusted interface 2, 57

**type** 57

---

Type of Service 48

## U

unhandled packets 33, 34, 36

unrecognized command 8

update

configuration 62

GAV signatures 20

IPS signatures 20

IPS/AV engine 46

signatures 17, 46

**update-history** 20

upgrade

from image 28

show audit trail 17

**upgrade** 28

user groups

configure for authentication 64

create alias 61

show settings 19

**user-group** 82

users

define for Firebox authentication 82

logged in 17

show users 19

**users** 19

## V

VLAN *See* bridge

VPN

enable global settings 48

show global settings 18

**vpn-setting** 18, 48

**vpn-tunnel** 28

## W

WG# 4, 13, 22

WG(confi g)# 13, 32

WG(confi g/i fe-eth0)# 13, 38, 46, 52

WG(confi g/pol i cy)# 13, 60

WG> 4, 13, 22

**who** 29

WINS

configure servers 39

show IP settings for 18

show settings 18

used for authentication 63

used for DHCP 44, 52

used for SSL VPN 80

## X

XTM 1



---

**ADDRESS:**

505 Fifth Avenue South  
Suite 500  
Seattle, WA 98104

**SUPPORT:**

[www.watchguard.com/support](http://www.watchguard.com/support)  
[support@watchguard.com](mailto:support@watchguard.com)  
U.S. and Canada +877.232.3531  
All Other Countries +1.206.613.0456

**SALES:**

U.S. and Canada +1.800.734.9905  
All Other Countries +1.206.521.8340

**ABOUT WATCHGUARD**

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. All products are backed by LiveSecurity® Service, a ground-breaking support and maintenance program. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please call 206.613.6600 or visit [www.watchguard.com](http://www.watchguard.com).