Check Point Embedded NGX

Internet Security Appliance

CLI Reference Guide

Version 8.2

Part No: 700797, November 2010

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

PREAMBLE

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with

modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

To receive the SofaWare GPL licensed code, contact info@sofaware.com.

SAFETY PRECAUTIONS

Carefully read the Safety Instructions the Installation and Operating Procedures provided in this User's Guide before attempting to install or operate the appliance. Failure to follow these instructions may result in damage to equipment and/or personal injuries.

- Before cleaning the appliance, unplug the power cord. Use only a soft cloth dampened with water for cleaning.
- When installing the appliance, ensure that the vents are not blocked.
- Do not place this product on an unstable surface or support. The product may fall, causing serious injury to a child or adult, as well as serious damage to the product.
- Do not use the appliance outdoors.
- Do not expose the appliance to liquid or moisture.
- Do not expose the appliance to extreme high or low temperatures.

- Do not disassemble or open the appliance. Failure to comply will void the warranty.
- Do not use any accessories other than those approved by Check Point. Failure to do so may result in loss of performance, damage to the product, fire, electric shock or injury, and will void the warranty.
- Route power adapter cords where they are not likely to be walked on or pinched by items placed on or against them. Pay particular attention to cords where they are attached to plugs and convenience receptacles, and examine the point where they exit the unit.
- Do not connect or disconnect power adapter cables and data transmission lines during thunderstorms.
- Do not overload wall outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard. Periodically examine the cord, and if its appearance indicates damage or deteriorated insulation, have it replaced by your service technician.
- If the unit or any part of it is damaged, disconnect the power plug and inform the responsible service personnel. Non-observance may result in damage to the router.

POWER ADAPTER

- Operate this product only from the type of power source indicated on the product's marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Use only the power adapter provided with your product. Check whether the device's set supply voltage is the same as the local supply voltage.
- To reduce risk of damage to the unit, remove it from the outlet by holding the power adapter rather than the cord.

SECURITY DISCLAIMER

The appliance provides your network with the highest level of security. However, no single security product can provide you with absolute protection. We recommend using additional security measures to secure highly valuable or sensitive information.

Contents

Chapter 1

Introduction

This chapter introduces the Check Point Embedded NGX appliance and this guide.

This chapter includes the following topics:

About Your Check Point Embedded NGX Appliance

The Check Point Embedded NGX appliance is an advanced Internet security appliance that enables secure high-speed Internet access from the office. Developed by SofaWare Technologies, an affiliate of Check Point Software Technologies, the worldwide leader in securing the Internet, the Embedded NGX family includes Safe@Office and UTM-1 appliances. The Embedded NGX firewall, based on the world-leading Check Point Embedded NGX Stateful Inspection technology, inspects and filters all incoming and outgoing traffic, blocking all unauthorized traffic.

Using This Reference

This reference guide explains how to use CLI commands to control your Embedded NGX appliance.

In the chapter ***CLI Commands*** on page 17, the CLI commands are divided into groups, according to their purpose. The commands are presented in alphabetical order within those groups.

Several CLI commands have CLI variables as their parameters. These CLI variables function as sub-commands and may have multiple fields.

This guide presents CLI variables in a separate chapter, ***CLI Variables*** on page 227. Like CLI commands, the CLI variables appear in alphabetical order. However, the variables are

not divided into groups, because a single variable may be used by more than one group of commands.

The following information is provided for each CLI command or variable:

Purpose	Describes the command or variable's purpose and provides background information
Effect	Describes the effect of running the command. Relevant for Appliance Operation commands only.
Syntax	The format of the command
Parameters	Describes the command's parameters, if there are any. Relevant for commands only.
Fields	Describes the variable's fields, if there are any. Relevant for variables only.
Return Values	The values returned in the command line interface. This information is provided only when running the command results in return values other than the typical values, for example when you run Informational commands. For information on the typical return values, see ***Typical Return Values*** on page 15. For information on Informational commands, see ***Informational Commands*** on page 65.
Examples	One or more examples that illustrate the command or variable's usage

Note: The information in this guide is relevant for both Safe@Office and UTM-1 appliances. For information on specific Embedded NGX appliance models, refer to your Embedded NGX appliance's User Guide (see ***Related Publications*** on page *3*).

Document Conventions and Syntax

To make finding information in this manual easier, some types of information are marked with special symbols or formatting.

Boldface type is used for button names.

Note: Notes are denoted by indented text and preceded by the Note icon.

Warning: Warnings are denoted by indented text and preceded by the Warning icon.

CLI commands and variables appear in `Courier` style:

`command`

CLI command syntax is presented in the following format:

command *mandatory-parameter* [*optional-parameter*]

CLI variable syntax is presented in the following format:

variable *mandatory-field* [*optional-field*]

Examples appear in `Courier` style in boxes:

```
This is an example of a CLI command.
```

Related Publications

Use this guide in conjunction with the User Guide provided with your appliance:

- *Check Point Safe@Office User Guide*

  Or

- *Check Point UTM-1 Embedded NGX User Guide*

Chapter 2

Using the Serial Console

You can connect a console to the Embedded NGX appliance, and use the console to control the appliance via the command line.

Note: Your terminal emulation software and your Embedded NGX appliance's Serial port must be configured for the same speed.

By default, the appliance's Serial port's speed is 57600 bps. For information on changing the Serial port's speed, see ***port serial*** on page 509.

To run commands using a console

1. Connect the serial console to your Embedded NGX appliance's Serial port, using an RS-232 Null modem cable.
2. Log in to the Embedded NGX Portal.

   For instructions, refer to the User Guide.
3. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.
4. Next to the Serial port, click Edit.

   The Port Setup page appears.
5. In the Assign to drop-down list, select Console.
6. Click Apply.

   You can now control the Embedded NGX appliance from the serial console.

Chapter 3

Using the Embedded NGX Command Line Interface

This chapter explains how to use the command line interface to run a CLI command and provides a list of typical return values.

This chapter includes the following topics:

General Guidelines

When running commands in the Embedded NGX appliance, follow these guidelines:

- Embedded NGX CLI commands, variables, and fields are case-sensitive.
- It is not necessary to type a command or variable in its entirety; it is sufficient to type the shortest string that is unique to the command or variable.

  For example, instead of typing:

```
delete netobj 3
```

  You can type:

```
del neto 3
```

  You cannot abbreviate `netobj` to `net`, because these letters are not unique to `netobj`.

- If a command or variable is composed of multiple words, you may only abbreviate the final word.

For example, instead of typing:

```
show qos classes 1
```

You can abbreviate the final word in the variable `qos classes`:

```
show qos cl 1
```

You cannot abbreviate `qos classes` to `qos`.

- Do not enclose commands, variables, or field names in quotation marks.
- Occasionally, a field's value will be a string containing one or more spaces. In this case, enclose the string in quotation marks.

  For example:

```
set dialup type "Hayes Accura 56K"
```

Tip: If you are unsure how to configure a particular setting via the command line, you can configure it in the Embedded NGX Portal tab, export the Embedded NGX appliance settings, and then examine the exported settings to find out how the CLI command for the desired setting looks.
For information on exporting settings via the command line, see ***export*** on page *74*.

Command Line Editing

When using SSH or Serial Console:

- You can press the TAB key to either complete the current command, or show a list of possible completions.

Note: CLI commands that are not supported by your hardware type and license are not displayed as possible command completions.

- All commands entered during a CLI session are saved in a command history. You can browse through the command history by using the UP and DOWN arrow keys.

Running Commands

Depending on your Embedded NGX model, you can control your appliance via the command line in the following ways:

- Using the Embedded NGX Portal's command line interface.

  See ***Using the Embedded NGX Portal*** on page 9.

- Using a console connected to the Embedded NGX appliance.

  For information, see ***Using the Serial Console*** on page 5.

- Using an SSH client.

  See ***Using SSH*** on page 10.

- Importing CLI scripts

  See ***Importing CLI Scripts*** on page 11.

- Sending CLI commands via text messages from your cellular phone

  See ***Sending CLI Commands via Text Messages*** on page 12.

Using the Embedded NGX Portal

You can run commands using the Embedded NGX Portal.

To run commands using the Embedded NGX Portal

1. Log in to the Embedded NGX Portal.

   For instructions, refer to the User Guide.

2. Click Setup in the main menu, and click the Tools tab.

   The Tools page appears.

3. Click Command.

   The Command Line page appears.

4. In the upper field, type a command.

5. Click Go.

   The command is implemented.

Return values appear in the lower field.

Using SSH

Embedded NGX users can control the appliance via the command line, using the SSH (Secure Shell) management protocol.

By default, SSH access is allowed only from the internal networks. You can allow SSH access via the Internet, by configuring remote SSH access.

Note: The Embedded NGX appliance supports SSHv2 clients only. The SSHv1 protocol contains security vulnerabilities and is not supported.

To enable SSH access from the Internet

1. Log on to the Embedded NGX Portal.

   For instructions, refer to the User Guide.

2. Click Setup in the main menu, and click the Management tab.

   The Management page appears.

3. Specify from where SSH access should be granted.

   See ***Access Options*** on page 11 for information.

Warning: If remote SSH is enabled, your Embedded NGX appliance settings can be changed remotely, so it is especially important to make sure all Embedded NGX appliance users' passwords are difficult to guess.

   If you selected IP Address Range, additional fields appear.

4. If you selected IP Address Range, enter the desired IP address range in the fields provided.

5. Click Apply.

   You can now control the Embedded NGX appliance using an SSHv2 client.

Note: If you need to enable SSH access from multiple IP address ranges, you can do so by creating a firewall rule for each range, in which the specified service is SSH, the connection source is the desired IP address range, and the connection destination is "This Gateway". For instructions, refer to the User Guide.

Table 1: Access Options

Select this option…	To allow access from…
Internal Network	The internal network only. This disables remote access capability. This is the default.
Internal Network and VPN	The internal network and your VPN.
IP Address Range	A particular range of IP addresses. Additional fields appear, in which you can enter the desired IP address range.
ANY	Any IP address.

Importing CLI Scripts

All Embedded NGX models enable you to import CLI scripts to the appliance.

To import CLI scripts

1. Do one of the following:
   - Write a CLI script in a text file with the extension *.cfg.
   - Edit an exported Embedded NGX configuration file.
     For information on exporting configuration files, refer to the User Guide.
2. Log on to the Embedded NGX Portal.
   For instructions, refer to the User Guide.
3. Click Setup in the main menu, and click the Tools tab.
   The Tools page appears.
4. Click Import.
   The Import Settings page appears.

5. Do one of the following:
   - In the Import Settings field, type the full path to the configuration file.

   Or

   - Click Browse, and browse to the configuration file.
6. Click Upload.

   A confirmation message appears.
7. Click OK.

   The Embedded NGX appliance settings are imported.

   The Import Settings page displays the configuration file's content and the result of implementing each configuration command.

Note: If the appliance's IP address changed as a result of the configuration import, your computer may be disconnected from the network; therefore you may not be able to see the results.

Sending CLI Commands via Text Messages

If the Embedded NGX has a USB modem attached, you can run CLI commands by sending text messages from your cellular phone.

To send commands via text messages

1. Connect a USB-based modem to one of your Embedded NGX appliance's USB ports.

   For information on locating the USB ports, refer to the User Guide.

Warning: Before attaching a USB modem, ensure that the total power drawn by all connected USB devices does not exceed 2.5W per port (0.5A at 5V). If the total current consumed by a port exceeds 0.5A, a powered USB hub must be used, to avoid damage to the gateway.

Note: In order to allow data calls and receiving text messages simultaneously, the modem must have two serial lines with AT command support. Alternatively, you can connect a dedicated modem for receiving text messages only. In this case, an active connection is not required.

2. Click Network in the main menu, and click the Ports tab.

The Ports page appears.

3. Next to USB, click Edit.

   The USB Devices page appears. If the Embedded NGX appliance detected the modem, the modem is listed on the page.

   If the modem is not listed, check that you connected the modem correctly, then click Refresh to refresh the page.

4. Next to the modem, click Edit.

   The USB Modem Setup page appears.

5. Complete the fields using the information in the following table.

6. Click Apply.

7. To check that the values you entered are correct, click Test.

   The page displays a message indicating whether the test succeeded.

8. Configure a Dialup Internet connection on the Cellular Modem port.

   For information, refer to the User Guide.

9. In the Embedded NGX Portal, configure remote CLI access settings, using the following commands:

   - `set remote-cli` - Enables and configures remote CLI access
   - `set remote-cli white-list` - Configures a white list of phone numbers from which the modem should receive remote CLI commands via text messages

   For information on using the Embedded NGX Portal to run commands, see ***Using the Embedded NGX Portal*** on page 9. For information on the relevant attributes for these commands, see ***remote-cli*** on page 530 and ***remote-cli white-list*** on page 532.

10. From your cellular phone, send text messages to the modem in the following format:

    #shared-secret#CLI-command

    Where:

    - *shared-secret* is the shared secret you configured in the `set remote-cli` command.

- *CLI-command* is the CLI command you want to run, written on a single line.

Notes:

- The maximum length of a SMS text message is 140 bytes. CLI commands longer than 140 bytes are not supported.
- Text messages sent in non-English character sets will be ignored.
- If the command line contains characters that are not valid CLI characters, then all commands will be ignored.

Table 2: USB Dialup Fields

In this field...	Do this...
Modem Type	Select the modem type. You can select one of the predefined modem types or Custom. If you selected Custom, the Installation String field is enabled. Otherwise, it is filled in with the correct installation string for the modem type.
Initialization String	Type the installation string for the custom modem type. If you selected a standard modem type, this field is read-only.
Dial Mode	Select the dial mode the modem uses.
Port Speed	Select the modem's port speed (in bits per second).
Answer incoming PPP calls	Select this option to specify that the modem should answer incoming PPP calls. This allows accessing the appliance out of band for maintenance purposes, in case the primary Internet connection fails. The client is assigned an IP address from the OfficeMode network; therefore, the OfficeMode network must be enabled. For information on enabling the OfficeMode network, refer to the User Guide.

In this field...	Do this...
Cellular	
APN	Type your Access Point Name (APN) as given by your cellular provider. If your cellular provider has not provided you with an APN, leave this field empty.
PIN	Type the Personal Identification Number (PIN) code that you received with your cellular SIM card, if required by your modem. The PIN code is usually 4 digits long. Warning: Entering an incorrect PIN code may cause your SIM card to be blocked.

Typical Return Values

When you run a command whose purpose is to display information, the return value is the information. For example, if you run the command `info fw`, then the command line interface returns information about the firewall. These return values are described after each relevant command and variable in this guide.

When you run a command whose purpose is not informational, the command line interface typically returns one of the values listed in the table below.

Table 3: Typical Return Values

Value	Explanation
`OK`	The command was implemented successfully.
`Failed`	The command failed.
`item {deleted | added | cleared}`	The add / delete / clear command was implemented successfully.

Value	Explanation
`item cannot be {deleted | added | cleared}`	The add / delete / clear command failed.
`Possible completions <list of possible completions>`	The command you entered is not complete, because a variable or a field is missing. Use the list provided to complete the command, and then run the command again.
`Missing value for property name`	The command you entered is not complete, because a field's value is missing. Complete the command, and then run the command again.
`Syntax error <error>`	The syntax of the command you entered is incorrect. The erroneous syntax is displayed.
`Invalid index`	The command you entered relates to a table in an incorrect way. For example, in the case of `delete device`, the command applies only to tables, and the variable is not a type of table.

Chapter 4

CLI Commands

This chapter provides a list of CLI commands for controlling your Embedded NGX appliance. The CLI commands are divided into the following groups:

- Variable Operation Commands. CLI commands for working with variables
- Appliance Operation Commands. CLI commands for managing the Embedded NGX appliance
- Informational Commands. CLI commands for displaying information about your Embedded NGX appliance, its settings

Several CLI commands use CLI variables. For information on CLI variables, see ***CLI Variables*** on page 227.

This chapter includes the following topics:

Variable Operation Commands

The commands in this section enable you to perform the following actions on variables:

- Add a variable to a table
- Delete a variable from a table
- Modify a variable
- Display a variable's settings
- Display a table of variables
- Clear a table of variables

For information on CLI variables, see ***CLI Variables*** on page 227.

add

PURPOSE

The add command is used for adding new variables to a table. Use this command to add any of the following:

- Access lists
- Access list rules
- BGP neighbors
- BGP networks
- Bridges
- A self-signed certificate
- DHCP scopes
- Firewall rules
- NAT rules
- Network objects
- Network service objects
- OSPF areas
- OSPF networks
- QoS classes
- RADIUS servers
- RIP networks
- Static routes
- SmartDefense CIFS worm patterns
- SmartDefense blocked and allowed FTP commands
- SmartDefense HTTP header patterns
- SmartDefense HTTP-based worm patterns
- SmartDefense SCADA Modbus commands

- Users
- VLAN networks / Virtual Access Points (VAPs) / Wireless Distribution System (WDS) links
- IP address ranges in the VPN internal encryption domain
- VPN sites
- VStream Antispam blocked senders
- VStream Antispam safe senders
- VStream Antivirus policy rules
- Web rules

SYNTAX

add *variable*

PARAMETERS

`variable`	String. The type of variable you want to add. This can be any of the following: • `access-list` - An access list • `access-list-rule` - An access list rule • `antispam blocked-senders list` - A VStream Antispam blocked sender • `antispam safe-senders list` - A VStream Antispam safe sender • `bgp neighbor` - A BGP neighbor • `bgp network` - A BGP network • `bridges` - A bridge • `certificate` - A self-signed certificate • `dhcp scopes` - A DHCP scope • `fw rules` - A firewall rule • `nat rules` - A NAT rule • `netobj` - A network object • `ospf area` - An OSPF area

- `ospf network` - An OSPF network
- `qos classes` - A QoS class
- `radius servers` - A RADIUS server
- `rip network` - A RIP network
- `routes` - A static route
- `smartdefense ai cifs file-sharing patterns` - A CIFS worm pattern that SmartDefense should detect
- `smartdefense ai ftp commands` - An FTP command that SmartDefense should allow or block
- `smartdefense ai http header-rejection patterns` - An HTTP header pattern that SmartDefense should detect
- `smartdefense ai http worm-catcher patterns` - An HTTP-based worm pattern that SmartDefense should detect
- `smartdefense ai scada modbus` - A SCADA Modbus command that SmartDefense should allow
- `svc-objects` - A network service object
- `users` - A Embedded NGX Portal user
- `vlan` - A VLAN network, VAP, or WDS link
- `vpn internal-encryption-domain ranges` - An IP address range that should be included in the VPN internal encryption domain
- `vpn sites` - A VPN site
- `vstream policy rules` - A VStream Antivirus policy rule
- `webfilter rule` - A Web rule

For information on these variables and how to use them with the `add` command, see ***CLI Variables*** on page 227.

RETURN VALUES

See ***Typical Return Values*** on page 15.

EXAMPLE

The following command adds the user JohnSmith and assigns him the password JohnS1.

```
add users name JohnSmith password JohnS1
```

clear

PURPOSE

The `clear` command is used for deleting all the variables in a table. Use this command to clear any of the following:

- Access lists
- Access list rules
- BGP neighbors
- BGP networks
- Bridges
- A certificate
- DHCP scopes
- Firewall rules
- NAT rules
- Network objects
- Network service objects
- OSPF areas
- OSPF networks
- QoS classes
- RADIUS servers
- RIP networks
- Static routes
- SmartDefense CIFS worm patterns
- SmartDefense blocked and allowed FTP commands
- SmartDefense HTTP header patterns
- SmartDefense HTTP-based worm patterns
- SmartDefense SCADA Modbus commands

- Users
- VLAN networks / Virtual Access Points (VAPs) / Wireless Distribution System (WDS) links
- IP address ranges in the VPN internal encryption domain
- VPN sites
- VStream Antispam blocked senders
- VStream Antispam safe senders
- VStream Antivirus policy rules
- Web rules

Note: You cannot delete the following:

- The admin user (user 1)
- The Default QoS class (QoS class 1)
- Implicitly defined NAT rules. For information on NAT rules, see ***nat rules*** on page 362.

SYNTAX

clear *variable*

PARAMETERS

`variable`	String. The type of variables in the table you want to clear. This can be any of the following: • `access-list` - Access lists • `access-list-rule` - Access list rules • `antispam blocked-senders list` - VStream Antispam blocked senders • `antispam safe-senders list` - VStream Antispam safe senders • `bgp neighbor` - BGP neighbors • `bgp network` - BGP networks • `bridges` - Bridges • `certificate` - A certificate

- `dhcp scopes` - DHCP scopes
- `fw rules` - Firewall rules
- `nat rules` - NAT rules
- `netobj` - Network objects
- `ospf area` - OSPF areas
- `ospf network` - OSPF networks
- `qos classes` - QoS classes
- `radius servers` - RADIUS servers
- `rip network` - RIP networks
- `routes` - Static routes
- `smartdefense ai cifs file-sharing patterns` - CIFS worm patterns that SmartDefense should detect
- `smartdefense ai ftp commands` - FTP commands that SmartDefense should allow or block
- `smartdefense ai http header-rejection patterns` - HTTP header patterns that SmartDefense should detect
- `smartdefense ai http worm-catcher patterns` - HTTP-based worm patterns that SmartDefense should detect
- `smartdefense ai scada modbus` - SCADA Modbus commands that SmartDefense should allow
- `svc-objects` - Network service objects
- `users` - Embedded NGX Portal users
- `vlan` - VLAN networks, VAPs, or WDS links
- `vpn internal-encryption-domain ranges` - IP address ranges in the VPN internal encryption domain
- `vpn sites` - VPN sites
- `vstream policy rules` - VStream Antivirus policy rules
- `webfilter rule` - Web rules

For information on these variables and how to use them with the `clear` command, see ***CLI Variables*** on page 227.

RETURN VALUES

See ***Typical Return Values*** on page 15.

EXAMPLE

The following command deletes all users except the "admin" user.

```
clear users
```

delete

PURPOSE

The `delete` command is used for deleting variables from a table. Use this command to delete any of the following:

- Access lists
- Access list rules
- BGP neighbors
- BGP networks
- Bridges
- DHCP scopes
- Firewall rules
- Firewall servers
- NAT rules
- Network objects
- Network service objects
- OSPF areas
- OSPF networks
- QoS classes
- RADIUS servers
- RIP networks
- Static routes
- SmartDefense CIFS worm patterns
- SmartDefense blocked and allowed FTP commands
- SmartDefense HTTP header patterns
- SmartDefense HTTP-based worm patterns
- SmartDefense SCADA Modbus commands

- Users
- VLAN networks / Virtual Access Points (VAPs) / Wireless Distribution System (WDS) links
- IP address ranges in the VPN internal encryption domain
- VPN sites
- VStream Antispam blocked senders
- VStream Antispam safe senders
- VStream Antivirus policy rules
- Web rules

Note: You cannot delete the following:

- The admin user (user 1)
- The Default QoS class (QoS class 1)
- Implicitly defined NAT rules. For information on NAT rules, see ***nat rules*** on page 362.

SYNTAX

delete *variable*

PARAMETERS

`variable`	String. The type of variable you want to delete. This can be any of the following: • `access-list` - An access list • `access-list-rule` - An access list rule • `antispam blocked-senders list` - A VStream Antispam blocked sender • `antispam safe-senders list` - A VStream Antispam safe sender • `bgp neighbor` - A BGP neighbor • `bgp network` - A BGP network • `bridges` - A bridge • `dhcp scopes` - A DHCP scope

- `fw rules` - A firewall rule
- `fw servers` - A firewall server rule
- `nat rules` - A NAT rule
- `netobj` - A network object
- `ospf area` - An OSPF area
- `ospf network` - An OSPF network
- `qos classes` - A QoS class
- `radius servers` - A RADIUS server
- `rip network` - A RIP network
- `routes` - A static route
- `smartdefense ai cifs file-sharing patterns` - A CIFS worm pattern that SmartDefense should detect
- `smartdefense ai ftp commands` - An FTP command that SmartDefense should allow or block
- `smartdefense ai http header-rejection patterns` - An HTTP header pattern that SmartDefense should detect
- `smartdefense ai http worm-catcher patterns` - An HTTP-based worm pattern that SmartDefense should detect
- `smartdefense ai scada modbus` - A SmartDefense SCADA Modbus command that SmartDefense should allow
- `svc-objects` - A network service object
- `users` - A Embedded NGX Portal user
- `vlan` - A VLAN network, VAP, or WDS link
- `vpn internal-encryption-domain ranges` - An IP address range in the VPN internal encryption domain
- `vpn sites` - A VPN site
- `vstream policy rules` - A VStream

Antivirus policy rule

- `webfilter rule` - A Web rule

For information on these variables and how to use them with the `delete` command, see ***CLI Variables*** on page 227.

RETURN VALUES

See ***Typical Return Values*** on page 15.

EXAMPLE 1

The following command deletes the second user in the Users table:

```
delete users 2
```

EXAMPLE 2

The following command deletes the FTP server rule in the Servers table:

```
delete fw servers ftp
```

set

PURPOSE

The `set` command is used for modifying existing variables.

Note: You cannot rename the Default QoS class (QoS class 1).

SYNTAX

set *variable*

PARAMETERS

`variable`	String. The type of variable you want to modify. This can be any variable except for the following: • `certificate` • A variable that represents a category of variables, but does not have fields of its own. For example, the variable `net` can be used in the command `show net` to display the settings for all variables in the `net` category (such as `net lan`, `net dmz`, etc), but it has no fields of its own and therefore cannot be used with `set`. For information on variables and how to use them with the `set` command, see ***CLI Variables*** on page 227.

RETURN VALUES

See ***Typical Return Values*** on page 15.

EXAMPLE 1

The following command sets the password for user 2 to "mysecretpassword":

```
set users 2 password mysecretpassword
```

EXAMPLE 2

The following command enables the SecuRemote Internal VPN Server:

```
set vpn internalserver mode enabled
```

EXAMPLE 3

The following command sets the FTP server rule so that only FTP connections made through a VPN are allowed.

```
set fw servers ftp enconly true
```

show

PURPOSE

The `show` command is used for displaying variables and their fields.

SYNTAX

`show` *variable*

PARAMETERS

`variable`	String. The type of variable you want to display. This can be any variable except `certificate`. For information on variables and how to use them with the `show` command, see ***CLI Variables*** on page 227.

RETURN VALUES

The desired variables and their fields.

Note: The following information is displayed in encrypted format:

- Embedded NGX Portal user passwords
- Password for authenticating to the ISP
- Passwords for VPN authentication
- Shared secrets for VPN authentication
- Registration key for authenticating to Service Center
- Passwords and keys for wireless authentication
- The Embedded NGX appliance certificate password

However, when using `set` or `add` commands to modify these fields, you can use either clear or encrypted format.

EXAMPLE 1

The following command displays all QoS classes:

```
show qos classes
```

The following command displays information about QoS class 3:

```
show qos classes 3
```

The following command displays the relative weight of QoS class 3:

```
show qos classes 3 weight
```

EXAMPLE 2

The following command displays all server rules:

```
show fw servers
```

The following command displays all of the FTP server rule's settings:

```
show fw servers ftp
```

Use the following command to find out whether the FTP server rule specifies that only FTP connections made through a VPN are allowed.

```
show fw servers ftp enconly
```

Appliance Operation Commands

The commands in this section enable you to manage your Embedded NGX appliance in the following ways:

- Log out of the current session, when connected to the Embedded NGX Portal via SSH or serial console
- Reset various 802.1x port-based security settings
- Reboot the ADSL modem
- Reset VStream Antispam to use the default antispam policy
- Replace the installed certificate with a new self-signed certificate
- Reset the Embedded NGX appliance to its default settings
- Reset the Embedded NGX appliance to the firmware version that shipped with the appliance
- Reboot the Embedded NGX appliance
- Clear the Event Log
- Clear the Security Log
- Reset the Traffic Shaper bandwidth policy to its default settings
- Reboot the my.firewall Web service
- Reset the SmartDefense list of CIFS worm patterns to its defaults
- Reset the SmartDefense list of HTTP header values to its defaults
- Reset the SmartDefense list of HTTP-based worm patterns to its defaults
- Clear Traffic Monitor reports
- Reboot the terminal server
- Uninstall the VStream Antivirus signature databases
- Reset VStream Antivirus to use the default antivirus policy
- Check for new security and software updates
- Backup the Embedded NGX appliance configuration to a USB flash drive

- Restore the Embedded NGX appliance configuration from a USB flash drive
- Swap the primary and secondary Internet connections

backup usb

PURPOSE

The `backup usb` command is used to back up the appliance configuration and device certificate to a USB flash drive. You can then restore the Embedded NGX appliance settings from the USB flash drive as needed. See ***restore usb*** on page 62.

The USB flash drive must have at least 64MB of free space.

Note: Prior to running the command, attach the USB flash drive to the appliance's USB port. Some USB flash drives may not be supported by the appliance.

This command is only relevant for models with a USB port.

EFFECT

The Embedded NGX appliance writes the following files to the USB flash drive:

- `embeddedngx.cfg`
- `embeddedngx.p12`

SYNTAX

backup usb [*folder*]

PARAMETERS

`folder`	String. The folder on the USB flash drive to which the files should be written. If the folder does not already exist, it will be created. If you do not include this parameter, the Embedded NGX appliance creates the folder `<MACAddress>` on the USB flash drive, where `<MACAddress>` is the appliance's MAC address, and backs up the appliance configuration and certificate to this folder.

RETURN VALUES

A message indicating that the Embedded NGX appliance was backed up successfully.

quit

PURPOSE

The `quit` command is used to log out of the current session, when connected to the Embedded NGX Portal via SSH or a serial console.

EFFECT

After you run this command, the SSH client or serial console logs off the Embedded NGX Portal.

SYNTAX

quit

PARAMETERS

None.

RETURN VALUES

None.

reset 802.1x all

PURPOSE

The `reset 802.1x all` command is used to do the following:

- Log off all 802.1x-authenticated hosts, forcing the users to re-authenticate. For information on logging off a specific host, see ***reset 802.1x mac*** on page 41.
- Reset the list of hosts that failed to authenticate to ports for which 802.1x port-based security is configured. For information on resetting the status of a specific host, see ***reset 802.1x mac*** on page 41.
- Reset the list of ports that are assigned to the Quarantine network. For information on resetting a specific port, see ***reset 802.1x port*** on page 42.
- Reset the list of hosts that are locked for each port. See ***reset 802.1x locking*** on page 40.

EFFECT

The LAN LEDs flash briefly, and the lists are reset.

SYNTAX

reset 802.1x all

PARAMETERS

None.

RETURN VALUES

A message indicating that the lists were reset successfully.

reset 802.1x locking

PURPOSE

The `reset 802.1x locking` command is used to reset the hosts that are locked for each port.

When 802.1x port-based security is configured for a LAN port, the first host that attempts to connect to this port is "locked" to the port. In order to connect a different computer to the port, you must first reset 802.1x locking by rebooting the gateway or using this command.

EFFECT

The LAN LEDs flash briefly, and the lists are reset.

SYNTAX

reset 802.1x locking

PARAMETERS

None.

RETURN VALUES

A message indicating that 802.1x locking was reset successfully.

reset 802.1x mac

PURPOSE

The `reset 802.1x mac` command is used to do the following:

- Log off an authenticated host according to its MAC address, forcing the user to re-authenticate.
- Reset the status of a host that failed to authenticate to a port for which 802.1x port-based security is configured. The user can then attempt to authenticate to the port again.

EFFECT

The host's status is reset to Unauthenticated.

SYNTAX

reset 802.1x mac *mac-address*

PARAMETERS

`mac-address`	String. The MAC address of the host whose status you want to reset.

RETURN VALUES

A message indicating that the host's status was reset successfully.

reset 802.1x port

PURPOSE

The `reset 802.1x port` command is used to reset a port's status to Unauthenticated, forcing the user connected to this port to re-authenticate.

EFFECT

The port's status is reset to Unauthenticated.

SYNTAX

reset 802.1x port *port*

PARAMETERS

`port`	String. The name of the port you want to reset. This can be any of the following: • `lan`*x* where *x* is the LAN port number. For example: `lan4` • `dmz/wan2`

RETURN VALUES

A message indicating that the port's status was reset successfully.

reset adsl

PURPOSE

The `reset adsl` command is used to reboot the ADSL modem. If you are having problems with the ADSL connection, resetting the modem may solve the problem.

This command is only relevant for models with a built-in ADSL modem.

EFFECT

The ADSL connection's status changes to "Modem Initializing".

SYNTAX

reset adsl

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 15.

reset antispam policy rules

PURPOSE

If desired, you can reset VStream Antispam to use the default antispam policy. For information on the default antispam policy, see the User Guide.

Note: This will delete any additional VStream Antispam rules you defined.

EFFECT

VStream Antispam is reset to use the default antispam policy.

SYNTAX

reset antispam policy rules

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 15.

reset certificate

PURPOSE

The `reset certificate` command is used to replace the installed device certificate and CA (Certificate Authority) certificate with new self-signed certificates.

Note: If your Embedded NGX appliance is centrally managed, a certificate is automatically generated and downloaded to your appliance. In this case, there is no need to generate a self-signed certificate.

EFFECT

After you run this command, the Embedded NGX appliance generates new self-signed certificates, and replaces the old device certificate and CA certificate with the new ones. This may take a few seconds.

SYNTAX

reset certificate

PARAMETERS

None.

RETURN VALUES

A message indicating that the certificates were replaced successfully.

reset defaults

PURPOSE

The `reset defaults` command is used to reset the Embedded NGX appliance to its default settings. When you reset your Embedded NGX appliance, it reverts to the state it was originally in when you purchased it. The current firmware version is retained. For information on resetting the firmware version, see ***reset firmware*** on page 47.

Warning: This operation erases all your settings and password information. You will have to set a new password and reconfigure your Embedded NGX appliance for Internet connection.

EFFECT

After you run this command, the Embedded NGX appliance is restarted. This may take a few minutes.

SYNTAX

reset defaults

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 15.

reset firmware

PURPOSE

The `reset firmware` command is used to reset the Embedded NGX appliance to the firmware version that shipped with the appliance.

EFFECT

The Embedded NGX appliance is restarted. This may take a few minutes.

SYNTAX

reset firmware

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 15.

reset gateway

PURPOSE

The `reset gateway` command is used to reboot the Embedded NGX appliance. If your Embedded NGX appliance is not functioning properly, rebooting it may solve the problem.

EFFECT

The Embedded NGX appliance is restarted. This may take a few minutes.

SYNTAX

reset gateway

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 15.

reset hard usb

PURPOSE

The `reset hard usb` command is used to reboot a connected USB modem. If you are having problems with the USB modem connection, resetting the modem may solve the problem.

EFFECT

The Embedded NGX appliance's USB ports are powered off and then powered back on, thereby rebooting the USB modem.

SYNTAX

reset hard usb

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 15.

reset logs event

PURPOSE

The `reset logs event` command is used to clear the Event Log. The Event Log displays general appliance events, including the date and the time that each event occurred.

EFFECT

The logs in the Event Log are cleared.

SYNTAX

reset logs event

PARAMETERS

None.

RETURN VALUES

A message indicating that the Event Log was reset successfully.

reset logs security

PURPOSE

The `reset logs security` command is used to clear the Security Log. The Security Log displays security-related events, including the date and the time that each event occurred, and its type.

EFFECT

The logs in the Security Log are cleared.

SYNTAX

reset logs security

PARAMETERS

None.

RETURN VALUES

A message indicating that the Security Log was reset successfully.

reset qos classes

PURPOSE

If desired, you can reset the Traffic Shaper bandwidth policy to use the four predefined classes, and restore these classes to their default settings. For information on these classes and their defaults, see the User Guide.

Note: This will delete any additional classes you defined in Traffic Shaper and reset all rules to use the Default class.

If one of the additional classes is currently used by a rule, you cannot reset Traffic Shaper to defaults. You can determine whether a class is in use or not, by viewing the Rules page.

EFFECT

The QoS classes are reset to their default settings.

SYNTAX

reset qos classes

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 15.

reset services

PURPOSE

The `reset services` command is used to restart the Embedded NGX Service Center connection.

EFFECT

The Embedded NGX Service Center connection is restarted.

SYNTAX

reset services

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 15.

reset smartdefense ai cifs file-sharing patterns

PURPOSE

The `reset smartdefense ai cifs file-sharing patterns` command is used to reset SmartDefense's list of CIFS worm patterns to its defaults.

For information on configuring this list, see ***smartdefense ai cifs file-sharing patterns*** on page 555.

EFFECT

The list of CIFS worm patterns is reset to its defaults.

SYNTAX

reset smartdefense ai cifs file-sharing patterns

PARAMETERS

None.

RETURN VALUES

A message indicating that the list of CIFS worm patterns was reset successfully.

reset smartdefense ai http header-rejection patterns

PURPOSE

The `reset smartdefense ai http header-rejection patterns` command is used to reset SmartDefense's list of HTTP header values to its defaults.

For information on configuring this list, see ***smartdefense ai http header-rejection patterns*** on page 570.

EFFECT

The list of HTTP header values is reset to its defaults.

SYNTAX

reset smartdefense ai http header-rejection patterns

PARAMETERS

None.

RETURN VALUES

A message indicating that the list of HTTP header values was reset successfully.

reset smartdefense ai http worm-catcher patterns

PURPOSE

The `reset smartdefense ai http worm-catcher patterns` command is used to reset SmartDefense's list of HTTP-based worm patterns to its defaults.

For information on configuring this list, see ***smartdefense ai http worm-catcher patterns*** on page 575.

EFFECT

The list of HTTP-based worm patterns is reset to its defaults.

SYNTAX

reset smartdefense ai http worm-catcher patterns

PARAMETERS

None.

RETURN VALUES

A message indicating that the list of HTTP-based worm patterns was reset successfully.

reset soft usb

PURPOSE

The `reset soft usb` command is used to reboot a connected USB modem. If you are having problems with the USB modem connection, resetting the modem may solve the problem.

EFFECT

The Embedded NGX appliance instructs the attached USB modem to restart.

If this approach is not effective, use the reset hard usb command. See ***reset hard usb*** on page 49.

SYNTAX

reset soft usb

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 15.

reset statistics

PURPOSE

The `reset statistics` command is used to clear the Traffic Monitor. The Traffic Monitor displays reports for incoming and outgoing traffic, for selected network interfaces and QoS classes.

EFFECT

The statistics displayed in all Traffic Monitor reports are cleared.

SYNTAX

reset statistics

PARAMETERS

None.

RETURN VALUES

A message indicating that the Traffic Monitor was reset successfully.

reset terminal-server

PURPOSE

The `reset terminal-server` command is used to reboot the Embedded NGX appliance's built-in terminal server. If you are experiencing problems with the connection between the attached serial device and the Telnet client or server, resetting the terminal server may solve the problem.

This command is only relevant for models with a built-in terminal server.

EFFECT

The terminal server is restarted, and any existing connection on the Serial port is terminated.

SYNTAX

reset terminal-server

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 15.

reset vstream database

PURPOSE

The `reset vstream database` command is used to uninstall the VStream Antivirus signature databases. This is useful for troubleshooting purposes.

EFFECT

Both the VStream Antivirus main database and daily database are uninstalled, and VStream Antivirus is disabled.

To re-install the VStream Antivirus databases, use the `updatenow` command. See ***updatenow*** on page 64.

Note: You must be subscribed to VStream Antivirus signature updates, in order to re-install the databases.

SYNTAX

reset vstream database

PARAMETERS

None.

RETURN VALUES

A message indicating that the VStream Antivirus databases were reset successfully.

reset vstream policy rules

PURPOSE

If desired, you can reset VStream Antivirus to use the default antivirus policy. For information on the default antivirus policy, see the User Guide.

Note: This will delete any additional VStream Antivirus rules you defined.

EFFECT

VStream Antivirus is reset to use the default antivirus policy.

SYNTAX

reset antivirus policy rules

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 15.

restore usb

PURPOSE

The `restore usb` command is used to restore the Embedded NGX appliance configuration and device certificate from a USB flash drive. For information on backing up the appliance to a USB flash drive, see ***backup usb*** on page 37.

Note: Prior to running the command, attach the USB flash drive to the appliance's USB port.

This command is only relevant for models with a USB port.

EFFECT

The Embedded NGX appliance is restored from the USB flash drive. This may take some time.

SYNTAX

restore usb [*folder*]

PARAMETERS

`folder`	String. The folder on the USB flash drive from which the Embedded NGX appliance should be restored. This folder must contain the following files: • `embeddedngx.cfg` • `embeddedngx.p12` If you do not include this parameter, the Embedded NGX appliance is restored from the `<MACAddress>` folder on the USB flash drive, where `<MACAddress>` is the appliance's MAC address.

RETURN VALUES

A message indicating that the Embedded NGX appliance was restored successfully.

swap wanconn

PURPOSE

The swap wanconn command is used to swap the roles of the primary and secondary connections, while simultaneously shifting all relevant port assignments between the primary and secondary connections.

EFFECT

The roles of primary and secondary connections and exchanged, including all relevant port assignments.

SYNTAX

swap wanconn

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 15.

updatenow

PURPOSE

The `updatenow` command is used to check for new security and software updates, as well as VStream Antivirus signature database updates.

Note: Software Updates and VStream Antivirus Signature Updates are only available if you are connected to a Service Center and subscribed to this service.

The Embedded NGX appliance automatically checks for software updates and installs them without user intervention, in the following cases:

- Your Embedded NGX appliance is remotely managed.
- Your Embedded NGX appliance is locally managed, and it is set it to automatically check for software updates.

However, you can still use this command to check for updates manually, if needed.

EFFECT

The system checks for new updates and installs them.

SYNTAX

updatenow

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 15.

Informational Commands

The commands in this section enable you to do the following:

- Display information about your Embedded NGX appliance and its settings
- Export your appliance's configuration
- Check whether a user name and password combination are valid
- Display help on any CLI command

authenticate

PURPOSE

The `authenticate` command is used to check whether a username and password combination is valid.

SYNTAX

authenticate *username password*

PARAMETERS

`username`	String. The username to authenticate
`password`	String. The password to authenticate

RETURN VALUES

An indication of whether the username and password combination is valid:

`ok`	Authentication succeeded. The combination is valid.
`failed`	Authentication failed. The username, password, or username-password combination is invalid.

Information about the user's permissions:

`write`	Indicates whether the user has write permissions. This can have the following values: • `true` - The user has write permissions. • `false` - The user does not have write permissions.
`users-manager`	Indicates whether the user is a Users Manager; that is, the user can add, edit, or delete "No Access"-level users, but cannot modify other system settings. This can have the following values: • `true` - The user is a Users Manager. • `false` - The user is not a Users Manager.

`read`	Indicates whether the user has read permissions. This can have the following values: • `true` - The user has read permissions. • `false` - The user does not have read permissions. Note: If this value is `false`, then the user cannot access the Embedded NGX Portal.
`vpnaccess`	Indicates whether the user is allowed to connect to the Embedded NGX appliance using their VPN client. This can have the following values: • `true` - The user has write permissions. • `false` - The user does not have write permissions. For information on setting up VPN remote access, refer to the User Guide.
`filteroverride`	Indicates whether the user is allowed to override Web Filtering. This can have the following values: • `true` - The user has write permissions • `false` - The user does not have write permissions This permission only appears if the Web Filtering service is defined.
`hotspotaccess`	Indicates whether to the user is allowed to log on to the My HotSpot page. This can have the following values: • `true` - The user can log on to the My HotSpot page. • `false` - The user cannot log on to the My HotSpot page. This field is only relevant if Secure HotSpot is configured.

`expire`

The expiration date and time for the user's account. When the user account expires, it is locked, and the user can no longer log on to the Embedded NGX appliance.

This can have the following values:

- `never` - The account never expires.
- A specific date and time in the format:
  `MMM DD YYYY hh:mm:ss<meridian>`
  where:
  MMM = month
  DD = day
  YYYY = year
  hh = hours
  mm = minutes
  `ss` = seconds
  `<meridian>` = AM or PM
  For example, "Dec 01 2005 06:16:00PM"

EXAMPLE

The following command authenticates the username "JohnS" and the password "mysecretpassword":

```
authenticate JohnS mysecretpassword
```

Running this command results in information such as the following:

```
[700000] ok [permissions: write true users-manager false read true
vpnaccess true filteroverride true ]
```

diag ping

PURPOSE

The `diag ping` command is used to check whether the Embedded NGX appliance can reach a specific IP address.

SYNTAX

diag ping *dest_ip* [*deadline*] [*hint*] [*qos*] [*size*] [*src_interface*] [*src_ip*] [*ttl*]

PARAMETERS

`dest_ip`	IP Address. The IP address for which to run the tool.
`deadline`	Integer. The number of seconds after which the ping command should be terminated. When no deadline is specified, five requests will be sent.
`hint`	String. The PMTU method. This can have the following values: • `do` - Prohibit all fragmentation, including local. • `want` - Perform PMTU discovery, and fragment locally when the packet size is too large. • `dont` - Do not set the DF flag. The default value is `want`.
`qos`	Integer. The Type of Service (ToS) value to use in the ping request's IP header. The default value is 0.
`size`	Integer. The ping packet's size in bytes. The default value is 58 bytes.

`src_interface`	String. The network interface from which the packets should originate. This can have the following values: • `auto` - The Embedded NGX appliance automatically chooses the best interface to use. • `wan` • `wan2` • `lan` • `dmz` • The name of a VLAN • The name of a bridge The default value is `auto`.
`src_ip`	IP Address or String. The IP address from which the packets should originate. This can have the following values: • An IP address • `auto` - The Embedded NGX appliance automatically chooses the best IP address to use. The default value is `auto`.
`ttl`	Integer. The packet's time to live. The default value is 64 hops.

RETURN VALUES

Information about the percentage of packet loss and the amount of time it took each packet to reach the specified host and return (round-trip) in milliseconds.

EXAMPLE

Running this command results in information such as the following:

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=51 time=109 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=51 time=112 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=51 time=112 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=51 time=109 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=51 time=109 ms
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4040ms
rtt min/avg/max/mdev = 109.293/110.594/112.233/1.345 ms
```

diag traceroute

PURPOSE

The `diag traceroute` command is used to display a list of all routers used to connect from the Embedded NGX appliance to a specific IP address.

SYNTAX

diag traceroute *dest_ip* [*src_interface*] [*src_ip*]

PARAMETERS

`dest_ip`	IP Address. The IP address for which to run the tool.
`src_interface`	String. The network interface from which the packets should originate. This can have the following values: • `auto` - The Embedded NGX appliance automatically chooses the best interface to use. • `wan` • `wan2` • `lan` • `dmz` • The name of a VLAN • The name of a bridge The default value is `automatic`.
`src_ip`	IP Address or String. The IP address from which the packets should originate. This can have the following values: • An IP address • `auto` - The Embedded NGX appliance automatically chooses the best IP address to use. The default value is `auto`.

RETURN VALUES

A list of routers used to make the connection.

EXAMPLE

Running this command results in information such as the following:

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 38 byte packets
 1  1.2.3.4  10.111 ms  9.790 ms  9.790 ms
 2  21.15.3.3  11.524 ms  11.288 ms  11.235 ms
 3  21.15.28.66  31.532 ms  31.687 ms  31.267 ms
 4  21.15.62.158  31.591 ms  31.575 ms  31.193 ms
 5  21.15.10.93  31.121 ms  34.982 ms  31.338 ms
 6  21.15.12.6  113.494 ms  110.934 ms  111.472 ms
 7  21.15.14.144  122.579 ms  102.869 ms  103.836 ms
 8  12.70.1.1  106.936 ms *  106.551 ms
 9  190.60.424.125  111.165 ms  111.713 ms  110.824 ms
10  62.233.145.25  108.805 ms  112.117 ms  194.902 ms
11  75.14.234.134  115.851 ms  121.130 ms  113.115 ms
12  217.129.49.45  113.425 ms  111.456 ms 209.85.252.83  114.084 ms
13  109.83.243.77  113.281 ms  121.679 ms  125.932 ms
14  8.8.8.8  111.053 ms  111.917 ms  109.483 ms
```

export

PURPOSE

The `export` command is used to display Embedded NGX appliance settings.

This is useful in the following cases:

- You are troubleshooting a problem and need to examine the appliance settings.
- You want to change the appliance configuration.

  After exporting the configuration, you can copy it and paste it in a *.cfg file. You can then change the settings as desired and import the modified file to one or more Embedded NGX appliances.

  For information on importing configuration files, refer to the User Guide.
- You want to backup the Embedded NGX appliance settings.

  After exporting the configuration, you can copy it and paste it in a *.cfg file. You can then use this file to backup and restore, as needed.

SYNTAX

export [*variable*]

PARAMETERS

`variable`	String. The type of settings you want to export. This can be any variable or a variable that represents a category of variables. For example, the variable `net` can be used in the command `export net` to display the settings for all variables in the `net` category (such as `net lan`, `net dmz`, etc). For information on variables and how to use them with the `export` command, see ***CLI Variables*** on page 227. If you do not include this parameter, all settings are exported.

RETURN VALUES

The desired Embedded NGX Portal appliance settings.

The exported settings are in CLI script format and can be executed.

EXAMPLE

The following command exports the Embedded NGX Portal appliance user database:

```
export
```

Running this command results in information such as the following:

```
    export
# Configuration script
# License: Edge N (Unlimited nodes)
# Gateway MAC: 00:08:da:79:00:7e
# firmware version: 8.2.14n

# Pre-configuration settings
clear nat rules

# Device settings
set device productkey 777777-66666-eeeeee hostname "" behindnat
undefined

...
```

```
# Anti spam sender
clear antispam safe-senders list

# List of blocked senders
set antispam blocked-senders mode off action reject track log
mark-subject-text [SPAM]

# Anti spam sender
clear antispam blocked-senders list
# END Configuration script
```

help

PURPOSE

The `help` command is used to display information about a command.

Note: Information is not displayed for commands that are not supported by your hardware type and license.

SYNTAX

help *command* [*variable*]

PARAMETERS

`command`	String. The command for which you want to display information.
`variable`	String. One or more variables that follow the command and create a valid expression.

RETURN VALUES

When you run this command, the following information appears:

- A brief description of the command
- A list of variables that can follow the command

EXAMPLE

To display information about the `add` command, enter the following command:

```
help add
```

The following information is displayed:

```
      help add
add                           Add an item to a table
subcommands:
----------------------------------------
radius                        RADIUS settings
bridges                       Bridge settings
vlan                          VLAN network settings
qos                           Quality of Service (Traffic Shaper) settings
svc-objects                   Service object settings
routes                        Static route settings
netobj                        Network object settings
vpn                           VPN settings
users                         User settings
fw                            Firewall settings
nat                           Firewall NAT settings
certificate                   Certificate settings
ospf                          OSPF router settings
bgp                           BGP router settings
rip                           RIP router settings
dhcp                          DHCP settings
vstream                       VStream Antivirus settings
smartdefense                  SmartDefense settings
webfilter                     Web Filtering settings
antispam                      Anti spam global settings
access-list                   Access-lists definition
access-list-rule              Access-lists-rule settings
```

EXAMPLE 2

You can add variables to the command, and display information about the final variable in the command:

```
help add users
```

The `users` variable's fields are listed:

```
      help add users
users                          User settings
subcommands:
---------------------------------------
name                           User´s username
password                       User´s password
adminaccess                    User´s level of access to the my.firewall portal
vpnaccess                      Indicates whether the user can log on using a VPN client
filteroverride                 Indicates whether the user can override Web Filtering
hotspotaccess                  Indicates whether the user can log on to the My HotSpot page
rdpaccess                      Indicates whether the user can use the Remote Desktop feature
users-manager                  Indicates whether the user can add/delete other users
networkaccess                  Indicates whether the user can use the Network Access feature
expire                         User account´s expiration date and time
```

EXAMPLE 3

You cannot display information about a variable alone:

```
help users
```

If you attempt to do so, an error message is displayed, along with suggestions for correcting the command syntax:

```
    help users
[700002] Syntax error: users
Possible completions:
help, authenticate, set, show, clear, delete, export, add, swap, reset,
backup, restore, updatenow, quit, diag, info
```

info adsl

PURPOSE

The `info adsl` command enables you to view information about the ADSL modem, ADSL connection parameters, and ADSL connection statistics. For information on displaying ADSL connection parameters only, see ***info adsl parameters*** on page 84. For information on displaying the ADSL modem's details only, see ***info adsl device*** on page 82. For information on displaying IPoA IP address only, see ***info adsl ipoa-ip*** on page 83. For information on displaying ADSL connection statistics, see ***info adsl statistics*** on page 86.

This command is only relevant for models with a built-in ADSL modem.

SYNTAX

info adsl

PARAMETERS

None.

RETURN VALUES

For examples of returned information, see ***info adsl parameters*** on page 84, ***info adsl device*** on page 82, ***info adsl ipoa-ip*** on page 83, and ***info adsl statistics*** on page 86.

info adsl device

PURPOSE

The `info adsl device` command is used to display information about your appliance's ADSL modem.

This command is only relevant for models with a built-in ADSL modem.

SYNTAX

info adsl device

PARAMETERS

None.

RETURN VALUES

`Running Firmware`	The version of the ADSL firmware that is currently in use.
`Primary Firmware`	The version of the primary ADSL firmware.
`Backup Firmware`	The version of the backup ADSL firmware. If no backup firmware is available, this field displays `N/A`.
`Hardware Version`	The version of the ADSL hardware.

EXAMPLE

Running this command results in information such as the following:

```
Running Firmware: SW2.0.11a
Primary Firmware: SW2.0.11a
Backup Firmware: SW2.0.8a
Hardware Version: 810100
```

info adsl ipoa-ip

PURPOSE

The `info adsl ipoa-ip` command is used to display the IP address of your gateway's ADSL interface, when running in IPoA mode.

This command is only relevant for models with a built-in ADSL modem.

SYNTAX

info adsl ipoa-ip

PARAMETERS

None.

RETURN VALUES

The IP address of your gateway's ADSL interface.

EXAMPLE

Running this command results in information such as the following:

```
IPoA Address: 212.515.2.1
```

info adsl parameters

PURPOSE

The `info adsl parameters` command is used to display statistics for the ADSL connection.

This command is only relevant for models with a built-in ADSL modem.

SYNTAX

info adsl parameters

PARAMETERS

None.

RETURN VALUES

`Tx line rate`	The line rate for transmission in kbps
`Rx line rate`	The line rate for reception in kbps
`Tx Power`	The local and remote transmission power in dB.
`Line Attenuation`	The local and remote line attenuation in dB. The line attenuation is the difference between the signal power transmitted to the local/remote line end, and that which it received.
`SNR Margin`	The local and remote Signal to Noise Ration (SNR) margin in dB. The SNR margin is the difference between the amount of noise received by the by the local/remote line end, and the amount of noise it can tolerate.
`Self Test`	Indicates whether DSL modem has passed a self-test. This can be either of the following: • `Passed` • `Failed`

DSL Standard	The DSL line's standard
Trellis Coding	The DSL line's trellis coding
Framing Structure	The DSL line's framing structure
Operation Mode	The DSL line's operation mode

EXAMPLE

Running this command results in information such as the following:

```
    Tx line rate: 508 kbps
    Rx line rate: 2040 kbps
    Tx Power:
        Local:       0.3 dB
        Remote:      8.5 dB
    Line Attenuation:
        Local:       2.0 dB
        Remote:      0.0 dB
    SNR Margin:
        Local:       44.5 dB
        Remote:      22.5 dB
    Self Test:       Passed
    DSL Standard:    ADSL2/2+
    Trellis Coding:  Disable
    Framing Structure: Unknown
    Operation Mode:  Showtime/Data
```

info adsl statistics

PURPOSE

The `info adsl statistics` command enables you to view ADSL connection counters, as well as statistics for ADSL connection failures and performance. For information on displaying ADSL connection counters only, see ***info adsl statistics counters*** on page 87. For information on displaying the ADSL connection failures only, see ***info adsl statistics failures*** on page 91. For information on viewing ADSL performance statistics only, see ***info adsl statistics performance*** on page 93.

This command is only relevant for models with a built-in ADSL modem.

SYNTAX

info adsl statistics

PARAMETERS

None.

RETURN VALUES

For examples of returned information, see ***info adsl statistics counters*** on page 87, ***info adsl statistics failures*** on page 91, and ***info adsl statistics performance*** on page 93.

info adsl statistics counters

PURPOSE

The `info adsl statistics counters` command enables you to view ADSL connection counters.

This command is only relevant for models with a built-in ADSL modem.

SYNTAX

info adsl statistics counters [*type* [*connection-end*]]

PARAMETERS

`type`	String. The type of counters to display. This can have the following values: • `management` - Display management counters. • `tps-tc` - Display Transport Protocol Specific Transmission Convergence (TPS-TC) counters. If you do not include this parameter, information is displayed for both counter types.
`connection-end`	String. The ADSL connection end for which to display counters. This can have the following values: • `local` - Display counters for the local end of the ADSL connection. • `remote` - Display counters for the remote end of the ADSL connection. If you include the `type` parameter, but do not include the `connection-end` parameter, the specified type of counters are displayed for both connection ends.

RETURN VALUES

Reports for the specified type(s) of counters.

The management counter report includes the following information for the specified ADSL connection end(s):

FEC	The number of forward error corrections anomalies for the interleaved data stream, on the specified end of the ADSL connection.
CRC	The number of cyclic redundancy check anomalies for the interleaved data stream, on the specified end of the ADSL connection.
NCD	The number of no-cell-delineation events for the interleaved data stream, on the specified end of the ADSL connection. These events are counted until the ADSL modem has synchronized with the ADSL service provider for the first time.
OCD	The number of out-of-cell delineation events for the interleaved data stream, on the specified end of the ADSL connection. These events are counted if the ADSL modem was synchronized with the ADSL service provider, and then went out of synch.
HEC	The number of header error checks for the interleaved data stream, on the specified end of the ADSL connection.
SEF	The number of severely errored frames on the specified end of the ADSL connection.
LOS	The number of loss-of-signal events on the specified end of the ADSL connection.

The TPS-TC counter report includes the following information for the specified ADSL connection end(s):

`CP HEC0`	The number of header error checks for bearer 0, on the specified end of the ADSL connection.
`CP UpperLayer`	The number of cells passed to the upper-layer ATM function, on the specified end of the ADSL connection.
`Bit Error`	The number of bit errors in the idle cell payload received in the ATM data path, on the specified end of the ADSL connection.

EXAMPLE 1

Running the following command:

```
info adsl statistics counters management
```

Results in information such as the following:

```
statistics:
 counters:
  management:
   local:
      FEC: Intrlvd 0  Fast 0000
      CRC: Intrlvd 0  Fast 0004
      NCD: Intrlvd 0  Fast 0000
      OCD: Intrlvd 3507  Fast 0000
      HEC: Intrlvd 0  Fast 0002
      SEF: 0
      LOS: 0
```

```
   remote:
      FEC: Intrlvd 0  Fast 0000
      CRC: Intrlvd 0  Fast 0000
      NCD: Intrlvd 0  Fast 0000
      OCD: Intrlvd -  Fast -
      HEC: Intrlvd 0  Fast 0000
      SEF: 0
      LOS: 0
```

EXAMPLE 2

Running the following command:

```
info adsl statistics counters tps-tc local
```

Results in information such as the following:

```
statistics:
 counters:
   tps-tc:
   local:
      CP HEC0: -
      CP UpperLayer: -
      Bit Error: -
```

info adsl statistics failures

PURPOSE

The `info adsl statistics failures` command enables you to view statistics for ADSL connection failures.

This command is only relevant for models with a built-in ADSL modem.

SYNTAX

info adsl statistics failures [*connection-end*]

PARAMETERS

`connection-end`	String. The ADSL connection end for which to display statistics. This can have the following values: • `local` - Display connection failures that occurred on the local end of the ADSL connection. • `remote` - Display connection failures that occurred on the remote end of the ADSL connection. If you do not include this parameter, statistics are displayed for both connection ends.

RETURN VALUES

Reports for the specified ADSL connection end(s).

Each report includes the following information:

LOS	The number of loss-of-signal events on the specified end of the ADSL connection. A DSL failure will occur if this value exceeds 127.
SEF	The number of severely-errored frames on the specified end of the ADSL connection. A DSL failure will occur if this value exceeds 127.

NCD	The number of no-cell-delineation events on the specified end of the ADSL connection. A DSL failure will occur if this value exceeds 127.

EXAMPLE

Running the following command:

```
info adsl statistics failures local
```

Results in information such as the following:

```
statistics:
 failures:
  local:
      LOS: 0
      SEF: 0
      NCD: 0
```

info adsl statistics performance

PURPOSE

The `info adsl statistics performance` command enables you to view statistics for the ADSL connection's performance.

This command is only relevant for models with a built-in ADSL modem.

SYNTAX

info adsl statistics performance

PARAMETERS

None.

RETURN VALUES

`15 Min. Errored Seconds`	The number of errored seconds in the current 15-minute interval.
`15 Min. Severely Errored Seconds`	The number of severely errored seconds in the current 15-minute interval.

EXAMPLE

Running this command results in information such as the following:

```
statistics:
 performance:
      15  Min. Errored Seconds: 0
      15  Min. Severely Errored Seconds: 0
```

info antispam

PURPOSE

The `info antispam` command is used to display statistics for the Content Based Antispam and Block List engines.

SYNTAX

info antispam

PARAMETERS

None.

RETURN VALUES

The following information is displayed for both SMTP and POP3 email messages:

`pending`	The number of email messages pending for the Content Based Antispam and Block List engines.
`spam`	The number of email messages that the Content Based Antispam and Block List engines determined to be spam.
`suspected-spam`	The number of email messages that the Content Based Antispam and Block List engines determined to be suspected spam.
`non-spam`	The number of email messages that the Content Based Antispam and Block List engines determined to be legitimate.
`not-scanned`	The number of email messages that the Content Based Antispam and Block List engines did not scan.
`total`	The total number of email messages scanned by the Content Based Antispam and Block List engines.

EXAMPLE

Running this command results in information such as the following:

```
smtp emails:
     pending: 1
     spam: 23
     suspected-spam: 45
     non-spam: 156
     not-scanned: 0
     total: 225

pop3 emails:
     pending: 4
     spam: 12
     suspected-spam: 56
     non-spam: 133
     not-scanned: 0
     total: 205
```

info antispam ip-reputation

PURPOSE

The `info antispam ip-reputation` command is used to display IP Reputation engine statistics.

SYNTAX

info antispam ip-reputation

PARAMETERS

None.

RETURN VALUES

The following information is displayed:

`pending-connections`	The number of SMTP email connections pending for the IP Reputation engine.
`blocked-connections`	The number of SMTP email connections blocked by the IP Reputation engine.
`allowed-connections`	The number of SMTP email connections allowed by the IP Reputation engine.
`total-connections`	The total number of SMTP email connections scanned by the IP Reputation engine.

EXAMPLE

Running this command results in information such as the following:

```
pending-connections: 3
blocked-connections: 36
allowed-connections: 154
total-connections: 193
```

info antispam servers

PURPOSE

The `info antispam servers` command is used to display information about the VStream Antispam data center's servers.

SYNTAX

info antispam servers

PARAMETERS

None.

RETURN VALUES

The following information is displayed for each server:

The server's IP address	
`Weight`	The server's load balancing weight.
`Response Time`	The server's response time (in milliseconds).
`Pending Requests`	The number of VStream Antispam requests pending for the server.
`Status`	The server's current status. This can have the following values: • `OK` • `Unavailable`

EXAMPLE

Running this command results in information such as the following:

```
74.208.45.33:
     Weight: 10
     Response Time: 112ms
     Pending Requests: 1
     Status: OK
87.106.183.224:
     Weight: 10
     Response Time: 23ms
     Pending Requests: 0
     Status: OK
...
```

info bgp

PURPOSE

The `info bgp` command is used to display general information about your appliance's BGP settings.

SYNTAX

info bgp

PARAMETERS

None.

RETURN VALUES

General BGP information.

EXAMPLE

Running this command results in information such as the following:

```
BGP table version is 0, local router ID is 62.90.32.148
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete


   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.10.0     62.90.32.88              0           100 11111 i
*> 192.168.50.0     0.0.0.0                  0         32768  i


Total number of prefixes 2
 Number of external LSA 0. Checksum Sum 0x00000000
 Number of opaque AS LSA 0. Checksum Sum 0x00000000
 Number of areas attached to this router: 0
```

info bgp neighbor

PURPOSE

The `info bgp neighbor` command is used to display information about your appliance's BGP neighbors.

SYNTAX

info bgp neighbor [*ip-address*]

PARAMETERS

`ip-address`	IP Address. The BGP neighbor's IP address.

RETURN VALUES

Information about yours appliance's BGP neighbor(s).

EXAMPLE

Running this command results in information such as the following:

```
BGP neighbor is 62.90.32.88, remote AS 11111, local AS 33333, external
link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 00:00:00, hold time is 180, keepalive interval is 60 seconds
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  0          0
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             0          0
    Route Refresh:          0          0
    Capability:             0          0
```

```
    Total:                  0          0
Minimum time between advertisement runs is 30 seconds
  Default weight 100

 For address family: IPv4 Unicast
  Community attribute sent to this neighbor(both)
  Inbound path policy configured
  Outbound path policy configured
  Incoming update network filter list is *2001
  Outgoing update network filter list is *2000
  0 accepted prefixes

  Connections established 0; dropped 0
  Last reset never
Next start timer due in 7 seconds
Read thread: off  Write thread: off
...
```

info bgp routes

PURPOSE

The `info bgp routes` command is used to display information about BGP routes.

SYNTAX

info bgp routes

PARAMETERS

None.

RETURN VALUES

A list of BGP-related routes. Each route is marked with a code that indicates its type. The Embedded NGX appliance supports the following route types:

K	A kernel route. Kernel routes are routes that are recognized by the OSPF daemon via the kernel. For example, a static route.
C	A connected route. Connected routes are routes that are created for each new network defined on the Embedded NGX appliance. For example, LAN.
S	A static route defined by the user.
R	A RIP route.
O	An OSPF route. OSPF routes are routes learned via OSPF.
I	An ISIS route.
B	A BGP route. BGP routes are learned via BGP.
>	A selected route.

EXAMPLE

Running this command results in information such as the following:

```
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

K>* 0.0.0.0/0 via 62.90.32.1, wan
C>* 62.90.32.0/24 is directly connected, wan
C>* 127.0.0.0/8 is directly connected, lo
B>* 192.168.10.0/24 [20/0] via 62.90.32.88, wan, 00:01:27
C>* 192.168.50.0/24 is directly connected, lan
C>* 192.168.201.0/24 is directly connected, br0
```

info bgp summary

PURPOSE

The `info bgp summary` command is used to display a summary of your appliance's BGP settings.

SYNTAX

info bgp summary

PARAMETERS

None.

RETURN VALUES

A summary of your appliance's BGP settings.

EXAMPLE

Running this command results in information such as the following:

```
BGP router identifier 62.90.32.148, local AS number 33333
RIB entries 3, using 168 bytes of memory
Peers 1, using 2464 bytes of memory

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
62.90.32.88     4 11111       4       5        0    0    0 00:01:36
1

Total number of neighbors 1
 Number of external LSA 0. Checksum Sum 0x00000000
 Number of opaque AS LSA 0. Checksum Sum 0x00000000
 Number of areas attached to this router: 0
```

info bridge

PURPOSE

The `info bridge` command enables you to view information about bridges. For information on displaying bridge statuses only, see ***info bridge status*** on page 108. For information on displaying bridge Spanning Tree Protocol (STP) details only, see ***info bridge stp*** on page 110. For information on viewing MAC addresses in the bridge's forwarding table only, see ***info bridge macs*** on page 106.

SYNTAX

info bridge

PARAMETERS

None.

RETURN VALUES

For examples of returned information, see ***info bridge macs*** on page 106, ***info bridge status*** on page 108, and ***info bridge stp*** on page 110.

info bridge macs

PURPOSE

The `info bridge mac` command is used to display the MAC addresses in each bridge's forwarding table.

SYNTAX

info bridge macs

PARAMETERS

None.

RETURN VALUES

A list of MAC addresses, grouped according to bridge and network.

EXAMPLE

Running this command results in information such as the following:

```
Bridge1:
  WDS1:
    aa:bb:cc:dd:12:ff
    00:23:bb:cc:00:ee
  WDS2:
    ff:ee:dd:cc:66:aa
    00:ff:ee:55:cc:bb
    aa:00:ff:ee:dd:cc
Bridge2:
  WDS3:
    aa:45:cc:22:ee:ff
    00:11:bb:bb:dd:ee
  WDS4:
    ff:10:dd:33:cc:aa
    00:ff:ee:44:cc:dd
```

info bridge status

PURPOSE

The `info bridge status` command is used to display bridges' statuses.

SYNTAX

info bridge status

PARAMETERS

None.

RETURN VALUES

The following information is displayed for each bridge:

`bridge-id`	The bridge's ID. A bridge's ID is composed of its priority and a bridged network's MAC address. The bridge with the lowest ID is elected as the root bridge.
`stp-mode`	Indicates whether Spanning Tree Protocol (STP) is enabled for the bridge. This can have the following values: • `enabled` - STP is enabled for the bridge. • `disabled` - STP is disabled for the bridge.
`bridged networks`	A list of networks assigned to the bridge.

EXAMPLE

Running this command results in information such as the following:

```
Bridge1:
  bridge-id:        8000.000000000000
  stp-mode:         disabled
  bridged networks:
    WDS2
    VLAN_s
    WLAN

Bridge2:
  bridge-id:        8000.0020ed087ae0
  stp-mode:         enabled
  bridged networks:
    VLAN_t
    WDS1
```

info bridge stp

PURPOSE

The `info bridge stp` command is used to display information about bridges' Spanning Tree Protocol (STP) settings.

SYNTAX

info bridge stp

PARAMETERS

None.

RETURN VALUES

The following information is displayed for each bridge:

`bridge-id`	The bridge's ID. A bridge's ID is composed of its priority and a bridged network's MAC address. The bridge with the lowest ID is elected as the root bridge.
`designated-root`	The bridge ID of the root bridge. All bridges in the spanning tree calculate the shortest distance to the root bridge, in order to eliminate loops in the topology and provide fault tolerance.
`root-port`	The root port's ID. The root port forwards frames out of the bridge.
`path-cost`	The port's cost. This value is only relevant if this port is not the root port.
`max-age`	The maximum amount of time (in seconds) that received protocol information is stored before it is discarded.

`bridge-max-age`	The value of the `max-age` parameter, when this bridge is the root bridge or is attempting to become the root bridge.
`hello-time`	The interval of time (in seconds) between transmissions of configuration BPDUs, by a bridge that is the root bridge or is attempting to become the root bridge.
`bridge-hello-time`	The value of the `hello-time` parameter, when this bridge is the root bridge or is attempting to become the root bridge.
`forward-delay`	The amount of time (in seconds) that a port should spend in the Listening State before moving to the Learning State, or in the Learning State before moving to the Forwarding State.
`bridge-forward-delay`	The value of the `forward-delay` parameter, when this bridge is the root bridge or is attempting to become the root bridge.
`ageing-time`	The amount of time (in seconds) a MAC address is kept in the forwarding database.
`hello-timer`	The value of the Hello Timer. This timer ensures periodic transmission of configuration BPDUs by the bridge, when it is the root bridge or attempting to become the root bridge.
`tcn-timer`	The value of the Topology Change Notification Timer. This timer ensures that the designated bridge on the LAN to which this bridge's root port is attached is notified of any detected topology change.

`topo-change-timer`	The value of the Topology Change Timer. This timer determines the interval of time (in seconds) at which the bridge should transmit configuration BPDUs with the Topology Change flag set, if this bridge is the root bridge and a topology change was detected.
`flags`	A list of flags used by the Spanning Tree Protocol.

In addition to the information above, the following information is displayed for each bridged network:

`port-id`	The port's ID. A port ID is composed of the port's priority and the port's logical number. The port with the lowest ID is elected as the root port, which forwards frames out of the bridge.
`state`	The port's current state. This can be any of the following: disabled, listening, learning , forwarding, or blocking.
`designated-root`	The bridge ID of the root bridge.
`designated-bridge`	The bridge ID of the of the designated bridge for this network.
`designated-port`	The designated port's ID.
`designated-cost`	If this port is the designated port, this value represents the path cost offered to the network to which the port is attached. Otherwise, this value represents the cost of the path to the root port, as offered by the current designated port of the network to which this port is attached.

`path-cost`	The port's cost. STP uses the available port with the lowest cost to forward frames to the root port. All other ports are blocked.
`message-age-timer`	The value of the Message Age Timer. This timer measures the age of the received protocol information recorded for a port, and ensures that this information is discarded when its age exceeds the value of the `max-age` parameter recorded by the bridge.
`forward-delay-timer`	The value of the Forward Delay Timer. This timer determines the amount of time (in seconds) spent by a port in the Listening State before moving to the Learning State, or in the Learning State before moving to the Forwarding State.
`hold-timer`	The value of the Hold Timer. This timer ensures that configuration BPDUs are not transmitted too frequently through any bridge.
`flags`	A list of flags used by the Spanning Tree Protocol.

EXAMPLE

Running this command results in information such as the following:

```
Bridge1:
  stp-mode is disabled
Bridge2:
  bridge-id:            8000.0020ed087ae0
  designated-root:      8000.0020ed087ae0
  root-port:            0
  path-cost:            0
  max-age:              20.00
  bridge-max-age:       20.00
  hello-time:           2.00
  bridge-hello-time:    2.00
  forward-delay:        15.00
  bridge-forward-delay: 15.00
  ageing-time:          300.00
  hello-timer:          0.91
  tcn-timer:            0.00
  topo-change-timer:    0.00
  flags:
    none
```

```
bridged networks:
  VLAN_t:
    network is currently disabled
  WDS1:
    port-id:             8001
    state:               listening
    designated-root:     8000.0020ed087ae0
    designated-bridge:   8000.0020ed087ae0
    designated-port:     8001
    designated-cost:     0
    path-cost:           100
    message-age-timer:   0.00
    forward-delay-timer: 8.60
    hold-timer:          0.91
    flags:
      none
```

info certificate

PURPOSE

The `info certificate` command is used to display information about the device certificate and CA (Certificate Authority) certificate currently installed on your appliance.

SYNTAX

info certificate

PARAMETERS

None.

RETURN VALUES

The following information is displayed for your appliance's certificate and for the CA's certificate:

`GMT`	The time zone of the Validity Start Time and Validity End Time, relative to GMT (Greenwich Mean Time).
`Validity Start Time`	The day of the week, date, and time from which this certificate is valid. This information is presented in the format: `Day MM DD hh:mm:ss YYYY` where: Day = the day of the week MM = the month DD = the date hh = hours mm = minutes ss = seconds YYYY = the year

`Validity End Time`	The day of the week, date, and time when this certificate expires. This information is provided in the same format as `Validity Start Time`.
`Certificate DN`	The Distinguished Name (DN) (identifying information).
`Fingerprint`	The certificate's fingerprint.

EXAMPLE

Running this command results in information such as the following:

```
[700000] Certificate Information:
Device Certificate
==================
GMT:                 GMT+02:00
Validity Start Time: Sat Aug  4 10:16:01 2007

Validity End Time:   Sat Jul 31 10:16:01 2027

Certificate DN:      /O=EmbeddedNG/OU=Gateways/CN=00:08:da:77:70:70
Fingerprint:         WENT BAIT TALL FREY HOOD HOST CUT BOSE YAP GRID
FAME GAUL
```

```
CA Certificate
==============
GMT:                 GMT+02:00
Validity Start Time: Sat Aug  4 10:15:58 2007


Validity End Time:   Sat Jul 31 10:15:58 2027


Certificate DN:
/O=EmbeddedNG/OU=LocalCA/CN=CA-00:08:da:77:70:70
Fingerprint:         TUB BET WING AVON STUN BOMB SEEN DESK BAWD RENT
SIR YE
```

info computers

PURPOSE

The `info computers` command is used to display information about the currently active computers on your network.

SYNTAX

info computers

PARAMETERS

None.

RETURN VALUES

The following information is displayed for each currently active device in each internal network or bridge.

The device's IP address

`mac`	The device's MAC address.
`type`	The device's type. This can be either of the following: • `firewall` • `computer`
`name`	The device's name.
`license`	The status of the device's license. This can be either of the following: • `licensed` - the device is licensed • `inactive` - the device did not communicate through the firewall, and therefore did not use a license • `N/A` - the device's license status is not available

In addition to the information above, the following information is displayed for each wireless station (in wireless models):

`tx rate`	The current transmission rate in Mbps
`signal`	The signal strength in dB
`qos`	Indicates whether the wireless client supports Wireless Multimedia (WMM). Possible values are: • `yes.` The wireless client supports WMM. • `no.` The wireless client does not support WMM.
`xr`	Indicates whether the wireless client supports Extended Range (XR) mode. Possible values are: • `yes.` The wireless client supports XR mode. • `no.` The wireless client does not support XR mode. • `not active.` XR mode is currently not active.
`cipher`	The security protocol used for the wireless connection

The following statistics are divided into receive and transmit for each wireless station (in wireless models):

`frames ok`	The total number of frames that were successfully transmitted and received
`management`	The total number of transmitted and received management packets
`control`	The total number of received control packets
`errors`	The total number of transmitted and received frames for which an error occurred
`retry ratio`	The percentage of retry packets that were received

`dup ratio`	The percentage of frames received more than once
`fail ratio`	The percentage of unsuccessful transmission attempts
`packet error ratio`	The percentage of retry packets that were transmitted

EXAMPLE

Running this command results in information such as the following:

```
lan:
  192.168.10.1:
    mac:              00:08:da:77:70:6e
    type:             firewall
    name:             Gateway
    license:          N/A
  192.168.10.21:
    mac:              00:0c:6e:41:5d:6a
    type:             computer
    name:             OFFICE
    license:          licensed
wlan:
  192.168.252.1:
    mac:              00:20:ed:08:7a:e0
    type:             firewall
    name:             Gateway
    license:          N/A
```

```
192.168.252.78:
  mac:              00:05:3c:09:65:18
  type:             computer
  name:             laptop
  license:          licensed
  tx rate:          11.0 Mbps
  signal:           46 dB
  qos:              no
  xr:               not active
  cipher:           WEP
  receive:
      frames ok:    1221
      management:   9
      control:      0
      errors:       0
      retry ratio:    0.24%
      dup ratio:      0.08%
  transmit:
      frames ok:    1078
      management:   10
      errors:       0
      fail ratio:     0.27%
      packet error ratio:    1.71%
```

info connections

PURPOSE

The `info connections` command is used to display information about currently active connections between your network and the external world.

SYNTAX

info connections

PARAMETERS

None.

RETURN VALUES

`Connection table`	The number of currently active connections.

The following information is displayed for each connection:

`src_ip`	The source IP address.
`sport`	The source port.
`dst_ip`	The destination IP address.
`dport`	The destination port.
`ip_p`	The IP protocol.
`time`	The connection timeout (in seconds). If no packets pass for this interval of time, the firewall terminates the connection.
`Options`	Displays further details about the connection: • `Plain` - The connection is not encrypted. • `AES/3DES` - The connection is encrypted. • `Through VPN` - The connection is a VPN connection. • `AntiVirus` - The connection is being scanned

by VStream Antivirus.

- AntiSpam - The connection is being scanned by VStream Antispam.

QoS class — The QoS class to which the connection belongs.

Internal attributes — The connection's internal attributes. This can be any of the following:

- BOTH_FIN ESTABLISHED - The connection was terminated by both parties.
- SRC_FIN ESTABLISHED - The connection was terminated by the source party.
- DST_FIN ESTABLISHED - The connection was terminated by the destination party.
- ESTABLISHED - The connection is in established state.
- MORE_INSPECT - The connection needs more inspection by the firewall.

EXAMPLE

Running this command results in information such as the following:

```
      info connect
Connection table - 8 connections
src_ip | sport | dst_ip | dport | ip_p | time | Options | QoS class | Internal attributes
-------------------------
192.168.10.12 | 3163 | 192.168.10.1 | 80 | 6 | 13 | Plain | Default | BOTH_FIN ESTABLISHED
192.168.10.12 | 3162 | 192.168.10.1 | 80 | 6 | 3 | Plain | Default | BOTH_FIN ESTABLISHED
               ....
```

info device

PURPOSE

The `info device` command is used to display information about your appliance, such as your current firmware version and additional details.

SYNTAX

info device

PARAMETERS

None.

RETURN VALUES

The following information is returned for all Embedded NGX appliances:

Hardware	Information about the Embedded NGX appliance hardware.
`Appliance Type`	The type of the current hardware.
`Version`	The version of the hardware.
General	General information.
`Name`	The gateway hostname.
`Uptime`	The time that elapsed from the moment the unit was turned on.
`CPU Usage`	The percentage of CPU that is currently in use.
`Flash Usage`	The percentage of flash memory that is currently in use.
License	Information about the Embedded NGX appliance's current license.
`MAC Address`	The appliance's WAN MAC address.
`Product Key`	The installed Product Key.

`Product Name`	The licensed software and the number of allowed nodes.
`Used Nodes`	The number of nodes used.
Firmware	Information about the Embedded NGX appliance's current firmware.
`Running`	The version of the firmware that is currently in use.
`Primary`	The version of the primary firmware.
`Backup`	The version of the backup firmware.
`Bootcode`	The version of the Embedded NGX bootloader.
`Debug Firmware`	Indicates whether the currently installed firmware is a special debug firmware. This can be either of the following: • `Yes` • `No` This field is used by support personnel.
Total Memory	Information about the Embedded NGX appliance's total memory.
`Main`	The total main memory in megabytes.
`DFA`	The amount of DFA memory installed in megabytes. DFA memory is used for antivirus acceleration.
`DFA Test`	The result of the DFA memory self-test.
Free Memory	Information about the Embedded NGX appliance's free memory.
`User`	The amount of free memory in the user module in kilobytes.
`Kernel`	The amount of free memory in the kernel module in kilobytes.

`Firewall`	The amount of free memory in the firewall module in kilobytes.
VStream Database	Information about the VStream Antivirus databases.
`Main`	Information about the VStream Antivirus main database: • The date and time at which the database was last updated • `Version` - The version number • `Size` - The database's size • `CRC` - The database's CRC (Cyclic Redundancy Check) value for file verification
`Daily`	Information about the VStream Antivirus daily database: • The date and time at which the database was last updated • `Version` - The version number • `Size` - The database's size • `CRC` - The database's CRC (Cyclic Redundancy Check) value for file verification
USB Device	Information about each connected USB device.
`Product`	The USB device's model.
`Manufacturer`	The USB device's manufacturer.
MAC Addresses	A list of the appliance's MAC addresses on each network interface.

EXAMPLE

Running this command results in information such as the following:

```
[700000] Device Information for gbw455.swbeta:

Hardware:
    Appliance Type:  SBox-200
    Version:         1.1G
General:
    Name:            gbw455.swbeta
    Uptime:          13 days, 12:45:57
    CPU Usage:       3%
    Flash Usage:     14%
License:
    MAC Address:     00:08:da:77:70:70
    Product Key:     8f8f8f-8f8f8f-8f8f8f
    Product Name:    Safe@Office 500WP, 25 nodes
    Used Nodes:      1
Firmware:
    Running:         8.0.19x
    Primary:         8.0.19x
    Backup:
    Bootcode:        19
    Debug Firmware:  No
Total Memory:
    Main:            50MB
    DFA:             Not Present
    DFA Test:        N/A
```

```
Free Memory:
    User:            911K
    Kernel:          1706K
    Firewall:        1518K
VStream Database:
    Main:            Mar 09, 2008 08:03 GMT. Version: 2.17.0   Size:
679881 bytes  CRC: 0x4a74817d
    Daily:           Mar 11, 2008 16:08 GMT. Version: 2.17.2   Size:
279854 bytes  CRC: 0xe57ec6be
USB Device 1:
    Product:         Generic USB Device
    Manufacturer:    ACME Corporation
MAC Addresses:
    WAN:             00:08:da:77:70:70
    DMZ/WAN2:        00:08:da:77:70:6f
    LAN:             00:08:da:77:70:6e
```

info dyn-obj

PURPOSE

The `info dyn-obj` command is used to display information about dynamic objects on your network. Dynamic objects can be downloaded from Check Point SmartLSM and referenced by the security policy.

SYNTAX

info dyn-obj

PARAMETERS

None.

RETURN VALUES

This command returns the number of dynamic objects on your network, followed by a list of dynamic objects.

The following information is displayed for each dynamic object:

`Num`	The dynamic object's number in the Dynamic Object table.
`Dynamic Object`	The dynamic object's IP address.
`Mapped Addresses`	The IP addresses to which the dynamic object is mapped.

EXAMPLE

Running this command results in information such as the following:

```
There are 1 dynamic objects installed


Num  Dynamic Object          Mapped Addresses
-----------------------------------------------------------------
1    0.0.0.1                 192.168.20.2-192.168.20.2
```

info fw rules

PURPOSE

The `info fw rules` command is used to display all firewall rules currently in effect, including:

- Implied firewall rules (rules applied before the user-defined rules)
- User-defined firewall rules
- Implied post firewall rules (rules applied after the user-defined rules)
- Virtual server rules
- Exposed host's IP address
- Firewall security level

SYNTAX

info fw rules [*setting*]

PARAMETERS

`setting`	String. The type of firewall setting to display. This can have the following values: • `exposed-host` - Exposed host's IP address • `implied-post-rules` - Implied post firewall rules • `implied-rules` - Implied firewall rules • `inspect-policy` - Firewall security level • `user-defined-rules` - User-defined firewall rules • `virtual-servers` - Virtual server rules If you do not include this parameter, all firewall settings are displayed.

RETURN VALUES

The returned firewall settings are grouped according to type.

For information on firewall rule fields, see ***fw rules*** on page 322. For information on virtual server rule fields, see ***fw servers*** on page 332. For information on exposed host and firewall security level fields, see ***fw*** on page 316.

EXAMPLE

Running this command results in information such as the following:

```
rules:
 implied-rules:
  1:
   service any
   action allow
   src gw
   dest any
   ports 0
   protocol any
   qosclass Default
   redirectport 0
   index 1
   log false
   disabled false
   description ""
   time always
...
```

```
 virtual-servers:
  web:
   hostip undefined
   enconly false

  ftp:
   hostip undefined
   enconly false
...
 user-defined-rules:
  1:
   service any
   action allow
   src laptop
   dest wan
   ports 0
   protocol any
   qosclass Default
   redirectport 0
   index 1
   log true
   disabled false
   description ""
   time always
...
```

```
 exposed-host:
   undefined

 implied-post-rules:
  1:
   service custom
   action allow
   src lan
   dest gw
   ports 53
   protocol udp
   qosclass Default
   redirectport 0
   index 1
   log false
   disabled false
   description ""
   time always
   disabled false
...

 inspect-policy:
   high
```

info ha

PURPOSE

The `info ha` command is used to display information about the appliance's current High Availability (HA) status.

SYNTAX

info ha

PARAMETERS

None.

RETURN VALUES

The following information is displayed:

`mode`	Indicates whether HA is enabled for the appliance. This can have the following values: • `enabled` - HA is enabled. • `disabled` - HA is disabled.
`sync-interface`	The network used as the synchronization interface.
`group-id`	The ID number of the HA cluster to which the gateway belongs.
`current-priority`	The gateway's current priority.
`base-priority`	The gateway's configured priority.

tracking	A list of Internet connections and appliance ports for which tracking is configured. Each Internet connection is followed by the amount to reduce the gateway's priority if the connection goes down, and the connection's current status (connected / disconnected). Each port is followed by the amount to reduce the gateway's priority if the port's Ethernet link is lost, and the port's current status (connected / disconnected).
status	
`state`	The gateway's current status. This can have the following values: • `master` - The gateway is the Active Gateway. • `backup` - The gateway is a Passive Gateway.
dependent-interfaces	
`wan1`	Indicates whether WAN HA is enabled for the primary Internet connection. This can have the following values: • `true` - WAN HA is enabled. • `false` - WAN HA is disabled.
`wan2`	Indicates whether WAN HA is enabled for the secondary Internet connection. This can have the following values: • `true` - WAN HA is enabled. • `false` - WAN HA is disabled.

EXAMPLE

Running this command results in information such as the following:

```
mode: enabled
sync-interface: lan
group-id: 55
current-priority: 40
base-priority: 50

tracking:
     wan1: 5, state: connected
     lan1: 10, state: disconnected

status:
     state: master

dependent-interfaces:
     wan1: false
     wan2: false
```

info load-balancing

PURPOSE

The `info load-balancing` command is used to display the distribution of traffic between the primary and secondary Internet connections.

SYNTAX

info load-balancing

PARAMETERS

None.

RETURN VALUES

`Load Balancing table`	The number of currently active source-destination pairs in the load balancing table.

The following information is displayed for each source-destination pair:

`src_ip`	The source IP address.
`dst_ip`	The destination IP address.
`isp`	The Internet connection to which the source-destination pair is assigned: • `wan1` - The primary Internet connection • `wan2` - The secondary Internet connection
`time`	The amount of time remaining (in seconds) until the source-destination pair will be removed from the load balancing table. This counter is reset each time traffic is passed between the pair.

EXAMPLE

Running this command results in information such as the following:

```
Load balancing table - 142 entries
src_ip          | dst_ip          | isp  | time
-------------------------------------------------
  192.168.10.14 |   66.230.115.66 | wan1 | 3590
  192.168.10.14 |  64.195.124.100 | wan1 | 3590
  192.168.10.14 |   12.208.67.187 | wan2 | 3589
  192.168.10.14 |  125.198.98.223 | wan1 | 3592
  192.168.10.14 |    77.31.240.55 | wan1 | 3593
  192.168.10.14 |  82.196.102.115 | wan2 | 3592
  ....
```

info logs event

PURPOSE

The `info logs event` command is used to display the Event Log. The Event Log lists general appliance events, including the date and the time that each event occurred.

SYNTAX

info logs event

PARAMETERS

None.

RETURN VALUES

The Event Log. The following information is displayed for each event:

Number	The log's number in the Event Log
Date	The date in the format: `day/month`
Time	The time in the format: `HH:MM:SS` where: `HH` = hours `MM` = minutes `SS` = seconds
`Log`	The log identification number

EXAMPLE

Running this command results in information such as the following:

```
Audit Logs:

00080   1/04 10:53:54 Log 60031: User admin logged in (Source
IP:192.168.10.21 Via:HTTP)

00079   1/04 09:53:31 Log 10015: Assigned 192.168.252.48 to
00:16:0a:00:1d:2e (feinerkids) via DHCP

00078   1/04 09:53:21 Log 10029: WLAN client 00:16:0A:00:1D:2E
associated to wlan network

00077   1/04 08:00:36 Log 40016: Successfully connected to the Service
Center

00076   1/04 08:00:34 Log 60038: Primary PPTP connection established,
IP address 89.138.21.153 assigned

00075   1/04 08:00:27 Log 60021: Failed to establish VPN tunnel with
194.90.1.5: N/A

00074   1/04 08:00:27 Log 60021: Failed to establish VPN tunnel with
194.90.1.5: N/A

...
```

info logs security

PURPOSE

The `info logs security` command is used to display the Security Log. The Security Log lists security-related events, including the date and the time that each event occurred, and its type.

SYNTAX

info logs security

PARAMETERS

None.

RETURN VALUES

The Security Log. The following information is displayed for each event:

Number	The log's number in the Event Log
Date	The date in the format: `day/month`
Time	The time in the format: `HH:MM:SS` where: `HH` = hours `MM` = minutes `SS` = seconds
`Log`	The log identification number and description of the logged event

The following additional information is displayed for logged connections:

`Src`	The source IP address
`SPort`	The source port
`Dst`	The destination IP address
`DPort`	The destination port
`IPP`	The IP protocol
`Rule`	The rule identification number. This can be any of the following: • A positive number - Indicates user -defined rules and default policy rules. • A negative number - Indicates an implied rule.
`Interface`	The network interface on which the connection was made

EXAMPLE

Running this command results in information such as the following:

```
Security Logs:

01446  25/03 11:17:18 Log 50017: www.yahoo.com/ from
192.168.10.21 was blocked by web rule no. 2

01445  25/03 11:08:45 Log 50000: Dropped Inbound packet (Policy
rule) Src:209.173.159.134 SPort:11684 Dst:89.138.72.55
DPort:33435 IPP:17 Rule:15 Interface:WAN (Internet)

01444  25/03 11:08:13 Log 50000: Dropped Inbound packet (Policy
rule) Src:89.138.197.197 SPort:22307 Dst:89.138.72.55
DPort:135 IPP:6 Rule:15 Interface:WAN (Internet)

01443  25/03 11:06:58 Log 50000: Accepted Outbound packet
(Custom rule) Src:192.168.252.48 SPort:1098
Dst:212.143.162.142 DPort:80 IPP:6 Rule:1 Interface:WLAN

01442  25/03 11:06:54 Log 50000: Accepted Outbound packet
(Custom rule) Src:192.168.252.48 SPort:1097 Dst:81.22.35.115
DPort:80 IPP:6 Rule:1 Interface:WLAN

...
```

info modem

PURPOSE

The `info modem` command is used to display information about 3G cellular modems attached to your appliance.

SYNTAX

info modem

PARAMETERS

None.

RETURN VALUES

`Manufacturer`	The modem manufacturer
`Model`	The modem model
`Revision`	The modem revision
`IMEI`	The modem serial number
`Operator`	The cellular operator
`Signal Str`	The current signal strength in dBm
`BER`	The bit error rate
`Access Technology`	The access technology used

EXAMPLE

Running this command results in information such as the following:

```
Manufacturer: huawei
Model: E176G
Revision: 11.126.03.00.170
IMEI: 357267023414133
Operator: IL ORANGE
Signal Str: -53 dBm
BER: Unknown
Access Technology: UMTS
```

info nat

PURPOSE

The `info nat` command is used to display the Network Address Translation (NAT) rules that are currently in effect, including:

- Hide NAT rules. Enables you to share a single public Internet IP address among several computers, by "hiding" the private IP addresses of the internal network computers behind the network's single Internet IP address.

  Hide NAT rules are implicitly defined when enabling Hide NAT for an internal network. For information, see ***net lan*** on page 387, ***net dmz*** on page 368, ***net wlan*** on page 442, and ***vlan*** on page 686.

  You can also configure custom Hide NAT rules. For information, see ***nat rules*** on page 362.

- Static NAT rules. Allows the mapping of Internet IP addresses or address ranges to hosts inside the internal network.

  Static NAT rules are implicitly defined when configuring Static NAT for a network object. For information, see ***netobj*** on page 465.

  You can also configure custom Static NAT rules. For information, see ***nat rules*** on page 362.

- Service-based NAT rules. Translation of a connection's original service to a different service.

  For information on configuring custom service-based NAT rules, see ***nat rules*** on page 362.

SYNTAX

info nat

PARAMETERS

None.

RETURN VALUES

`NAT Table`	The number of NAT rules.

The following information is displayed for each NAT rule:

Number	The NAT rule's number.
`original source`	The original source address. This can be the following: • An internal network • An IP address • An IP range • `any` - Any source
`original destination`	The original destination address. This can be the following: • An internal network • An IP address • An IP range • `any` - Any destination
`original ports`	The original port. This can be the following: • A port • A range of ports • `any` - Any port
`translated source`	The translated source address. This can be the following: • An internal network • An IP address • An IP range • `original` - The original source address (that is, the source address does not change)
`translated destination`	The translated destination address. This can be the following: • An internal network • An IP address • An IP range • `original` - The original destination (that is, the destination address does not change)

`translated ports`	The translated ports. This can be the following: • A port • A range of ports • `original` - The original port (that is, the port does not change)
`protocol`	The protocol to which the NAT rule applies. This can be the following: • `any` - The rule applies to all protocols. • `tcp` • `icmp` • `udp` • `gre` • `esp`
`type`	The type of NAT used. This can be the following: • `hide` - Hide NAT • `static` - Static NAT
`source`	The source of the NAT rule. This can be the following: • `local` - The rule was created locally, by configuring a custom NAT rule, an Allow & Forward rule, Hide NAT for an internal network, or Static NAT for a network object. • `management` - The rule was downloaded as part of a compiled security policy received from the remote management.

EXAMPLE

Running this command results in information such as the following:

```
NAT Table - 2 NAT rules
   1 :
    original source: lan
    original destination: any
    original ports: any
    translated source: 89.139.169.188
    translated destination: original
    translated ports: original
    protocol: any
    type: hide
    source: local

   2 :
    original source: wlan
    original destination: any
    original ports: any
    translated source: 89.139.169.188
    translated destination: original
    translated ports: original
    protocol: any
    type: hide
    source: local
```

info net

PURPOSE

The `info net` command is used to display information about your appliance's network interfaces and bridges.

SYNTAX

info net

PARAMETERS

None.

RETURN VALUES

The following information is displayed for each Internet connection:

`Type`	The Internet connection's type
`Status`	The Internet connection's status
`IP Address`	The appliance's current IP address on the network interface
`MAC Address`	The appliance's MAC address on the network interface
Internet	
`Mode`	The Internet connection method used
`Connected`	The connection duration, in the format hh:mm:ss, where: hh=hours mm=minutes ss=seconds
`Remote IP Address`	The IP address of the PPP peer. This field is only relevant for PPPoE and PPPoE Internet connections.

Connection Probing	
Probing Method	The connection probing method configured for the Internet connection
ADSL	These fields only appear for ADSL connections.
`Standard`	The DSL line's standard
`Annex`	The Embedded NGX ADSL model (Annex A, Annex B)
`Self Test`	Indicates whether DSL modem has passed a self-test
`Trellis Coding`	The DSL line's trellis coding
`Framing Structure`	The DSL line's framing structure
`Line Rate`	The line rate for transmission (TX) and reception (RX) in kbps
`ADSL Firmware`	The installed ADSL firmware
`ADSL Firmware [Backup]`	The installed backup ADSL firmware
RF status	These fields only appear for ADSL connections.
Tx Power	The local and remote transmission power in dB
SNR Margin	The local and remote Signal to Noise Ration (SNR) margin in dB. The SNR margin is the difference between the amount of noise received by the by the local/remote line end, and the amount of noise it can tolerate.

Line Attenuation	The local and remote line attenuation in dB. The line attenuation is the difference between the signal power transmitted to the local/remote line end, and that which it received.
Statistics	Statistics only appear if the Internet connection is connected
`Packets`	The total number of transmitted and received packets
`Errors`	The total number of transmitted and received packets for which an error occurred
`Dropped`	The total number of transmitted and received packets that the firewall dropped
`Overruns`	The total number of transmitted and received packets that were lost, because they were sent or arrived more quickly that the appliance could handle
`Frame/Carrier`	The total number of frame alignment and carrier errors. Frame alignment errors occur when a frame that has extra bits is received. The number of such errors appears in the Received column. Carrier errors occur when the carrier is not present at the start of data transmission, or when the carrier is lost during transmission. Such errors usually indicate a problem with the cable. The number of such errors appears in the Transmitted column.

The following information is displayed for each wired network:

`Type`	The network's type.
`Status`	The network's current status. This can have the following values: • `Enabled` • `Disabled`
`IP Address`	The appliance's current IP address on the network interface.
`MAC Address`	The appliance's MAC address on the network interface. This field does not appear for the OfficeMode network.
Statistics	Statistics only appear if the network is enabled.
`Packets`	The total number of transmitted and received packets.
`Errors`	The total number of transmitted and received packets for which an error occurred.
`Dropped`	The total number of transmitted and received packets that the firewall dropped.
`Overruns`	The total number of transmitted and received packets that were lost, because they were sent or arrived more quickly that the appliance could handle.

Frame/Carrier	The total number of frame alignment and carrier errors. Frame alignment errors occur when a frame that has extra bits is received. The number of such errors appears in the Received column. Carrier errors occur when the carrier is not present at the start of data transmission, or when the carrier is lost during transmission. Such errors usually indicate a problem with the cable. The number of such errors appears in the Transmitted column.

The following information is displayed for each wireless network:

Type	The network's type, in this case "Wireless"
Status	The network's current status. This can have the following values: • Enabled • Disabled
IP Address	The IP address of the wireless network's default gateway
MAC Address	The MAC address of the wireless network interface
Wireless	
Wireless Mode	The operation mode used by the WLAN, followed by the transmission rate in Mbps
Domain	The Embedded NGX access point's region
Country	The country configured for the WLAN
Channel	The radio frequency used by the WLAN
Security	The security mode used by the wireless network

Statistics	Statistics only appear if the network is enabled
`Frames OK`	The total number of frames that were successfully transmitted and received
`Errors`	The total number of transmitted and received frames for which an error occurred
`Wrong NWID/ESSID`	The total number of received packets that were dropped, because they were destined for another access point
`Invalid Encryption Key`	The total number of transmitted and received packets with the wrong encryption key
`Missing Fragments`	The total number of packets missed during transmission and reception that were dropped, because fragments of the packet were lost
`Discarded Retries`	The total number of discarded retry packets that were transmitted and received
`Discarded Misc`	The total number of transmitted and received packets that were discarded for other reasons

The following information is displayed for each bridge:

`Type`	The network's type, in this case "Bridge"
`IP Address`	The appliance's current IP address on the bridge interface
Statistics	Statistics only appear if the bridge is enabled
`Packets`	The total number of transmitted and received packets
`Errors`	The total number of transmitted and received packets for which an error occurred

Dropped	The total number of transmitted and received packets that the firewall dropped
Overruns	The total number of transmitted and received packets that were lost, because they were sent or arrived more quickly that the appliance could handle
Frame/Carrier	The total number of frame alignment and carrier errors. Frame alignment errors occur when a frame that has extra bits is received. The number of such errors appears in the Received column. Carrier errors occur when the carrier is not present at the start of data transmission, or when the carrier is lost during transmission. Such errors usually indicate a problem with the cable. The number of such errors appears in the Transmitted column.

EXAMPLE

Running this command results in information such as the following:

```
Primary Internet
Type                        Ethernet
Status                      Connected
IP Address                  89.138.72.55
MAC Address                 00:0c:6e:41:5d:6a
Internet
Mode                        PPTP
Connected                   0 days, 00:44:48
Remote IP Address           212.143.205.229
Connection Probing
Probing Method              None
Statistics
                          Receive                   Transmit
Packets                   27126                     14510
Errors                    0                         0
Dropped                   0                         0
Overruns                  0                         0
Frame/Carrier             0                         0
...
```

info ospf

PURPOSE

The `info ospf` command is used to display general information about your appliance's OSPF settings.

SYNTAX

info ospf

PARAMETERS

None.

RETURN VALUES

General OSPF information.

EXAMPLE

Running this command results in information such as the following:

```
     OSPF Routing Process, Router ID: 212.150.8.77
 Supports only single TOS (TOS0) routes
 This implementation conforms to RFC2328
 RFC1583Compatibility flag is disabled
 OpaqueCapability flag is disabled
 Stub router advertisement is configured
   Enabled for 2s prior to full shutdown
 Initial SPF scheduling delay 200 millisec(s)
 Minimum hold time between consecutive SPFs 1000 millisec(s)
 Maximum hold time between consecutive SPFs 10000 millisec(s)
 Hold time multiplier is currently 1
 SPF algorithm has not been run
 SPF timer is inactive
 Refresh timer 10 secs
 Number of external LSA 0. Checksum Sum 0x00000000
 Number of opaque AS LSA 0. Checksum Sum 0x00000000
 Number of areas attached to this router: 0
```

info ospf database

PURPOSE

The `info ospf database` command is used to display information about the OSPF link-state database.

SYNTAX

info ospf database

PARAMETERS

None.

RETURN VALUES

Information about reported link states.

EXAMPLE

Running this command results in information such as the following:

```
       OSPF Router with ID (62.90.32.158)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
62.90.32.158    62.90.32.158     569 0x80000005 0x65da 1
192.168.10.3    192.168.10.3     630 0x80000005 0xfb66 1
192.168.10.4    192.168.10.4     631 0x80000006 0xfa62 1
192.168.10.10   192.168.10.10    634 0x80000005 0x0629 1
192.168.10.11   192.168.10.11    570 0x80000008 0xe85d 1

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
192.168.10.11   192.168.10.11    570 0x80000004 0x24e8
```

```
                Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Route
1.1.2.0         192.168.10.4    1053 0x80000001 0x36a1 1.1.2.0/24
10.0.0.0        192.168.10.11      3 0x80000002 0xb613 10.0.0.0/24

                ASBR-Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
# 62.90.32.131    192.168.10.4     997 0x80000001 0x6d31

                Router Link States (Area 2.2.2.2)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
62.90.32.158    62.90.32.158     590 0x80000001 0xeac9 0

                AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route
0.0.0.0         62.90.32.131     999 0x80000001 0x0120 E1 0.0.0.0/0
[0x0]
0.0.0.0         192.168.10.3    1090 0x80000001 0xb2bd E2 0.0.0.0/0
[0x0]
0.0.0.0         192.168.10.4    1057 0x80000001 0xa34e E2 0.0.0.0/0
[0x0]
62.90.32.0      192.168.10.3     634 0x80000004 0x7a12 E2
62.90.32.0/24 [0x0]
```

info ospf interface

PURPOSE

The `info ospf interface` command is used to display the status and OSPF settings of each network interface and VTI (Virtual Tunnel Interface).

SYNTAX

info ospf interface

PARAMETERS

None.

RETURN VALUES

OSPF information for each network interface and VIT.

EXAMPLE

Running this command results in information such as the following:

```
lan is up
  ifindex 9, MTU 1500 bytes, BW 0 Kbit
<UP,BROADCAST,RUNNING,MULTICAST>
  Internet Address 192.168.10.101/24, Broadcast 192.168.10.255, Area
0.0.0.0
  MTU mismatch detection:enabled
  Router ID 192.168.10.101, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.10.101, Interface Address
192.168.10.101
  No backup designated router on this network
  Multicast group memberships: OSPFAllRouters OSPFDesignatedRouters
  Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit
5
    Hello due in 7.952s
  Neighbor Count is 0, Adjacent neighbor count is 0
wan is up
  ifindex 3, MTU 1500 bytes, BW 0 Kbit
<UP,BROADCAST,RUNNING,MULTICAST>
  OSPF not enabled on this interface
dmz is up
  ifindex 4, MTU 1500 bytes, BW 0 Kbit   <UP,BROADCAST,MULTICAST>
  OSPF not enabled on this interface
```

info ospf neighbor

PURPOSE

The `info ospf neighbor` command is used to display information about your appliance's OSPF neighbors.

SYNTAX

info ospf neighbor

PARAMETERS

None.

RETURN VALUES

A list of OSPF neighbors. The information provided for each OSPF neighbor includes the following:

`Neighbor ID`	The OSPF neighbor's router ID.
`Dead Time`	The interval of time in seconds after which the OSPF neighbor will be considered "dead", if it does not communicate in any way.
`Interface`	The Embedded NGX appliance's IP address used for communicating with this neighbor.

EXAMPLE

Running this command results in information such as the following:

```
Neighbor ID Pri State          Dead Time Address      Interface
RXmtL RqstL DBsmL

192.168.10.3  1 Full/DROther  34.231s 192.168.10.3
lan:192.168.10.101  0     0     0

192.168.10.4  1 Full/DROther  34.234s 192.168.10.4
lan:192.168.10.101  0     0     0

192.168.10.10 1 Full/DROther  33.112s 192.168.10.10
lan:192.168.10.101  0     0     0

192.168.10.11 1 Full/Backup   34.230s 192.168.10.11
lan:192.168.10.101  0     0     0
```

info ospf routes

PURPOSE

The `info ospf routes` command is used to display information about OSPF routes.

SYNTAX

info ospf routes

PARAMETERS

None.

RETURN VALUES

A list of OSPF-related routes. Each route is marked with a code that indicates its type. The Embedded NGX appliance supports the following route types:

K	A kernel route. Kernel routes are routes that are recognized by the OSPF daemon via the kernel. For example, a static route.
C	A connected route. Connected routes are routes that are created for each new network defined on the Embedded NGX appliance. For example, LAN.
S	A static route defined by the user.
R	A RIP route.
O	An OSPF route. OSPF routes are routes learned via OSPF.
I	An ISIS route.
B	A BGP route. BGP routes are learned via BGP.
>	A selected route.

EXAMPLE

Running this command results in information such as the following:

```
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

K>* 0.0.0.0/0 via 212.143.205.164, ppp0
C>* 127.0.0.0/8 is directly connected, lo
C>* 172.27.144.0/20 is directly connected, wan
C>* 192.168.10.0/24 is directly connected, lan
C>* 192.168.252.0/24 is directly connected, wlan
C>* 192.168.254.1/32 is directly connected, lo
C>* 212.143.205.164/32 is directly connected, ppp0
K>* 212.143.205.253/32 via 172.27.144.1, wan
```

info ports

PURPOSE

The `info ports` command is used to display the status of the Embedded NGX appliance's ports, including each Ethernet connection's duplex state. This is useful if you need to check whether the appliance's physical connections are working, and you cannot see the LEDs on front of the appliance.

SYNTAX

info ports

PARAMETERS

None.

RETURN VALUES

A list of the enabled ports, including their statuses, security schemes, and assignments.

The following information is displayed for each port:

Status	The port's current status. This can be the following: `speed: mode: -` The current link speed (10 Mbps or 100 Mbps) and duplex (Full Duplex or Half Duplex) `no link -` Indicates that the appliance does not detect anything connected to the port
`security`	The port's security scheme. This can be the following: • `none -` No security scheme is defined for the port. • `802.1x -` An 802.1x security scheme is defined for the port.
`802.1x`	The port's security status. This can be the following: • `N/A -` No security scheme is defined for the port. • `unauthorized -` An 802.1x security scheme is defined for the port. Users have not yet connected to the port and attempted to authenticate, *or* a user failed to authenticate and no Quarantine network is configured.

- `authorized (network)` - An 802.1x security scheme is defined for the port. A user connected to the port, authenticated successfully, and was assigned to a network. The name of the assigned network appears in parentheses.
- `quarantine (network)` - An 802.1x security scheme is defined for the port. A user connected to the port, failed to authenticate, and was assigned to the Quarantine network. The name of the Quarantine network appears in parentheses.

`assigned-to`

The network or purpose to which the port is currently assigned.

This can be the following:

- `internet` - The port is assigned to a WAN Internet connection.
- A specific network
- `none` - The port is disabled.

If the port is configured for dynamic VLAN assignment, this field does not appear.

EXAMPLE

Running this command results in information such as the following:

```
     info ports
wan:
     speed: 100 Mbps mode: full duplex
     security: none
     802.1x: N/A
     assigned-to: internet
dmz/wan2:
     no link
     security: none
     802.1x: N/A
     assigned-to: dmz
lan 1:
     speed: 100 Mbps mode: full duplex
     security: none
     802.1x: N/A
     assigned-to: lan
lan 2:
     no link
     security: none
     802.1x: N/A
     assigned-to: lan
```

```
lan 3:
     no link
     security: 802.1x
     802.1x: unauthorized
lan 4:
     no link
     security: none
     802.1x: N/A
     assigned-to: lan
```

info probe

PURPOSE

The `info probe` command is used to display connection probing results for the primary and secondary Internet connections on specific ports. Connection probing is a way to detect Internet failures that are more than one hop away.

To generate information for this report, you must configure connection probing for the desired port. While the primary Internet connection uses the WAN port, the secondary Internet connection can use either the WAN port or the WAN2 port, depending on your Embedded NGX appliance's configuration. For information on configuring connection probing for the WAN port, see ***net wan probe*** on page 425. For information on configuring connection probing for the WAN2 port, see ***net wan2 probe*** on page 439.

SYNTAX

info probe

PARAMETERS

None.

RETURN VALUES

For each configured Internet connection, the following information is displayed:

- The connection probing method used. This can be the following:

`DNS`	This method probes the primary and secondary DNS servers.
`PING`	This method pings anywhere from one to three servers.
`RDP`	This method sends RDP echo requests to up to three Check Point VPN gateways.

- The Internet connection's status, as determined by the probing a specific server. This can be the following:

UP	Probing the server succeeded.
DOWN	Probing the server failed for 45 seconds.

  If probing failed for all listed servers (all statuses are DOWN), then the Internet connection is considered to be down.

- The IP address or DNS name of the probed server.

EXAMPLE

Running this command results in information such as the following:

```
wan1:
     DNS:  UP:   194.90.1.5
     DNS:  DOWN: 212.143.212.143
```

In this example, one DNS server responded to probing within 45 seconds, and the Internet connection is therefore up.

info rip

PURPOSE

The info rip command is used to display general information about your appliance's RIP settings.

This command is only relevant for N series appliances.

SYNTAX

info rip

PARAMETERS

None.

RETURN VALUES

General RIP information.

EXAMPLE

Running this command results in information such as the following:

```
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) - redistribute,
      (i) - interface

     Network            Next Hop         Metric From            Tag
Time
C(i) 6.6.6.6/32         0.0.0.0               1 self             0
C(i) 192.168.10.0/24    0.0.0.0               1 self             0
R(n) 192.168.20.0/24    5.5.5.5               2 5.5.5.5          0
59:52
```

info rip routes

PURPOSE

The `info rip routes` command is used to display information about RIP routes.

This command is only relevant for N series appliances.

SYNTAX

info rip routes

PARAMETERS

None.

RETURN VALUES

A list of RIP-related routes. Each route is marked with a code that indicates its type. The Embedded NGX appliance supports the following route types:

K	A kernel route. Kernel routes are routes that are recognized by the RIP daemon via the kernel. For example, a static route.
C	A connected route. Connected routes are routes that are created for each new network defined on the Embedded NGX appliance. For example, LAN.
S	A static route defined by the user.
R	A RIP route.
O	An OSPF route. OSPF routes are routes learned via OSPF.
I	An ISIS route.
B	A BGP route. BGP routes are learned via BGP.

>	A selected route.

EXAMPLE

Running this command results in information such as the following:

```
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

K>* 0.0.0.0/0 via 80.90.32.1, wan
C>* 5.5.5.5/32 is directly connected, VPN_52
C>* 80.90.32.0/24 is directly connected, wan
C>* 127.0.0.0/8 is directly connected, lo
C>* 192.168.10.0/24 is directly connected, lan
R>* 192.168.20.0/24 [120/2] via 5.5.5.5, VPN_52, 00:00:47
C>* 192.168.254.1/32 is directly connected, lo
```

info rip status

PURPOSE

The `info rip status` command is used to display a summary of your appliance's RIP settings.

This command is only relevant for N series appliances.

SYNTAX

info rip status

PARAMETERS

None.

RETURN VALUES

A summary of your appliance's RIP settings.

EXAMPLE

Running this command results in information such as the following:

```
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in -1288184556
seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive any version
    Interface        Send  Recv   Key-chain
    eth0             2     1 2
    vpnt0            2     1 2
  Routing for Networks:
    6.6.6.6/32
    192.168.10.0/24
  Routing Information Sources:
    Gateway          BadPackets BadRoutes  Distance Last Update
    5.5.5.5                   0         0       120   00:00:22
  Distance: (default is 120)
```

info routes

PURPOSE

The `info routes` command is used to display the routing table currently in effect on the Embedded NGX appliance.

SYNTAX

info routes

PARAMETERS

None.

RETURN VALUES

The following information is displayed for each route:

`Source`	The route's source
`Destination`	The route's destination
`Service`	The network service for which the route is configured
`Gateway`	The gateway's IP address
`Metric`	The route's metric
`Interface`	The interface for which the route is configured
`Origin`	The route's type: • `connected-route` - A route to a network that is directly connected to the Embedded NGX appliance • `static-route` - A destination-based or service-based static route. See ***routes*** on page 549. • `dynamic-route` - A route obtained through a dynamic routing protocol, such as OSPF • `source-route` - A source-based static route. See See ***routes*** on page 549.

EXAMPLE

Running this command results in information such as the following:

```
       info routes
Source              Destination         Service Gateway          Metric Interface Origin

-------------------------------------------------------------------------------------------

Any                 212.143.205.167/32   Any      NA               0      none
connected-route
Any                 212.143.205.253/32   Any      172.24.192.1     0      wan       static-route
Any                 192.168.252.0/24     Any      NA               0      wlan
connected-route
Any                 192.168.10.0/24      Any      NA               0      lan
connected-route
Any                 172.24.192.0/19      Any      NA               0      wan
connected-route
Any                 default              Any      212.143.205.167 99      none      static-route
```

info security-zones

PURPOSE

The `info security-zone` command is used to display information about security zones on your network. Security zones can be downloaded from Check Point SmartLSM and referenced by the security policy.

SYNTAX

info security-zones

PARAMETERS

None.

RETURN VALUES

This command returns the number of security zones on your network, followed by a list of security zones.

The following information is displayed for each security zone:

`Num`	The security zone's number in the Security Zones table.
`Interface Name`	The network interface to which the security zone is mapped.
`Zone`	The security zone's name.
`Bogus IP`	The security zone's IP address.

EXAMPLE

Running this command results in information such as the following:

```
There are 5 security zones installed

Num Interface Name Zone            Bogus IP
-----------------------------------------------------------------
1   lan            InternalZone    0.0.0.4
2   vlan1          vlan1           0.0.0.6
3   vlan2          vlan2           0.0.0.7
4   dmz            DMZZone         0.0.0.2
5   wan            ExternalZone    0.0.0.3
```

info services

PURPOSE

The `info services` command is used to display information about your service subscription.

SYNTAX

info services

PARAMETERS

None.

RETURN VALUES

`Services`	The gateway's subscription services status. This can be one of the following: • `Not Subscribed` - You are not subscribed to security services. • `Connection Failed` - The Embedded NGX appliance failed to connect to the Service Center. • `Connecting` - The Embedded NGX appliance is connecting to the Service Center. • `Connected` - You are connected to the Service Center, and security services are active.
`Gateway ID`	Your gateway ID.
`Base Server 1`	The primary base server's IP address.
`Base Server 2`	The secondary base server's IP address.
`Current Server 1`	The current primary server's IP address.
`Current Server 2`	The current secondary server's IP address.

`Setup Update Interval`	The interval of time between software updates, in the format: `HH:MM:SS` where: `HH` = hours `MM` = minutes `SS` = seconds
`Time Since Last Setup Response`	The amount of time since the gateway checked for software updates, in the format: `HH:MM:SS` where: `HH` = hours `MM` = minutes `SS` = seconds
`Logging Rate Limit`	The amount of time within which the gateway can send up to one logging packet to the Service Center, in the format: `HH:MM:SS` where: `HH` = hours `MM` = minutes `SS` = seconds For example, if the logging rate is 00:05:00, the gateway can send up to one packet every five minutes.
`Download Status`	The gateway download status. This can be one of the following: • `Downloading` - The gateway is currently downloading data from the Service Center. • `Not downloading` - The gateway is not downloading data from the Service Center.

This is followed by a list of services available in your service plan. For each service, the following information appears:

Subscription status	The status of your subscription to the service. This can be one of the following: • `Subscribed` • `Not Subscribed`
Service status	The status of the service. This can be one of the following: • `Connected` - You are connected to the service through the Service Center. • `Connecting` - Connecting to the Service Center. • `N/A` - The service is not available.
Service mode	The mode to which the service is set. If you are subscribed to Dynamic DNS, your gateway's domain name appears. For further information, see ***webfilter*** on page 796, ***mailfilter antispam*** on page 356, and ***mailfilter antivirus*** on page 358.

EXAMPLE

Running this command results in information such as the following:

```
Services:  Connected
 Gateway ID: gbw455
 Base Server 1: 192.114.68.116
 Base Server 2: 212.150.2.131
 Current Server 1: 192.114.68.116
 Current Server 2: 212.150.2.131
 Setup Update Interval: 01:00:00
 Time Since Last Setup Response: 00:47:46
 Logging Rate Limit: 00:05:00
 Download Status: Not downloading
 Software Updates: Subscribed  Connected  Automatic
 Remote Management: Subscribed  Connected
 Web Filtering: Subscribed  Connected  On
 Email Antivirus: Subscribed  Connected  On
 Email Antispam: Subscribed  Connected  On
 VStream Antivirus Signature Updates: Subscribed  Connected
 Dynamic DNS: Subscribed  Connected  gbw455.mysofaware.net
 Dynamic VPN: Not Subscribed  N/A
 Logging Reporting: Subscribed  Connected
 Vulnerability Scan: Not Subscribed  N/A
```

info statistics

PURPOSE

The `info statistics` command enables you to view Traffic Monitor reports for incoming and outgoing traffic for all enabled network interfaces, bridges, and QoS classes. This enables you to identify network traffic trends and anomalies, and to fine tune Traffic Shaper QoS class assignments.

For information on displaying traffic reports for specific traffic types on specific network interfaces, see ***info statistics interface*** on page 193. For information on displaying traffic reports for specific traffic types on specific bridges, see ***info statistics bridge*** on page 191. For information on displaying traffic reports for specific QoS classes, see ***info statistics qos*** on page 195.

SYNTAX

info statistics

PARAMETERS

None.

RETURN VALUES

A list of traffic reports for all currently enabled networks and bridges. For example, if the DMZ network is enabled, it will appear in the list. If Traffic Shaper is enabled, the list also includes the defined QoS classes.

Each traffic report row displays traffic rates in kilobits/second for a specific interval of time. If desired, you can change this interval. For information, see ***statistics*** on page 660.

The following information is displayed in each row:

`Time`	The interval's start and end time, in the format: `HH:MM:SS-HH:MM:SS` where `HH` = hours `MM` = minutes `SS` = seconds
`Incoming`	The rate of incoming traffic in kilobits/second.
`Outgoing`	The rate of outgoing traffic in kilobits/second.

EXAMPLE

Running this command results in information such as the following:

```
Interfaces Traffic Report:
wan Interface (Total Traffic):
       Time          Incoming (kbits/seconds)    Outgoing
(kbits/seconds)
13:29:32-13:59:32               15                          1
13:59:32-14:29:32                2                          2
14:29:32-14:59:32                1                          0
14:59:32-15:29:32                3                          1
15:29:32-15:59:32               11                          0
...
```

```
lan Interface (Total Traffic):
       Time          Incoming (kbits/seconds)    Outgoing
(kbits/seconds)
07:59:32-08:29:32               0                         1
08:29:32-08:59:32               0                         4
08:59:32-09:29:32               0                         2
09:29:32-09:59:32               0                         2
09:59:32-10:29:32               0                        11
...

Bridges Traffic Report:
Bridge Bridge1 (Total Traffic):
       Time          Incoming (kbits/seconds)    Outgoing
(kbits/seconds)
13:29:32-13:59:32              15                         1
13:59:32-14:29:32               2                         2
14:29:32-14:59:32               1                         0
...

QoS Traffic Report:
Class Default (Total Traffic):
       Time          Incoming (kbits/seconds)    Outgoing
(kbits/seconds)
03:29:32-03:59:32               15                        11
03:59:32-04:29:32               1                         4
04:29:32-04:59:32               11                        19
04:59:32-05:29:32               0                         3
05:29:32-05:59:32               0                         15
...
```

info statistics bridge

PURPOSE

The `info statistics bridge` command enables you to view Traffic Monitor reports for specific types of traffic on specific bridges. This enables you to identify bridge traffic trends and anomalies.

Note: The firewall blocks broadcast packets used during the normal operation of your network. This may lead to a certain amount of blocked traffic that appears under normal circumstances and usually does not indicate an attack.

SYNTAX

info statistics bridge [*bridge type*]

PARAMETERS

`bridge`	String. The name of the bridge for which to display traffic statistics. If you do not include this parameter (together with the `type` parameter), information is displayed for all bridges.
`type`	String. The type of traffic to display. This can have the following values: • `allowed` - Allowed traffic • `blocked` - Blocked traffic • `encrypted` - Encrypted traffic • `total` - All traffic

RETURN VALUES

Reports for the specified type of traffic on the specified bridges.

Each traffic report row displays traffic rates in kilobits/second for a specific interval of time. If desired, you can change this interval. For information, see ***statistics*** on page 660.

The following information is displayed in each row:

`Time`	The interval's start and end time, in the format: `HH:MM:SS-HH:MM:SS` where `HH` = hours `MM` = minutes `SS` = seconds
`Incoming`	The rate of incoming traffic in kilobits/second.
`Outgoing`	The rate of outgoing traffic in kilobits/second.

EXAMPLE

Running the following command:

```
info statistics bridge Bridge1 allowed
```

Results in information such as the following:

```
Bridges Traffic Report:
Bridge Bridge1 (Allowed Traffic):
       Time          Incoming (kbits/seconds)    Outgoing
(kbits/seconds)
04:01:34-04:31:34               0                          4
04:31:34-05:01:34               0                          11
05:01:34-05:31:34               23                         0
05:31:34-06:01:34               0                          0
06:01:34-06:31:34               2                          0
...
```

info statistics interface

PURPOSE

The `info statistics interface` command enables you to view Traffic Monitor reports for specific types of traffic on specific network interfaces. This enables you to identify network traffic trends and anomalies.

Note: The firewall blocks broadcast packets used during the normal operation of your network. This may lead to a certain amount of blocked traffic that appears under normal circumstances and usually does not indicate an attack.

SYNTAX

info statistics interface [*interface type*]

PARAMETERS

`interface`	String. The network interface for which to display traffic statistics. If you do not include this parameter (together with the `type` parameter), information is displayed for all network interfaces.
`type`	String. The type of traffic to display. This can have the following values: • `allowed` - Allowed traffic • `blocked` - Blocked traffic • `encrypted` - Encrypted traffic • `total` - All traffic

RETURN VALUES

Reports for the specified type of traffic on the specified interfaces.

Each traffic report row displays traffic rates in kilobits/second for a specific interval of time. If desired, you can change this interval. For information, see ***statistics*** on page 660.

The following information is displayed in each row:

`Time`	The interval's start and end time, in the format: `HH:MM:SS-HH:MM:SS` where `HH` = hours `MM` = minutes `SS` = seconds
`Incoming`	The rate of incoming traffic in kilobits/second.
`Outgoing`	The rate of outgoing traffic in kilobits/second.

EXAMPLE

Running the following command:

```
info statistics interface lan blocked
```

Results in information such as the following:

```
Interfaces Traffic Report:
lan Interface (Dropped Traffic):
       Time          Incoming (kbits/seconds)    Outgoing
(kbits/seconds)
04:01:34-04:31:34               0                        4
04:31:34-05:01:34               0                        11
05:01:34-05:31:34               23                       0
05:31:34-06:01:34               0                        0
06:01:34-06:31:34               2                        0
...
```

info statistics qos

PURPOSE

The `info statistics qos` command enables you to view Traffic Monitor reports for specific QoS classes, when Traffic Shaper is enabled. This enables you to fine tune Traffic Shaper QoS class assignments.

SYNTAX

info statistics qos [class *class*]

PARAMETERS

`class`	String. The QoS class for which to display traffic statistics. If you do not include this parameter, information is displayed for all QoS classes.

RETURN VALUES

Traffic reports for the specified type of QoS class.

Each traffic report row displays traffic rates in kilobits/second for a specific interval of time. If desired, you can change this interval. For information, see ***statistics*** on page 660.

The following information is displayed in each row:

`Time`	The interval's start and end time, in the format: `HH:MM:SS-HH:MM:SS` where `HH` = hours `MM` = minutes `SS` = seconds
`Incoming`	The rate of incoming traffic in kilobits/second.
`Outgoing`	The rate of outgoing traffic in kilobits/second.

EXAMPLE

Running the following command:

```
info statistics qos class Urgent
```

Results in information such as the following:

```
QoS Traffic Report:
Class Urgent (Total Traffic):
       Time          Incoming (kbits/seconds)    Outgoing
(kbits/seconds)
04:09:50-04:39:50               1                        10
04:39:50-05:09:50               8                        0
05:09:50-05:39:50               3                        3
05:39:50-06:09:50               0                        5
06:09:50-06:39:50               9                        7
...
```

info terminal-server

PURPOSE

The `info terminal-server` command is used to display the terminal server's current status.

This command is only relevant for models with a built-in terminal server.

SYNTAX

info terminal-server

PARAMETERS

None.

RETURN VALUES

`Status`	The terminal server's status: • `off` - The terminal server is disabled. • `waiting` - The terminal server is enabled, and no device is attached. • `connected` - The terminal server is enabled, and a device is attached. • `terminating` - The terminal server is restarting.

EXAMPLE

Running this command results in information such as the following:

```
status:
connected
```

info usb

PURPOSE

The `info usb` command is used to display information about connected USB modems, printers, and storage devices. For information on displaying USB modem details only, see ***info usb modem*** on page 199. For information on displaying printer details only, see ***info usb printers*** on page 201. For information on displaying storage device details only, see ***info usb storage*** on page 203.

Displaying printer details is only relevant for models supporting a print server.

SYNTAX

info usb

PARAMETERS

None.

RETURN VALUES

For examples of returned information, see ***info usb modem*** on page 199, ***info usb printers*** on page 201, and ***info usb storage*** on page 203.

info usb modems

PURPOSE

The `info usb modems` command is used to display information about connected USB modems.

SYNTAX

info usb modems

PARAMETERS

None.

RETURN VALUES

The following information is displayed for each USB modem:

`Vendor name`	The manufacturer of the modem.
`Product name`	The model of the modem.
`Serial number`	The serial number of the modem.
`Status`	The modem's status. A modem can have the following statuses: • `Not Present` - No USB modem is detected. • `Idle` - The USB modem is detected, but it is not in use. • `Connected` - The USB modem is connected to the Internet.

EXAMPLE

Running this command results in information such as the following:

```
usb:
 modems:
Vendor name  : Silicon Labs
Product name : CP2102 USB to UART Bridge
Serial number: 0001
Status       : Ready
```

info usb printers

PURPOSE

The `info usb printers` command is used to display information about your printers, such as their statuses and the ports used, and additional details.

This command is only relevant for models supporting a print server.

SYNTAX

info usb printers

PARAMETERS

None.

RETURN VALUES

The following information is displayed for each printer:

`Vendor name`	The manufacturer of the printer.
`Product name`	The model of the printer.
`Serial number`	The serial number of the printer.
`TCP Port`	The TCP port used by the print server for this printer.
`Pending Jobs`	The number of print jobs in queue for the printer.
`Status`	The printer's status. A printer can have the following statuses: • `Initialize` - The printer is initializing. • `Ready` - The printer is ready. • `Not Ready` - The printer is not ready. For example, it may be out of paper. • `Printing` - The printer is processing a print job. • `Restarting` - The print server is restarting. • `Fail` - An error occurred. See the Event Log for details.

EXAMPLE

Running this command results in information such as the following:

```
usb:
 printers:
Vendor name  : Hewlett-Packard
Product name : PSC 2100 Series
Serial number: MY31TF62YJ0F
TCP Port     : 9100
Pending Jobs : 0
Status       : Ready
```

info usb storage

PURPOSE

The `info usb storage` command is used to display information about connected USB flash drives.

SYNTAX

info usb storage

PARAMETERS

None.

RETURN VALUES

The following information is displayed for each USB flash device:

`Vendor name`	The manufacturer of the device.
`Product name`	The model of the device.
`Serial number`	The serial number of the device.

EXAMPLE

Running this command results in information such as the following:

```
     info usb storage
Vendor name   : SanDisk
Product name  : U3 Cruzer Micro
Serial number : 0875710C4841D5A1
```

info vpn

PURPOSE

The `info vpn` command enables you to view information about the current VPN topology, split DNS mappings, trusted certificate authorities (CAs), MEP configuration, and established tunnels.

For information on displaying the VPN sites topology only, see ***info vpn sites*** on page 207. For information on displaying split DNS mappings only, see ***info vpn split-dns*** on page 209. For information on displaying trusted CAs only, see ***info vpn trusted-ca*** on page 211. For information on displaying MEP configuration only, see ***info vpn mep*** on page 205. For information on displaying VPN tunnels only, see ***info vpn tunnels*** on page 212.

SYNTAX

info vpn

PARAMETERS

None.

RETURN VALUES

For examples of returned information, see ***info vpn mep*** on page 205, ***info vpn sites*** on page 207, ***info vpn split-dns*** on page 209, ***info vpn trusted-ca*** on page 211, and ***info vpn tunnels*** on page 212.

info vpn mep

PURPOSE

The `info vpn mep` command enables you to view information about Multiple Entry Point (MEP) VPN communities, in which multiple VPN gateways are configured to access the same destination address.

SYNTAX

info vpn mep

PARAMETERS

None.

RETURN VALUES

The following information is displayed for each MEP community:

number	The MEP community's index number.
`group-id`	The MEP community's ID.
`mechanism`	The MEP mechanism used for this community. This can be any of the following: • `First-to-respond` - Open a VPN tunnel to the first gateway that responds. • `Load-balancing` - Open a VPN tunnel to any gateway that responds, (regardless of the response time). • `Unknown` - The MEP mechanism is unknown.
`chosen-gateway`	The gateway to which all gateways in this community should open a VPN tunnel. This gateway is selected by the MEP mechanism.
`backup-stickiness`	Indicates whether to continue using the gateway selected by the MEP mechanism, if another gateway has a higher priority: • `True` - Continue using the selected gateway. • `False` - Use the MEP mechanism to select a new gateway.

`permanent-tunnel` Indicates whether to keep VPN tunnels between gateways in this MEP group permanently alive:

- `True` - Keep VPN tunnels permanently alive.
- `False` - Close VPN tunnels when there is no network traffic along them.

EXAMPLE

Running this command results in information such as the following:

```
0:
     group-id: mep_1
     mechanism: First-to-respond
     chosen-gateway: GAr65
     backup-stickiness: False
     permanent-tunnel: False
```

info vpn sites

PURPOSE

The `info vpn sites` command is used to display topology information about VPN sites defined on the appliance.

SYNTAX

info vpn sites

PARAMETERS

None.

RETURN VALUES

The following information is displayed for each VPN site:

The VPN site's name	
`Split DNS`	The VPN site's split DNS mappings. When split DNS is configured for a VPN site, certain domain suffixes are mapped to corporate DNS servers. This means that requests for these domain suffixes are sent to the specific DNS servers to which they are mapped, while all other requests are sent to the ISP's DNS servers. For example, a VPN site's split DNS mappings might indicate that all requests for the domain suffix ".acme.com" should be sent to the Acme company's corporate DNS servers.
`Trusted CAs`	A list of root CAs at the VPN site, whose certificates are trusted by this gateway.
`Sub-CAs`	A list of second-level CAs at the VPN site, which are signed by a trusted root CA.

EXAMPLE

Running this command results in information such as the following:

```
Enterprise
Split DNS
DNS Server:                1.1.1.1
Domain Name:               domain1.com [Max Label Count: 99]
Domain Name:               domain2.com [Max Label Count: 99]
DNS Server:                2.2.2.2
Domain Name:               domain3.com [Max Label Count: 99]
Domain Name:               domain4.com [Max Label Count: 99]
Trusted CAs
internal_CA                ou=ca,o=global,dc=vsmp,dc=com
Sub-CAs
None
...
```

info vpn split-dns

PURPOSE

The `info vpn split-dns` command is used to display the split DNS mappings for this gateway.

When split DNS is configured, certain domain suffixes are mapped to corporate DNS servers. This means that requests for these domain suffixes are sent to the specific DNS servers to which they are mapped, while all other requests are sent to the ISP's DNS servers. For example, the split DNS mappings might indicate that all requests for the domain suffix ".acme.com" should be sent to the Acme company's corporate DNS servers.

SYNTAX

info vpn split-dns

PARAMETERS

None.

RETURN VALUES

The gateway's split DNS mappings.

EXAMPLE

Running this command results in information such as the following:

```
site       Enterprise:
     dns-server 1.1.1.1:
       domain-name: domain1.com
          max prefix label count: 99
       domain-name: domain2.com
          max prefix label count: 99

     dns-server 2.2.2.2:
       domain-name: domain3.com
          max prefix label count: 99
       domain-name: domain4.com
          max prefix label count: 99
```

info vpn trusted-ca

PURPOSE

The `info vpn trusted-ca` command is used to display a list of root CAs whose certificates are trusted by this gateway.

SYNTAX

info vpn trusted-ca

PARAMETERS

None.

RETURN VALUES

A list of root CAs whose certificates are trusted by this gateway

EXAMPLE

Running this command results in information such as the following:

```
internal_CA:
     Trusted CA
     dn: ou=ca,o=global,dc=vsmp,dc=com
```

info vpn tunnels

PURPOSE

The `info vpn tunnels` command is used to display a list of currently established VPN tunnels. VPN tunnels are created and closed as follows:

- Remote Access VPN sites configured for Automatic Login, and Site-to-Site VPN Gateways

  A tunnel is created whenever your computer attempts any kind of communication with a computer at the VPN site. The tunnel is closed when not in use for a period of time.

- Remote Access VPN sites configured for Manual Login

  A tunnel is created whenever your computer attempts any kind of communication with a computer at the VPN site, *after you have manually logged on to the site*. All open tunnels connecting to the site are closed when you manually log off.

SYNTAX

info vpn tunnels

PARAMETERS

None.

RETURN VALUES

The following information is displayed for each VPN tunnel:

`site`	The name of the VPN gateway to which the tunnel is connected.
`src`	The source IP address of the tunnel.
`dst`	The destination IP address of the tunnel.

`encryption`	The security protocol (IPSec), the type of encryption used to secure the connection, and the type of Message Authentication Code (MAC) used to verify the integrity of the message. This information is presented in the following format: Security protocol: Encryption type/Authentication type Note: All VPN settings are automatically negotiated between the two sites. The encryption and authentication schemes used for the connection are the strongest of those used at the two sites. Your Embedded NGX appliance supports AES, 3DES, and DES encryption schemes, and MD5 and SHA authentication schemes.
`time established`	The time at which the tunnel was established. This information is presented in the format: `HH:MM:SS` where: `HH` = hours `MM` = minutes `SS` = seconds
`username`	The user logged on to the VPN site. This can have the following values: • A user name • `N/A` - The user name is unavailable.
`status`	Indicates whether the VPN tunnel is functional. This can have the following values: • `OK` - The tunnel is functional. • `Fail` - The VPN peer is not responding.

`is_l2tp` Indicates whether the user connected using an L2TP (Layer 2 Tunneling Protocol) VPN Client. This can have the following values:

- `yes` - The user connected using an L2TP VPN client.
- `no` - The user did not connect using an L2TP VPN client.

EXAMPLE

Running this command for all network interfaces results in information such as the following:

```
site     src           dst           encryption   time established username  status     is_l2tp
office   212.150.8.84  192.114.68.8  3DES/SHA1    0:00:02:01       JohnS     ok         no
office_2 212.150.8.84  212.150.8.81  AES-256/SHA1 0:00:00:22       N/A       ok         no
```

info vstream

PURPOSE

The `info vstream` command is used to display VStream Antivirus statistics and information about the VStream Antivirus signature databases.

VStream Antivirus maintains two databases: a daily database and a main database. The daily database is updated frequently with the newest virus signatures. Periodically, the contents of the daily database are moved to the main database, leaving the daily database empty. This system of incremental updates to the main database allows for quicker updates and saves on network bandwidth.

SYNTAX

info vstream

PARAMETERS

None.

RETURN VALUES

`Main database`	The date and time at which the main database was last updated, followed by the version number.
`Daily database`	The date and time at which the daily database was last updated, followed by the version number.
`Next update`	The date and time at which the Embedded NGX appliance will check for updates.
`Status`	The current status of the database. This includes the following statuses: • `Database Not Installed` • `OK`

EXAMPLE

Running this command results in information such as the following:

```
Main database: Mar 09, 2008 08:03 GMT
Daily database: Mar 11, 2008 16:08 GMT
Next update: Mar 24, 2008 12:55 GMT
Status: OK
```

info vstream file-types

PURPOSE

The `info vstream file-types` command is used to display a list of safe file types and potentially unsafe file types.

You can configure VStream Antivirus to automatically pass all safe file types and to block all potentially unsafe file types. For information, see ***vstream options*** on page 770.

SYNTAX

info vstream file-types [*type*]

PARAMETERS

`type`	String. The type of file types to display. This can have the following values: • `allowed` - Safe file types • `blocked` - Potentially unsafe file types If you do not include this parameter, both safe and potentially unsafe file types are displayed.

RETURN VALUES

A list of file types of the specified type.

EXAMPLE

Running the following command:

```
info vstream file-types allowed
```

Results in information such as the following:

```
Safe file type list:
     GIF
     BMP
     JFIF standard
     EXIF standard
     PNG
     MPEG video stream
     MPEG sys stream
     Ogg Stream
     MP3 file with ID3 version 2
     MP3
     PDF
     PostScript
     WMA/WMV/ASF
     RealMedia file
```

info wan

PURPOSE

The `wan` command is used to display information about the defined Internet connections.

SYNTAX

info wan [*connection*]

PARAMETERS

`connection`	Integer. The Internet connection for which to display information. This can have the following values: • `1` - Display information for the primary connection. • `2` - Display information for the secondary connection. If you do not include this parameter, and both connections are configured, information is displayed for both connections.

RETURN VALUES

The following information is displayed for each Internet connection

Number	The connection's number.
`name`	The connection's name. This can have the following values: • `primary` • `secondary`
`connected`	Indicates whether the connection is currently up. This can have the following values: • `true.` The connection is up. • `false.` The connection is down.
`idle_timeout`	The amount of time (in minutes) that the connection can remain idle. Once this period of time has elapsed, the dialup modem will disconnect. This field is only relevant for the Dialup connection type.

EXAMPLE

In the following example, a dialup Internet connection is configured as the secondary connection, and information is displayed for all connections:

```
wan:
 1:
  name primary
  connected true
  idle_timeout 0

 2:
  name secondary
  connected false
  idle_timeout 15
```

info wireless

PURPOSE

The `info wireless` command is used to display general information about your appliance's wireless hardware.

This command is only relevant for models supporting a wireless interface.

SYNTAX

info wireless

PARAMETERS

None.

RETURN VALUES

`Region`	The region within which the Embedded NGX appliance is certified for use. This can be any of the following: • `ETSI-A` • `ETSI-B` • `ETSI-C` • `FCCA` • `World` - All other regions Warning: Using the Embedded NGX appliance outside of the certified region may result in the violation of government regulations.
`Country`	The country where you are located.

EXAMPLE

Running this command results in information such as the following:

```
Region: WORLD
Country: United States
```

info wireless ap

PURPOSE

The `info wireless ap` command is used to display information about your appliance's primary wireless network (WLAN) and virtual access points (VAPs).

This command is only relevant for models supporting a wireless interface.

SYNTAX

info wireless ap

PARAMETERS

None.

RETURN VALUES

The following information is displayed for the primary WLAN and for each VAP:

`Protocol`	The protocol used for the wireless connection. This can be any of the following: • `IEEE 802.11b` • `IEEE 802.11g` • `IEEE 802.11bg` • `IEEE 802.11n` • `IEEE 802.11ng`
`MAC`	The MAC address of the appliance's wireless interface.
`SSID`	The network name (SSID) that identifies the wireless network.
`Channel`	The channel currently used for the wireless connection, followed by the exact frequency in parenthesis.

In addition to the above information, the following statistics appear for received data for each access point:

`frames ok`	The total number of frames that were successfully received
`errors`	The total number of received frames for which an error occurred
`discarded: nwid`	The total number of received packets with the wrong SSID
`discarded: crypt`	The total number of received packets with the wrong encryption key
`discarded: fragment`	The total number of packets missed during reception that were dropped, because fragments of the packet were lost

The following statistics appear for transmitted data for each access point:

`frames ok`	The total number of frames that were successfully transmitted
`errors`	The total number of transmitted frames for which an error occurred
`discarded: retries`	The total number of discarded retry packets that were transmitted
`discarded: misc`	The total number of transmitted packets that were discarded for other reasons

EXAMPLE

Running this command results in information such as the following:

```
wlan:
Protocol: IEEE 802.11g
MAC: 00:14:85:ce:7d:d0
SSID: John_Smith_office
Channel: 3 (2422 Mhz)
receive:
     frames ok: 457
     errors: 0
     discarded:
     nwid: 1144
     crypt: 0
     fragment: 0
transmit:
     frames ok: 334
     errors: 0
     discarded:
     retries: 0
     misc: 0
```

```
vap1:
Protocol: IEEE 802.11g
MAC: 06:14:85:ce:7d:d0
SSID: John_Smith_
Channel: 3 (2422 Mhz)
receive:
     frames ok: 151
     errors: 0
     discarded:
     nwid: 1145
     crypt: 0
     fragment: 0
transmit:
     frames ok: 41
     errors: 0
     discarded:
     retries: 0
     misc: 0
```

Chapter 5

CLI Variables

This chapter provides a list of CLI variables that can be used with the CLI commands in ***CLI Commands*** on page 17.

Note: The syntax for using a CLI variable as part of an `export` command is identical to the syntax for using the variable as part of a `show` command. Therefore, the syntax and examples provided for `show` can be used for `export` as well.

This chapter includes the following topics:

access-list

PURPOSE

The `access-list` variable is used for working with BGP access lists in the following ways:

- Adding new access lists
- Configuring an access list's name
- Deleting access lists
- Displaying and exporting access lists
- Clearing the Access Lists table

You can configure the Embedded NGX appliance to filter the routing information that it learns from or advertises to BGP neighbors, by defining access lists.

Once you have used this variable to define an access list, you must add rules to the list, specifying the routing information to block or allow. You can then apply the access list to the desired BGP neighbors. For information on adding rules, see ***access-list-rule*** on page 235. For information on configuring BGP neighbors, see ***bgp neighbor*** on page 273.

These settings are only relevant if BGP is enabled. For information, see ***bgp*** on page 270.

These settings are only available through the command line.

SYNTAX

When used with `add`:

add access-list name *name*

When used with `set`:

set access-list *number* name *name*

When used with `delete`:

delete access-list *number*

When used with `show`:

show access-list [*number*]

When used with `clear`:

clear access-list

FIELDS

`number`	Integer. The access list's row in the Access Lists table.
`name`	String. The access list's name.

EXAMPLE 1

The following command adds an access list called "Incoming1":

```
add access-list name Incoming1
```

EXAMPLE 2

The following command changes the name of the first access list in the Access Lists table:

```
set access-list 1 name Incoming2
```

EXAMPLE 3

The following command deletes the first access list in the Access Lists table:

```
delete access-list 1
```

EXAMPLE 4

The following command displays all access lists in the Access Lists table:

```
show access-list
```

EXAMPLE 5

The following command clears the Access Lists table:

```
clear access-list
```

access-list-rule

PURPOSE

The `access-list-rule` variable is used for working with access list rules in the following ways:

- Adding new access list rules
- Modifying access list rules
- Deleting access list rules
- Displaying and exporting access list rules
- Clearing the Access List Rules table

Access list rules specify which routing information should be blocked or allowed.

These settings are only available through the command line.

SYNTAX

When used with `add`:

add access-list-rule access-list *access-list* action *action* address *address* netmask *netmask* [address-wildcard *address-wildcard*] [netmask-wildcard *netmask-wildcard*]

When used with `set`:

set access-list-rule *number* [access-list *access-list*] [action *action*] [address *address*] [netmask *netmask*] [address-wildcard *address-wildcard*] [netmask-wildcard *netmask-wildcard*]

When used with `delete`:

delete access-list-rule *number*

When used with `show`:

show access-list-rule [*number*] [access-list | action | address | netmask | address-wildcard | netmask-wildcard]

When used with `clear`:

clear access-list-rule

FIELDS

`number`	Integer. The access list rule's row in the Access List Rules table.
`access-list`	String. The name of the access list to which the rule should be assigned. For information on creating access lists, see ***access-list*** on page 233.
`action`	String. The type of rule you want to create. This can have the following values: • `permit` - Allow routing information that matches this rule. • `deny` - Block routing information that matches this rule.
`address`	IP Address. The IP address in routing information that should be allowed/blocked.
`netmask`	IP Address. The subnet mask in routing information that should be allowed/blocked.
`address-wildcard`	IP Address. The wildcard bitmask that should be applied to the IP address in the `address` field. The wildcard bitmask contains “0” for bits that must match or “1” for bit locations that must not match (“wildcard”). The bitmask is formatted as 4 octets (bytes). For example, if you set this field to 0.0.0.0, then the access list rule will only apply to IP addresses that exactly match all four octets of the IP address specified in the `address` field. In contrast, if you set this field to 0.0.0.255, then the access list rule will apply to all IP addresses that exactly match the first three octets of the IP address specified in the `address` field.

The fourth octet is a wildcard and can be any number.

The default value is 0.0.0.0.

`netmask-wildcard` IP Address. The wildcard bitmask that should be applied to the subnet mask in the `netmask` field.

The wildcard bitmask contains “0” for bits that must match or “1” for bit locations that must not match (“wildcard”). The bitmask is formatted as 4 octets (bytes).

For example, if you set this field to 0.0.0.0, then the access list rule will only apply to subnet masks that exactly match all four octets of the subnet mask specified in the `netmask` field.

In contrast, if you set this field to 0.0.0.255, then the access list rule will apply to all subnet masks that exactly match the first three octets of the subnet mask specified in the `netmask` field. The fourth octet is a wildcard and can be any number.

The default value is 0.0.0.0.

EXAMPLE 1

The following command adds a Deny rule to the Outgoing1 access list:

```
add access-list-rule access-list Outgoing1 action deny address 1.2.3.4
netmask 255.255.255.24
```

EXAMPLE 2

The following command modifies rule 1 in the Access List Rules table, so that it becomes a Deny rule:

```
set access-list-rule 1 action deny
```

EXAMPLE 3

The following command deletes rule 1 in the Access List Rules table:

```
delete access-list-rule 1
```

EXAMPLE 4

The following command displays the action for rule 1 in the Access List Rules table:

```
show access-list-rule 1 action
```

EXAMPLE 5

The following command deletes all rules in the Access List Rules table:

```
clear access-list-rule
```

antispam blocked-senders

PURPOSE

The `antispam blocked-senders` variable is used for working with VStream Antispam's Block List engine in the following ways:

- Enabling/disabling the Block List engine
- Configuring Block List engine settings
- Displaying and exporting the above settings
- Displaying and exporting all Block List engine settings, including blocked senders.

  For information on configuring, displaying, and exporting specific blocked senders, see ***antispam blocked-senders list*** on page 242.

VStream Antispam allows configuring a list of senders whose emails should be blocked. When an email reaches your mail server, the Block List engine determines whether the sender's email address appears on the list. If so, then VStream Antispam blocks the emails.

SYNTAX

When used with `set`:

set antispam blocked-senders [mode *mode*] [action *action*] [track *track*] [mark-subject-text *mark-subject-text*]

When used with `show`:

show antispam blocked-senders [mode | action | track | mark-subject-text]

FIELDS

mode

String. The Block List engine's mode. This can have the following values:

- `on` - The Block List engine is on. VStream Antispam will check email messages against a list of blocked senders. Emails that fail the check will handled according to configured Block List settings.
- `monitor` - The Block List engine is on. VStream Antispam will check email messages against a list of blocked senders. Emails that fail the check will be logged only; no other action will be performed.
- `off` - The Block List engine is off.

The default value is `off`.

action

String. The action VStream Antispam should perform upon receiving an email from a blocked sender. This can have the following values:

- `none` - Take no action.
- `reject` - Block the email.
- `mark-subject` - Mark the email's Subject line.

The default value is `reject`.

If you select `mark-subject`, you must set the `mark-subject-text` field.

Note: If the Block List engine is set to Monitor mode, then this field is ignored.

track

String. Indicates whether VStream Antispam should log emails from blocked senders. This can have the following values:

- `log` - Log emails from blocked senders.
- `none` - Do not log emails from blocked senders.

The default value is `log`.

`mark-subject-text` String. The prefix to the text appearing in the Subject field of the spam notification email.

For example, if you set this field to `[SPAM]` and the original email's Subject field displays "Earn Money the Easy Way", the spam notification email's Subject field will display: "[SPAM] Earn Money the Easy Way".

The default value is `[SPAM]`.

Note: If your email client allows defining rules based on the Subject field, you can create rules specifying that emails whose Subject field contains certain words should be moved to specific folders. For example, you can configure your email client to move all emails whose Subject field contains `[SPAM]` directly to the Deleted Items folder.

EXAMPLE 1

The following command enables the Block List engine and configures it to block and log emails from blocked senders:

```
set antispam blocked-senders mode on action reject track log
```

EXAMPLE 2

The following command displays all Block List engine settings, including blocked senders:

```
show antispam blocked-senders
```

antispam blocked-senders list

PURPOSE

The `antispam blocked-senders list` variable is used for working with the Block List engine's list of blocked senders in the following ways:

- Adding new blocked senders
- Modifying blocked senders
- Deleting blocked senders
- Displaying and exporting blocked senders
- Clearing the Blocked Senders table

You can configure a list of email addresses and domain names that VStream Antispam should automatically block, if the Block List engine is enabled.

For information on enabling and configuring the Block List engine, see ***antispam blocked-senders*** on page 239.

SYNTAX

When used with `add`:

add antispam blocked-senders list address *address*

When used with `set`:

set antispam blocked-senders list *number* address *address*

When used with `delete`:

delete antispam blocked-senders list *number*

When used with `show`:

show antispam blocked-senders list [*number*] [address]

When used with `clear`:

clear antispam blocked-senders list

FIELDS

`number`	Integer. The blocked sender's row in the Blocked Senders table.
`address`	IP Address or String. The email address or the domain name to block. For example, if you set this field's value to `spammer@special-offer.com`, then this email address will be blocked. In contrast, if you set this field's value to the domain name `@special-offers.com`, then email addresses such as johns@special-offers.com and sarahm@special-offers.com will be blocked.

EXAMPLE 1

The following command adds the email address spammer@special-offer.com as a blocked sender:

```
add antispam blocked-senders list address spammer@special-offer.com
```

EXAMPLE 2

The following command modifies blocked sender 1 in the Blocked Senders table:

```
set antispam blocked-senders list 1 address @special-offer.com
```

EXAMPLE 3

The following command deletes blocked sender 1 in the Blocked Senders table:

```
delete antispam blocked-senders list 1
```

EXAMPLE 4

The following command displays all blocked senders in the Blocked Senders table:

```
show antispam blocked-senders list
```

EXAMPLE 5

The following command deletes all blocked senders in the Blocked Senders table:

```
clear antispam blocked-senders list
```

antispam content-based

PURPOSE

The `antispam content-based` variable is used for working with VStream Antispam's Content Based Antispam engine in the following ways:

- Enabling/disabling the Content Based Antispam engine
- Displaying and exporting the Content Based Antispam engine mode
- Displaying and exporting all Content Based Antispam engine settings, including spam and suspected spam settings

  For information on configuring, displaying, and exporting specific spam and suspected spam settings, see ***antispam content-based spam*** on page 247 and ***antispam content-based suspected-spam*** on page 250.

The Content Based Antispam engine calculates a “spam fingerprint” for each incoming email message. The fingerprint is then sent to a VStream Antispam data center and compared to a constantly updated database of spam messages. The data center returns a "spam score", which is a value in percentages indicating the likelihood that the message is spam. If the spam score exceeds a user-configurable threshold called the “confidence level”, the message header and/or subject can be flagged as spam, or the message can be deleted altogether.

SYNTAX

When used with `set`:

set antispam content-based mode *mode*

When used with `show`:

show antispam content-based [mode]

FIELDS

`mode`

String. The Content Based Antispam engine's mode. This can have the following values:

- `on` - The Content Based Antispam engine is on. VStream Antispam will check email fingerprints against an online spam detection database. Emails that fail the check will be handled according to configured Content Based Antispam settings.
- `monitor` - The Content Based Antispam engine is on. VStream Antispam will check email fingerprints against an online spam detection database. Emails that fail the check will be logged only; no other action will be performed.
- `off` - The Content Based Antispam engine is off.

The default value is `off`.

EXAMPLE 1

The following command enables the Content Based Antispam engine:

```
set antispam content-based mode on
```

EXAMPLE 2

The following command displays all Content Based Antispam engine settings, including including spam and suspected spam settings:

```
show antispam content-based
```

antispam content-based spam

PURPOSE

The `antispam content-based spam` variable is used for working with the Content Based Antispam engine's spam settings in the following ways:

- Configuring the Content Based Antispam engine's spam settings
- Displaying and exporting the Content Based Antispam engine's spam settings

You can configure how VStream Antispam should handle spam that is detected by the Content Based Antispam engine.

For information on enabling the Content Based Antispam engine, see ***antispam content-based*** on page 245.

SYNTAX

When used with `set`:

set antispam content-based spam [action *action*] [track *track*] [confidence-level *confidence-level*] [mark-subject-text *mark-subject-text*]

When used with `show`:

show antispam content-based spam [action | track | confidence-level | mark-subject-text]

FIELDS

`action`

String. The action VStream Antispam should perform upon detecting spam. This can have the following values:

- `none` - Take no action.
- `reject` - Block the email. The email will be permanently deleted.
- `mark-subject` - Mark the email's Subject line.

The default value is `reject`.

If you select `mark-subject`, you must set the `mark-subject-text` field.

Note: If the Content Based Antispam engine is set to Monitor mode, then this field is ignored.

`track`

String. Indicates whether VStream Antispam should log spam. This can have the following values:

- `log` - Log spam.
- `none` - Do not log spam.

The default value is `log`.

`confidence-level`

Integer. The minimum spam confidence level (SCL). If an email's SCL matches or exceeds this threshold, the email is considered spam.

Setting a higher SCL reduces the number of legitimate emails erroneously identified as spam. Setting a lower SCL increases the amount of spam that is identified as legitimate email.

The default value is 90.

`mark-subject-text` String. The prefix to the text appearing in the Subject field of the spam notification email.

For example, if you set this field to `[SPAM]` and the original email's Subject field displays "Earn Money the Easy Way", the spam notification email's Subject field will display: "[SPAM] Earn Money the Easy Way".

The default value is `[SPAM]`.

Note: If your email client allows defining rules based on the Subject field, you can create rules specifying that emails whose Subject field contains certain words should be moved to specific folders. For example, you can configure your email client to move all emails whose Subject field contains `[SPAM]` directly to the Deleted Items folder.

EXAMPLE 1

The following command configures the Content Based Antispam engine to block and log emails detected as spam:

```
set antispam content-based spam action reject track log
```

EXAMPLE 2

The following command displays all of the Content Based Antispam engine's spam settings:

```
show antispam content-based spam
```

antispam content-based suspected-spam

PURPOSE

The `antispam content-based suspected-spam` variable is used for working with the Content Based Antispam engine's suspected spam settings in the following ways:

- Configuring the Content Based Antispam engine's suspected spam settings
- Displaying and exporting the Content Based Antispam engine's suspected spam settings

You can configure how VStream Antispam should handle suspected spam that is detected by the Content Based Antispam engine.

For information on enabling the Content Based Antispam engine, see ***antispam content-based*** on page 245.

SYNTAX

When used with `set`:

set antispam content-based suspected-spam [action *action*] [track *track*] [confidence-level *confidence-level*] [mark-subject-text *mark-subject-text*]

When used with `show`:

show antispam content-based suspected-spam [action | track | confidence-level | mark-subject-text]

FIELDS

`action`

String. The action VStream Antispam should perform upon detecting suspected spam. This can have the following values:

- `none` - Take no action.
- `reject` - Block the email. The email will be permanently deleted.
- `mark-subject` - Mark the email's Subject line.

The default value is `mark-subject`.

If you select `mark-subject`, you must set the `mark-subject-text` field.

Note: If the Content Based Antispam engine is set to Monitor mode, then this field is ignored.

`track`

String. Indicates whether VStream Antispam should log suspected spam. This can have the following values:

- `log` - Log suspected spam.
- `none` - Do not log suspected spam.

The default value is `log`.

`confidence-level`

Integer. The minimum spam confidence level (SCL). If an email's SCL matches or exceeds this threshold, the email is considered suspected spam.

Setting a higher SCL reduces the number of legitimate emails erroneously identified as suspected spam. Setting a lower SCL increases the amount of potential spam that is identified as legitimate email.

The default value is 90.

`mark-subject-text`

String. The prefix to the text appearing in the Subject field of the suspected spam notification email.

For example, if you set this field to `[SUSPECTED SPAM]` and the original email's Subject field displays "Earn Money the Easy Way", the suspected spam notification email's Subject field will display: "[SUSPECTED SPAM] Earn Money the Easy Way".

The default value is `[SUSPECTED SPAM]`.

Note: If your email client allows defining rules based on the Subject field, you can create rules specifying that emails whose Subject field contains certain words should be moved to specific folders. For example, you can configure your email client to move all emails whose Subject field contains `[SUSPECTED SPAM]` directly to a Quarantine folder.

EXAMPLE 1

The following command configures the Content Based Antispam engine to block and log emails detected as suspected spam:

```
set antispam content-based suspected-spam action reject track log
```

EXAMPLE 2

The following command displays all of the Content Based Antispam engine's suspected spam settings:

```
show antispam content-based suspected-spam
```

antispam ip-reputation

PURPOSE

The `antispam ip-reputation` variable is used for working with VStream Antispam's IP Reputation engine in the following ways:

- Enabling/disabling the IP Reputation engine
- Displaying and exporting the IP Reputation engine mode
- Displaying and exporting all IP Reputation engine settings, including spam and suspected spam settings

  For information on configuring, displaying, and exporting specific spam and suspected spam settings, see ***antispam ip-reputation spam*** on page 255 and ***antispam ip-reputation suspected-spam*** on page 257.

The IP Reputation engine checks the email sender's IP address against an online and constantly updated IP reputation database, before accepting the SMTP email connection. If the IP address belongs to a known spammer, the connection can be immediately blocked at the TCP connection level, thereby stopping the spam before it reaches your mail server.

Note: It is recommended to enable the IP Reputation engine as a first line of defense for incoming SMTP connections. When enabled, the IP Reputation engine blocks emails that would otherwise reach your mail server and require extensive analysis by the Content Based Antispam and Block List engines, both of which examine email content and consume network, gateway, and mail server resources. By reducing the amount of emails that require in-depth analysis, the IP Reputation engine helps prevent Denial of Service (DoS) attacks on your gateway or mail server.

SYNTAX

When used with `set`:

set antispam ip-reputation mode *mode*

When used with `show`:

show antispam ip-reputation [mode]

FIELDS

mode

String. The IP Reputation engine's mode. This can have the following values:

- `on` - The IP Reputation engine is on. VStream Antispam will check the reputation of email senders against an online IP reputation database prior to accepting the TCP connection. Emails that fail the check will handled according to configured IP Reputation settings.
- `monitor` - The IP Reputation engine is on. VStream Antispam will check the reputation of email senders against an online IP reputation database. Emails that fail the check will be logged only; no other action will be performed.
- `off` - The IP Reputation engine is off.

The default value is `off`.

EXAMPLE 1

The following command enables the IP Reputation engine:

```
set antispam ip-reputation mode on
```

EXAMPLE 2

The following command displays all IP Reputation engine settings, including including spam and suspected spam settings:

```
show antispam ip-reputation
```

antispam ip-reputation spam

PURPOSE

The `antispam ip-reputation spam` variable is used for working with the IP Reputation engine's spam settings in the following ways:

- Configuring the IP Reputation engine's spam settings
- Displaying and exporting the IP Reputation engine's spam settings

You can configure how VStream Antispam should handle spam that is detected by the IP Reputation engine.

For information on enabling the IP Reputation engine, see ***antispam ip-reputation*** on page 253.

SYNTAX

When used with `set`:

set antispam ip-reputation spam [action *action*] [track *track*] [confidence-level *confidence-level*]

When used with `show`:

show antispam ip-reputation spam [action | track | confidence-level]

FIELDS

`action`	String. The action VStream Antispam should perform upon detecting spam. This can have the following values: • `none` - Take no action. • `reject` - Block the email. The default value is `reject`. Note: If the IP Reputation engine is set to Monitor mode, then this field is ignored.

`track`	String. Indicates whether VStream Antispam should log spam. This can have the following values: • `log` - Log spam. • `none` - Do not log spam. The default value is `log`.
`confidence-level`	Integer. The minimum spam confidence level (SCL). If an email's SCL matches or exceeds this threshold, the email is considered spam. Setting a higher SCL reduces the number of legitimate emails erroneously identified as spam. Setting a lower SCL increases the amount of spam that is identified as legitimate email. The default value is 90.

EXAMPLE 1

The following command configures the IP Reputation engine to block and log emails detected as spam:

```
set antispam ip-reputation spam action reject track log
```

EXAMPLE 2

The following command displays all of the IP Reputation engine's spam settings:

```
show antispam ip-reputation spam
```

antispam ip-reputation suspected-spam

PURPOSE

The `antispam ip-reputation suspected-spam` variable is used for working with the IP Reputation engine's suspected spam settings in the following ways:

- Configuring the IP Reputation engine's suspected spam settings
- Displaying and exporting the IP Reputation engine's suspected spam settings

You can configure how VStream Antispam should handle suspected spam that is detected by the IP Reputation engine.

For information on enabling the IP Reputation engine, see ***antispam ip-reputation*** on page 253.

SYNTAX

When used with `set`:

set antispam ip-reputation suspected-spam [action *action*] [track *track*] [confidence-level *confidence-level*] [mark-subject-text *mark-subject-text*]

When used with `show`:

show antispam ip-reputation suspected-spam [action | track | confidence-level | mark-subject-text]

FIELDS

`action`	String. The action VStream Antispam should perform upon detecting suspected spam. This can have the following values: • `none` - Take no action. • `reject` - Block the email. The default value is `none`. Note: If the Content Based Antispam engine is set to Monitor mode, then this field is ignored.

`track`	String. Indicates whether VStream Antispam should log suspected spam. This can have the following values: • `log` - Log suspected spam. • `none` - Do not log suspected spam. The default value is `log`.
`confidence-level`	Integer. The minimum spam confidence level (SCL). If an email's SCL matches or exceeds this threshold, the email is considered suspected spam. Setting a higher SCL reduces the number of legitimate emails erroneously identified as suspected spam. Setting a lower SCL increases the amount of potential spam that is identified as legitimate email. The default value is 90.

EXAMPLE 1

The following command configures the IP Reputation engine to block and log emails detected as suspected spam:

```
set antispam ip-reputation suspected-spam action reject track log
```

EXAMPLE 2

The following command displays all of the IP Reputation engine's suspected spam settings:

```
show antispam ip-reputation suspected-spam
```

antispam non-spam

PURPOSE

The `antispam non-spam` variable is used for working with VStream Antispam in the following ways:

- Configuring how VStream Antispam should handle legitimate mail
- Displaying and exporting the these settings

You can specify how VStream Antispam should handle email that is detected as legitimate mail.

SYNTAX

When used with `set`:

set antispam non-spam track *track*

When used with `show`:

show antispam non-spam [track]

FIELDS

`track`	String. Indicates whether VStream Antispam should log email that is detected as legitimate mail. This can have the following values: • `log` - VStream Antispam should log email that is detected as legitimate mail. • `none` - VStream Antispam should not log email that is detected as legitimate mail. The default value is `none`.

EXAMPLE 1

The following command configures VStream Antispam to log legitimate mail:

```
set antispam non-spam track log
```

EXAMPLE 2

The following command displays VStream Antispam's settings for legitimate mail:

```
show antispam non-spam
```

antispam policy rules

PURPOSE

The `antispam policy rules` variable is used for working with VStream Antispam rules in the following ways:

- Adding new VStream Antispam rules
- Modifying VStream Antispam rules
- Deleting VStream Antispam rules
- Displaying and exporting VStream Antispam rules
- Clearing the Vstream Antispam Policy Rule table

VStream Antispam includes a flexible mechanism that allows the user to define exactly which emails should be scanned for spam and which should be considered safe, by specifying the protocol, and the source and destination IP addresses.

VStream Antispam processes policy rules in the order they appear in the Antispam Policy table, so that rule 1 is applied before rule 2, and so on. This enables you to define exceptions to rules, by placing the exceptions higher up in the table.

Note: You must enable at least *one of the three* VStream Antispam engine in order for VStream Antispam to work. For information on enabling the IP Reputation engine, see ***antispam ip-reputation*** on page *253*. For information on enabling the Block List engine, see ***antispam blocked-senders*** on page *239*. For information on enabling the Content Based Antispam engine, see ***antispam content-based*** on page *245*.

SYNTAX

When used with `add`:

add antispam policy rules type *type* [service *service*] [src *src*] [dest *dest*] [index *index*] [disabled *disabled*] [description *description*]

When used with `set`:

set antispam policy rules *number* [type *type*] [service *service*] [src *src*] [dest *dest*] [index *index*] [disabled *disabled*] [description *description*]

When used with `delete`:

delete antispam policy rules *number*

When used with `show`:

show antispam policy rules [*number*] [type | service | src | dest | index | disabled | description]

When used with `clear`:

clear antispam policy rules

FIELDS

`number`	Integer. The VStream Antispam rule's row in the VStream Antispam Policy Rule table.
`type`	String. The type of rule you want to create. This can have the following values: • `pass` - Enables you to specify that VStream Antispam should not scan emails matching the rule. • `scan` - Enables you to specify that VStream Antispam should scan emails matching the rule. • `reject` - Enables you to specify that VStream Antispam should reject emails matching the rule, without scanning the emails.
`service`	Integer or String. The service to which the rule should apply. This can have the following values: • `smtp` • `pop3` • `any` - The rule should apply to any service. The default value is `smtp`.

`src`

IP Address or String. The source of the connections you want to scan or pass. This can have the following values:

- An IP address
- An IP address range - To specify a range, use the following format:
  `<Start IP Address>-<End IP Address>`
- `any` - The rule should apply to any source.
- `wan`
- `lan`
- `dmz`
- `vpn`
- `notvpn` - Not VPN
- The name of a VPN site
- The name of a network object
- The name of a bridge
- The name of a VLAN
- The name of a VAP
- The name of a WDS link

The default value is `any`.

`dest`

IP Address or String. Select the destination of the connections you want to scan or pass. This can have the following values:

- An IP address
- An IP address range - To specify a range, use the following format:
  `<Start IP Address>-<End IP Address>`
- `any` - The rule should apply to any destination.
- `wan`
- `lan`
- `dmz`
- `vpn`
- `notvpn` - Not VPN

- The name of a VPN site
- The name of a network object
- The name of a bridge
- The name of a VLAN
- The name of a VAP
- The name of a WDS link

The default value is `any`.

`index`

Integer. The VStream Antispam rule's row in the VStream Antispam Policy Rules table.

Use this field to move the rule up or down in the VStream Antispam Policy Rules table. The appliance processes rules higher up in the table (lower indexes) before rules lower down in the table (higher indexes).

If you do not include this field when adding a rule, the rule is automatically added to the bottom of the VStream Antispam Policy Rules table.

`disabled`

String. Indicates whether the rule is disabled. This can have the following values:

- `true` - The rule is disabled.
- `false` - The rule is enabled.

The default value is `false`.

`description`

String. A description of the rule.

EXAMPLE 1

The following command creates a Scan rule for SMTP connections from the WAN to the LAN:

```
add antispam policy rules type scan service smtp src wan dest lan
```

EXAMPLE 2

The following command modifies rule 1 in the VStream Antispam Policy Rule table, so that it becomes a Pass rule:

```
set antispam policy rules 1 type pass
```

EXAMPLE 3

The following command deletes rule 1 in the VStream Antispam Policy Rule table:

```
delete antispam policy rules 1
```

EXAMPLE 4

The following command displays the description of rule 1 in the VStream Antispam Policy Rule table:

```
show antispam policy rules 1 description
```

EXAMPLE 5

The following command deletes all rules in the VStream Antispam Policy Rule table:

```
clear antispam policy rules
```

antispam safe-senders

PURPOSE

The `antispam safe-senders` variable is used for working with VStream Antispam's Safe Sender List in the following ways:

- Configuring how VStream Antispam should handle emails from safe senders
- Displaying and exporting Safe Sender List settings
- Displaying and exporting all Safe Sender List settings, including safe senders.

  For information on configuring, displaying, and exporting specific safe senders, see ***antispam safe-senders list*** on page 268.

VStream Antispam allows you to define a Safe Sender List, which consists of senders who are exempt from the Block List and Content Based Antispam engines. You can specify how VStream Antispam should handle email from senders on this list.

SYNTAX

When used with `set`:

set antispam safe-senders track *track*

When used with `show`:

show antispam safe-senders [track]

FIELDS

`track`	String. Indicates whether VStream Antispam should log emails from safe senders. This can have the following values: • `log` - Log emails from safe senders. • `none` - Do not log emails from safe senders. The default value is `none`.

EXAMPLE 1

The following command configures VStream Antispam to log emails from safe senders:

```
set antispam safe-senders track log
```

EXAMPLE 2

The following command displays all Safe Sender List settings, including safe senders:

```
show antispam safe-senders
```

antispam safe-senders list

PURPOSE

The `antispam safe-senders list` variable is used for working with the Safe Sender List in the following ways:

- Adding new safe senders
- Modifying safe senders
- Deleting safe senders
- Displaying and exporting safe senders
- Clearing the Safe Senders table

VStream Antispam allows you to define a Safe Sender List, which consists of email addresses and domain names that are "safe".

Note: The IP Reputation check is performed *before* accepting the TCP connection, at which point the sender's email address is not yet available. Therefore, if the IP Reputation engine is enabled, and an SMTP session is received from an IP address that is reputed to be a source of spam, VStream Antispam will block the connection, regardless of whether the sender's email address is on the Safe Sender List.

SYNTAX

When used with `add`:

add antispam safe-senders list address *address*

When used with `set`:

set antispam safe-senders list *number* address *address*

When used with `delete`:

delete antispam safe-senders list *number*

When used with `show`:

show antispam safe-senders list [*number*] [address]

When used with `clear`:

clear antispam safe-senders list

FIELDS

`number`	Integer. The safe sender's row in the Safe Senders table.
`address`	IP Address or String. The email address or the domain name to allow. For example, if you set this field's value to `manager@mycompany.com`, then this email address will be allowed. In contrast, if you set this field's value to the domain name `@mycompany.com`, then email addresses such as johns@mycompany.com and sarahm@mycompany.com will be allowed.

EXAMPLE 1

The following command adds the email address manager@mycompany.com as a safe sender:

```
add antispam safe-senders list address manager@mycompany.com
```

EXAMPLE 2

The following command modifies safe sender 1 in the Safe Senders table:

```
set antispam safe-senders list 1 address @mycompany.com
```

EXAMPLE 3

The following command deletes safe sender 1 in the Safe Senders table:

```
delete antispam safe-senders list 1
```

EXAMPLE 4

The following command displays all safe senders in the Safe Senders table:

```
show antispam safe-senders list
```

EXAMPLE 5

The following command deletes all safe senders in the Safe Senders table:

```
clear antispam safe-senders list
```

bgp

PURPOSE

The bgp variable is used for working with Border Gateway Protocol (BGP) settings in the following ways:

- Enabling/disabling BGP
- Specifying the BGP router identifier
- Setting the BGP log level
- Specifying the Embedded NGX appliance's local AS
- Displaying and exporting the above BGP settings
- Displaying and exporting all BGP settings, including:
  - BGP neighbors
  - BGP networks
  - Routing information distribution settings
  - Interval timers

  For information on configuring, displaying, and exporting specific BGP neighbors, see ***bgp neighbor*** on page 273. For information on configuring, displaying, and exporting specific BGP networks, see ***bgp network*** on page 278. For information on configuring, displaying, and exporting specific routing information distribution settings, see ***bgp redistribute*** on page 280. For information on configuring, displaying, and exporting interval timers, see ***bgp timers*** on page 282.

The Embedded NGX appliance supports Border Gateway Protocol (BGP), the highly scalable dynamic routing protocol on which the Internet is based. You can use BGP to do the following:

- Distribute routing information between routers in a single autonomous system (AS). This is called Internal Border Gateway Protocol (iBGP).
- Distribute routing information between routers in different ASs. This is called External Border Gateway Protocol (eBGP).

Each BGP-enabled router advertises its internal routes to other BGP-enabled routers, or *BGP neighbors*, over a TCP connection. The neighbors use the received routing information to choose the best route for sending packets, and to reroute traffic around failures for high

resiliency. After the initial exchange of routing information, neighbors only advertise updates to their IP routing tables.

If desired, BGP can be used for *multihoming* purposes: you can connect your network to two different ISPs, and use BGP to select the ISP that provides the optimal route to a desired destination. This provides Internet connection redundancy.

To use BGP, you must add a firewall rule for each neighbor, allowing traffic on TCP port 179 from the neighbor to this gateway. For information on configuring rules, see ***fw rules*** on page 322.

Note: To use BGP, your Embedded NGX appliance must be installed with a BGP-enabled firmware. Such firmwares have a "b" appended to their version number, for example 8.0.21xb.

BGP-enabled firmwares do not support OSPF.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set bgp [**mode** *mode*] [**local-as** *local-as*] [**router-id** *router-id*] [**log-level** *log-level*]

When used with `show`:

show bgp [**mode** | **local-as** | **router-id** | **log-level**]

FIELDS

`mode`	String. The BGP mode. This can have the following values: • `disable` - BGP is disabled. • `enable` - BGP is enabled. The default value is `disable`.
`local-as`	Integer. The number of the autonomous system (AS) to which the Embedded NGX appliance belongs. The default value is 0.

`router-id`	IP Address or String. The BGP router identifier. This can have the following values: • An IP address • `undefined` - No BGP router is defined. The IP address with the highest numeric value will be used as the router ID. The default value is `undefined`.
`log-level`	String. The level of BGP logs that should be written to the Embedded NGX appliance's Event Log. This can have the following values: • `low` • `medium` • `high` The default value is `medium`.

EXAMPLE 1

The following command enables BGP:

```
set bgp mode enable
```

EXAMPLE 2

The following command displays all BGP settings:

```
show bgp
```

bgp neighbor

PURPOSE

The `bgp neighbor` variable is used for working with BGP neighbors in the following ways:

- Adding BGP neighbors
- Modifying BGP neighbors
- Deleting BGP neighbors
- Displaying and exporting BGP neighbors
- Clearing the BGP Neighbors table

To enable BGP sessions with a neighboring router, you must add the router as a BGP neighbor.

These settings are only available through the command line.

SYNTAX

When used with `add`:

add bgp neighbor address *address* remote-as *remote-as* [access-list-in *access-list-in*] [access-list-out *access-list-out*] [advertise-default-route *advertise-default-route*] [ebgp-multihop *ebgp-multihop*] [next-hop-self *next-hop-self*] [weight *weight*]

When used with `set`:

set bgp neighbor *number* [address *address*] [remote-as *remote-as*] [access-list-in *access-list-in*] [access-list-out *access-list-out*] [advertise-default-route *advertise-default-route*] [ebgp-multihop *ebgp-multihop*] [next-hop-self *next-hop-self*] [weight *weight*]

When used with `delete`:

delete bgp neighbor *number*

When used with `show`:

show bgp neighbor *number* [address | remote-as | access-list-in | access-list-out | advertise-default-route | ebgp-multihop | next-hop-self | weight]

When used with `clear`:

clear bgp neighbor

FIELDS

number	Integer. The network 's row in the BGP Networks table.
`address`	IP Address. The neighbor's IP address.
`remote-as`	Integer. The number of the autonomous system (AS) to which the neighbor belongs.
`access-list-in`	String. The access list to apply to incoming publications from the neighbor. For information on defining access lists, see ***access-list*** on page 233.
`access-list-out`	String. The access list to apply to outgoing publications to the neighbor. For information on defining access lists, see ***access-list*** on page 233.
`advertise-default-route`	String. Indicates whether to advertise the local default route to this neighbor. This can have the following values: • `true` - Advertise the local default route to this neighbor. The neighbor can use the local default route to reach the Embedded NGX appliance when all other routes are unavailable. • `false` - Do not advertise the local default route. The default value is `false`.

`ebgp-multihop`

Integer. The maximum number of hops that the BGP session may traverse to reach this neighbor.

By default, BGP allows establishing sessions with external neighbors, only if they are on a directly connected network. That is, the BGP session may traverse only one hop to reach an external neighbor.

If desired, you can allow BGP sessions with an external neighbor that is not directly connected, by setting this field to the number of hops required to reach it.

This must be a value between 1 and 255. The default value is 1.

`next-hop-self`

String. Indicates whether to specify the Embedded NGX appliance's IP address as the next hop in all updates sent to this neighbor.

By default, BGP selects the next hop automatically. However, if the network is not fully meshed, meaning that neighbors do not have direct access to all other neighbors on the same subnet, automatic next-hop selection can lead to broken routes. In this case, you must specify the Embedded NGX appliance's IP address as the next hop.

This can have the following values:

- `true` - Specify the Embedded NGX appliance's IP address as the next hop in all updates sent to this neighbor.
- `false` - Do not specify the Embedded NGX appliance's IP address as the next hop in all updates sent to this neighbor.

The default value is `false`.

`weight`	Integer. The weight to assign all routes learned from this neighbor. Weight is used to control path selection. When multiple routes to the same destination exist, the BGP router will send packets through the route with the highest weight. For example, if one neighbor's routes are assigned a weight of 100, and another neighbor's routes are assigned a weight of 50, packets will be sent via the first neighbor's routes. Note: Weight values are local to the router. The default value is 100.

EXAMPLE 1

The following command adds a BGP neighbor and specifies that incoming connections from this neighbor should be filtered using the access list Incoming1:

```
add bgp neighbor address 1.2.3.4 remote-as 1 access-list-in Incoming1
```

EXAMPLE 2

The following command modifies AS of neighbor 1 in the BGP Neighbors table:

```
set bgp neighbor 1 remote-as 3
```

EXAMPLE 3

The following command deletes network 1 in the BGP Neighbors table:

```
delete bgp neighbor 1
```

EXAMPLE 4

The following command displays all BGP neighbors:

```
show bgp neighbor
```

EXAMPLE 5

The following command deletes all networks in the BGP Neighbors table:

```
clear bgp neighbor
```

bgp network

PURPOSE

The `bgp network` variable is used for working with BGP networks in the following ways:

- Adding BGP networks
- Modifying BGP networks
- Deleting BGP networks
- Displaying and exporting BGP networks
- Clearing the BGP Networks table

To advertise a network as originating in the local AS, you must add the network as a BGP network. You can add networks learned from connected routes, static routes, or dynamic routing.

These settings are only available through the command line.

SYNTAX

When used with `add`:

add bgp network address *address* **netmask** *netmask*

When used with `set`:

set bgp network *number* [**address** *address*] [**netmask** *netmask*]

When used with `delete`:

delete bgp network *number*

When used with `show`:

show bgp network *number* [**address** | **netmask**]

When used with `clear`:

clear bgp network

FIELDS

number	Integer. The network 's row in the BGP Networks table.
address	IP Address. The network's IP address.
mask	IP Address. The network's subnet mask.

EXAMPLE 1

The following command adds a BGP network:

```
add bgp network address 1.2.3.4 netmask 255.255.255.255
```

EXAMPLE 2

The following command modifies the subnet mask of network 1 in the BGP Networks table:

```
set bgp network 1 netmask 255.255.255.0
```

EXAMPLE 3

The following command deletes network 1 in the BGP Networks table:

```
delete bgp network 1
```

EXAMPLE 4

The following command displays all BGP networks:

```
show bgp network
```

EXAMPLE 5

The following command deletes all networks in the BGP Networks table:

```
clear bgp network
```

bgp redistribute

PURPOSE

The `bgp redistribute` variable is used for working with BGP routing information distribution settings in the following ways:

- Configuring BGP routing information distribution settings for directly connected networks
- Configuring BGP routing information distribution settings for routes updated in the Embedded NGX Portal
- Displaying and exporting all BGP routing information distribution settings.

You can control how BGP routing information is redistributed.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set bgp redistribute [connected *connected*] [kernel *kernel*]

When used with `show`:

show bgp redistribute [connected | kernel]

FIELDS

`connected`	String. Indicates whether to enable redistribution of BGP routing information for connected networks. This can have the following values: • `enabled` - Enable redistribution. • `disabled` - Disable redistribution. The default value is `disabled`.

`kernel`	String. Indicates whether to enable redistribution of BGP routing information for routes updated in the Embedded NGX Portal. This can have the following values: • `enabled` - Enable redistribution. • `disabled` - Disable redistribution. The default value is `disabled`.

EXAMPLE 1

The following command enables redistributing routing information for connected networks:

```
set bgp redistribute connected enabled
```

EXAMPLE 2

The following command displays all BGP routing information distribution settings:

```
show bgp redistribute
```

bgp timers

PURPOSE

The `bgp timers` variable is used for working with BGP timer settings in the following ways:

- Configuring BGP timer settings
- Displaying and exporting BGP timer settings

You can modify BGP timer settings.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set bgp timers [**keepalive** *keepalive*] [**holdtime** *holdtime*]

When used with `show`:

show bgp timers [**keepalive** | **holdtime**]

FIELDS

`keepalive`	Integer. The interval of time (in seconds) between transmissions of keepalive messages to BGP neighbors. The default value is 60 seconds.
`holdtime`	Integer. The interval of time (in seconds) after which the Embedded NGX appliance will terminate the connection to a BGP neighbor, if the neighbor does not send a keepalive message. The default value is 180 seconds.

EXAMPLE 1

The following command modifies the BGP timer settings:

```
set bgp timers keepalive 50 holdtime 150
```

EXAMPLE 2

The following command displays all BGP timer settings:

```
show bgp timers
```

bridges

PURPOSE

The `bridges` variable is used for working with bridges in the following ways:

- Adding new bridges
- Configuring a bridge's settings, including:
  - The bridge's name
  - The bridge's IP address and subnet mask
  - The bridge's traffic settings
- Deleting bridges
- Displaying and exporting the above bridge settings
- Displaying and exporting all bridge settings, including High Availability settings and STP settings.

  For information on configuring, displaying, and exporting specific bridge High Availability settings, see ***bridges ha*** on page 288. For information on configuring, displaying, and exporting specific bridge STP settings, see ***bridges stp*** on page 290.
- Clearing the Bridges table

The Embedded NGX appliance enables you to connect multiple network segments at the data-link layer, by configuring a bridge. You can use bridges to compartmentalize your network into several security zones, without changing the IP addressing scheme or reconfiguring the routers.

Bridges operate at layer 2 of the OSI model, therefore adding a bridge to an existing network is completely transparent and does not require any changes to the network's structure.

Note: The following Embedded NGX models do not support using bridge mode with port-based VLAN:

- SBX166-LHGE-2
- SBX166-LHGE-3

Note: After adding a bridge, you must add the desired internal networks and Internet connections to the bridge. For instructions, see ***net dmz*** on page *368*, ***net lan*** on page *387*, ***net wan*** on page *399*, ***net wan2*** on page *430*, and ***vlan*** on page *686*.

SYNTAX

When used with `add`:

add bridges name *name* [firewall *firewall*] [non-ip-traffic *non-ip-traffic*] [address *address*] [netmask *netmask*]

When used with `set`:

set bridges *number* [name *name*] [firewall *firewall*] [non-ip-traffic *non-ip-traffic*] [address *address*] [netmask *netmask*]

When used with `delete`:

delete bridges *number*

When used with `show`:

show bridges [*number*] [name | firewall | non-ip-traffic | address | netmask]

When used with `clear`:

clear bridges

FIELDS

`number`	Integer. The bridge's row in the Bridges table.
`name`	String. The bridge's name.
`firewall`	String. Indicates whether the firewall should be enabled between networks on this bridge. This can have the following values: • `enabled` - The firewall is enabled, and it will inspect traffic between networks on the bridge. • `disabled` - The firewall is disabled between networks on this bridge. The default value is `enabled`.

`non-ip-traffic`	String. Indicates how the firewall should handle non-IP protocol traffic between networks on this bridge. This can have the following values: • `block` - The firewall will block all non-IP protocol traffic on this bridge. • `pass` - The firewall will allow all non-IP protocol traffic on this bridge. The default value is `block`.
`address`	IP Address or String. The IP address to use for this gateway on the bridge. This can have the following values: • An IP address • `undefined` - The Primary DNS server is not defined. Note: The bridge must not overlap other networks.
`netmask`	IP Address. The bridge's subnet mask.

EXAMPLE 1

The following command adds a bridge called "Bridge1":

```
add bridges name Bridge1
```

EXAMPLE 2

The following command disables the firewall between networks on the first bridge in the Bridges table:

```
set bridges 1 firewall disabled
```

EXAMPLE 3

The following command deletes the first bridge in the Bridges table:

```
delete bridges 1
```

EXAMPLE 4

The following command displays the IP address used for this gateway on the first bridge in the Bridges table:

```
show bridges 1 address
```

EXAMPLE 5

The following command clears the Bridges table:

```
clear bridges
```

bridges ha

PURPOSE

The `bridges ha` variable is used for working with a bridge's High Availability settings in the following ways:

- Configuring a bridge's High Availability settings
- Displaying and exporting a bridge's High Availability settings

You can create a High Availability cluster consisting of two or more Embedded NGX appliances. For more information on High Availability, see ***ha*** on page 335.

SYNTAX

When used with `set`:

set bridges *number* ha virtualip *virtualip*

When used with `show`:

show bridges *number* ha [virtualip]

FIELDS

`number`	Integer. The bridge's row in the Bridges table.
`virtualip`	IP Address or String. The default gateway IP address. This can have the following values: • An IP address - This can be any unused IP address on the bridge, and must be the same for both gateways. • `undefined` - High Availability is not configured for this bridge. The default value is `undefined`.

EXAMPLE 1

The following command sets the virtual IP address of the first bridge in the Bridges table:

```
set bridges 1 ha virtualip 192.168.10.14
```

EXAMPLE 2

The following command displays the High Availability settings of the first bridge in the Bridges table:

```
show bridges 1 ha
```

bridges stp

PURPOSE

The `bridges stp` variable is used for working with a bridge' STP settings in the following ways:

- Configuring a bridge's STP settings
- Displaying and exporting a bridge's STP settings

When using multiple bridges, you can enable fault tolerance and optimal packet routing, by configuring Spanning Tree Protocol (STP - IEEE 802.1d). When STP is enabled, each bridge communicates with its neighboring bridges or switches to discover how they are interconnected. This information is then used to eliminate loops, while providing optimal routing of packets. STP also uses this information to provide fault tolerance, by re-computing the topology in the event that a bridge or a network link fails.

For more information on bridges and STP, refer to the User Guide.

SYNTAX

When used with `set`:

set bridges *number* stp [mode *mode*] [bridge-priority *bridge-priority*] [hello-time *hello-time*] [forward-delay-time *forward-delay-time*] [max-aging-time *max-aging-time*]

When used with `show`:

show bridges *number* stp [mode | bridge-priority | hello-time | forward-delay-time | max-aging-time]

FIELDS

`number`	Integer. The bridge's row in the Bridges table.
`mode`	String. Indicates whether to enable STP for this bridge. This can have the following values: • `enabled` - STP is enabled. • `disabled` - STP is disabled. The default value is `disabled`.

`bridge-priority`	Integer. The bridge's STP priority. The bridge's priority is combined with a bridged network's MAC address to create the bridge's ID. The bridge with the lowest ID is elected as the root bridge. The other bridges in the tree calculate the shortest distance to the root bridge, in order to eliminate loops in the topology and provide fault tolerance. To increase the chance of this bridge being elected as the root bridge, select a lower priority. Note: If you select the same priority for all bridges, the root bridge will be elected based on MAC address. This must be an integer between 0 and 61440, in increments of 4096. The default value is 32768. This field is only relevant if you want to configure STP for the bridge.
`hello-time`	Integer. The interval of time (in seconds) between transmissions of configuration BPDUs. The default value is 2 seconds. This setting is only available through the command line.
`forward-delay-time`	Integer. The amount of time (in seconds) that a port should spend in the Listening State before moving to the Learning State, or in the Learning State before moving to the Forwarding State. The default value is 15 seconds. This setting is only available through the command line.

`max-aging-time`	Integer. The maximum amount of time (in seconds) that received protocol information is stored before it is discarded. The default value is 20 seconds. This setting is only available through the command line.

EXAMPLE 1

The following command enables STP on the first bridge in the Bridges table:

```
set bridges 1 stp mode enabled
```

EXAMPLE 2

The following command displays the STP priority of the first bridge in the Bridges table:

```
show bridges 1 stp bridge-priority
```

certificate

PURPOSE

The `certificate` variable is used for working with certificates in the following ways:

- Generating a self-signed certificate
- Clearing an installed certificate

A digital certificate is a secure means of authenticating the Embedded NGX appliance to other Site-to-Site VPN Gateways. The certificate is issued by the Certificate Authority (CA) to entities such as gateways, users, or computers. The entity then uses the certificate to identify itself and provide verifiable information.

The certificate includes the Distinguished Name (DN) (identifying information) of the entity, as well as the public key (information about itself). After two entities exchange and validate each other's certificates, they can begin encrypting information between themselves using the public keys in the certificates.

The Embedded NGX appliance supports certificates encoded in the PKCS#12 (Personal Information Exchange Syntax Standard) format.

Note: If a certificate is already installed, you must clear the certificate, before generating a new one.

Note: To use certificates authentication, each Embedded NGX appliance should have a unique certificate. Do not use the same certificate for more than one gateway.

Note: If your Embedded NGX appliance is centrally managed, a certificate is automatically generated and downloaded to your appliance. In this case, there is no need to generate a self-signed certificate.

SYNTAX

When used with `add`:

add certificate country *country* organization *organization* unit *unit* gatewayname *gatewayname* expyear *expyear* expmonth *expmonth* expday *expday*

When used with `clear`:

clear certificate

FIELDS

`country`	String. The country code of the country in which you are located. For a list of country codes, see ***Country Codes*** on page 807.
`organization`	String. The name of your organization.
`unit`	String. The name of your division.
`gatewayname`	String. The gateway's name. This name will appear on the certificate, and will be visible to remote users inspecting the certificate.
`expyear`	Integer. The year when this certificate should expire. This can be any year until 2037. Note: You must renew the certificate when it expires.
`expmonth`	Integer. The month when this certificate should expire. This can be any number between 1 and 12.
`expday`	Integer. The day when this certificate should expire. This can be any number between 1 and 31.

EXAMPLE 1

The following command generates a self-signed certificate for the gateway 00:08:DA:77:70:70, where the organization is MyCompany, the division is Marketing, the country is Great Britain, and the certificate's expiration date is December 31, 2014.

```
add cert country GB organization MyCompany unit Marketing gatewayname
00:08:DA:77:70:70 expyear 2014 expmonth 12 expday 31
```

EXAMPLE 2

The following command clears the installed certificate:

```
clear certificate
```

clock

PURPOSE

The `clock` variable is used for working with clock settings in the following ways:

- Setting the appliance time
- Displaying and exporting the appliance clock settings

SYNTAX

When used with `set`:

set clock [time *time*] [day *day*] [month *month*] [year *year*] [timezone *timezone*] [ntp1 *ntp1*] [ntp2 *ntp2*]

When used with `show`:

show clock [time | day | month | year | timezone | ntp1 | ntp2]

FIELDS

`time`	String. The current time, in the format: `HH:MM:SS<meridian>` where `HH` = hours `MM` = minutes `SS` = seconds `<meridian>` = AM or PM
`day`	Integer. The day of the month. For example, 4.
`month`	Integer. The current month. For example, December is 12.
`year`	Integer. The current year.

`timezone`	String. The local time zone, in the format: `GMT<sign>HH:MM` where: `<sign>` = + or - `HH` = hours `MM` = minutes For example, GMT+05:00 or GMT-04:00.
`ntp1`	String. The IP address of the Primary NTP server.
`ntp2`	String. The IP address of the Secondary NTP server.

EXAMPLE 1

The following command sets the time to January 2, 2008, 12:00 PM:

```
set clock time 12:00:00PM day 2 month 1 year 2008
```

EXAMPLE 2

The following command shows the first NTP server configured for the appliance:

```
show clock ntp1
```

device

PURPOSE

The `device` variable is used for working with device settings in the following ways:

- Setting device details, including Product Key and hostname
- Specifying whether the appliance is located behind a NAT device
- Displaying and exporting the above device details
- Displaying and exporting all device details, including internal DNS server settings.

  For information on configuring, displaying, and exporting specific internal DNS server settings, see ***device dns*** on page 300.

SYNTAX

When used with `set`:

set device [behindnat *behindnat*] [hostname *hostname*] [productkey *productkey*]

When used with `show`:

show device [behindnat | hostname | productkey]

FIELDS

`behindnat`

IP Address or String. Indicates whether the appliance is located behind a NAT device.

This can have the following values:

- The NAT device's IP address. This address will be used as the appliance's public IP address.
- `undefined` - The appliance is not located behind a NAT device.

This setting is only available through the command line.

`hostname`	String. The hostname used to identify the gateway. Note: Configuring the gateway hostname is only available if the Embedded NGX is not subscribed to the Remote Management service. When remotely managed, the gateway hostname is set by the Service Center.
`productkey`	String. The Product Key.

EXAMPLE 1

The following command sets the hostname to "mycomputer1" and the Product Key to "aaaaaa-bbbbbb-cccccc":

```
set device hostname mycomputer1 productkey aaaaaa-bbbbbb-cccccc
```

EXAMPLE 2

The following command displays the appliance's public IP address:

```
show device behindnat
```

device dns

PURPOSE

The `device dns` variable is used for working with internal DNS server settings in the following ways:

- Configuring internal DNS server settings
- Displaying and exporting internal DNS server settings

The Embedded NGX appliance includes an internal DNS server, which can resolve DNS names for internal network hosts defined as network objects. The name of the network object representing a host is used as the host's DNS name. For example, if a computer with the IP address 192.188.22.1 is represented by a network object called "server1", then the computer's DNS name will be "server1", and the internal DNS server will reply to all internal hosts' DNS requests for "server1" with the IP address 192.188.22.1.

Note: The internal DNS server responds to DNS requests from internal network hosts only. It does not respond to requests from the Internet.

In addition, the internal DNS server can be configured with a domain name suffix, in which case it will also resolve DNS names in the format `<dnsname>.<domainsuffix>`. For example, if the DNS suffix is “mycompany.com”, the internal DNS server will reply to all internal hosts' DNS requests for "server1.mycompany.com" with the IP address 192.188.22.1.

If a gateway hostname is defined, the DNS server will reply to DNS requests in the format `<hostname>.<domainsuffix>` with the gateway’s internal IP address. For information on configuring the gateway's hostname, see ***device*** on page 298.

SYNTAX

When used with `set`:

set device dns [**resolving** *resolving*] [**domain-name** *domain-name*]

When used with `show`:

show device dns [**resolving** | **domain-name**]

FIELDS

`resolving`	String. Indicates the internal DNS server is enabled. This can have the following values: • `enabled` - The internal DNS server is enabled. • `disabled` - The internal DNS server is disabled. The default value is `disabled`. If the internal DNS server is enabled, you must set the `domain-name` field.
`domain-name`	String. The domain name suffix that the internal DNS server should resolve.

EXAMPLE 1

The following command enables the internal DNS server and configures it with the domain name suffix "mycompany.com":

```
set device dns resolving enabled domain-name mycompany.com
```

EXAMPLE 2

The following command displays all internal DNS server settings:

```
show device dns
```

dhcp scopes

PURPOSE

The `dhcp scopes` variable is used for working with DHCP (Dynamic Host Configuration Protocol) scopes in the following ways:

- Adding a DHCP scope for a settings for an internal network
- Modifying an internal network's DHCP scope
- Deleting an internal network's DHCP scope
- Displaying and exporting DHCP scopes
- Clearing the DHCP Scopes table

An internal network's DHCP scope specifies a set of custom DHCP settings.

SYNTAX

When used with `add`:

add dhcp scopes network *network* [domain *domain*] [dns *dns*] [dns1 *dns1*] [dns2 *dns2*] [wins *wins*] [wins1 *wins1*] [wins2 *wins2*] [ntp1 *ntp1*] [ntp2 *ntp2*] [callmgr1 *callmgr1*] [callmgr2 *callmgr2*] [tftpserver *tftpserver*] [tftpbootfile *tftpbootfile*] [xwin-dispmgr *xwin-dispmgr*] [default-gw *default-gw*] [avaya-voip-param *avaya-voip-param*] [nortel-voip-param *nortel-voip-param*] [thomson-voip-param *thomson-voip-param*] [wyse-rapport-server *wyse-rapport-server*] [wyse-rapport-port *wyse-rapport-port*]

When used with `set`:

set dhcp scopes *number* [network *network*] [domain *domain*] [dns *dns*] [dns1 *dns1*] [dns2 *dns2*] [wins *wins*] [wins1 *wins1*] [wins2 *wins2*] [ntp1 *ntp1*] [ntp2 *ntp2*] [callmgr1 *callmgr1*] [callmgr2 *callmgr2*] [tftpserver *tftpserver*] [tftpbootfile *tftpbootfile*] [xwin-dispmgr *xwin-dispmgr*] [default-gw *default-gw*] [avaya-voip-param *avaya-voip-param*] [nortel-voip-param *nortel-voip-param*] [thomson-voip-param *thomson-voip-param*] [wyse-rapport-server *wyse-rapport-server*] [wyse-rapport-port *wyse-rapport-port*]

When used with `delete`:

delete dhcp scopes *number*

When used with `show`:

show dhcp scopes [*number*] [network | domain | dns dns | dns1 | dns2 | wins | wins1 | wins2 | ntp1 | ntp2 | callmgr1 | callmgr2 | tftpserver | tftpbootfile | xwin-dispmgr | default-gw | avaya-voip-param | nortel-voip-param | thomson-voip-param | wyse-rapport-server | wyse-rapport-port]

When used with `clear`:

clear dhcp scopes

FIELDS

number	Integer. The DHCP scope's row in the DHCP Scopes table.
`network`	String. The name of the network whose DHCP scope you want to affect. This can have the following values: • `lan` • `dmz` • `officemode` • `wlan` • The name of a VLAN network
`domain`	String. A default domain suffix that should be passed to DHCP clients. The DHCP client will automatically append the domain suffix for the resolving of non-fully qualified names. For example, if the domain suffix is set to "mydomain.com", and the client tries to resolve the name “mail”, the suffix will be automatically appended to the name, resulting in “mail.mydomain.com”.

`dns`

String. The DNS server mode. This can have the following values:

- `automatic` - The gateway should act as a DNS relay server and automatically pass its own IP address to DHCP clients. This is the recommended value.
- `manual` - The gateway should not act as a DNS relay server. Instead, the DNS servers specified in the `dns1` and `dns2` fields should be used.
- `none` - No DNS server is used.

The default value is `automatic`.

If this field is set to `manual`, the `dns1` and `dns2` fields must be specified.

`dns1`

IP Address or String. The IP address of the Primary DNS server to pass to DHCP clients instead of the gateway. This can have the following values:

- An IP address
- `undefined` - The Primary DNS server is not defined.

The default value is `undefined`.

This field is only relevant if the `dns` field is set to `manual`.

`dns2`

IP Address or String. The IP address of the Secondary DNS server to pass to DHCP clients instead of the gateway. This can have the following values:

- An IP address
- `undefined` - The Secondary DNS server is not defined.

The default value is `undefined`.

This field is only relevant if the `dns` field is set to `manual`.

`wins`

String. The WINS server mode. This can have the following values:

- `automatic` - DHCP clients should be automatically assigned the same WINS servers as specified by the Internet connection.
- `manual` - DHCP clients should not be automatically assigned the WINS servers specified by the Internet connection. Instead, the WINS servers specified in the `wins1` and `wins2` fields should be used.
- `none` - No WINS server is used.

The default value is `automatic`.

If this field is set to `manual`, the `wins1` and `wins2` fields must be specified.

`wins1`

IP Address or String. The IP address of the Primary WINS server to use instead of the gateway. This can have the following values:

- An IP address
- `undefined` - The Primary WINS server is not defined.

The default value is `undefined`.

This field is only relevant if the `wins` field is set to `manual`.

`wins2`

IP Address or String. The IP address of the Secondary WINS server to use instead of the gateway. This can have the following values:

- An IP address
- `undefined` - The Secondary WINS server is not defined.

The default value is `undefined`.

This field is only relevant if the `wins` field is set to `manual`.

`ntp1`

IP Address or String. The IP address of the Primary Network Time Protocol (NTP) server to use for synchronizing the time on the DHCP clients. This can have the following values:

- An IP address
- `undefined` - The Primary NTP server is not defined.

The default value is `undefined`.

`ntp2`

IP Address or String. The IP address of the Secondary NTP server to use for synchronizing the time on the DHCP clients. This can have the following values:

- An IP address
- `undefined` - The Secondary NTP server is not defined.

The default value is `undefined`.

`callmgr1`

IP Address or String. The IP address of the Primary Voice over Internet Protocol (VoIP) call managers to assign to the IP phones. This can have the following values:

- An IP address
- `undefined` - The Primary VoIP server is not defined.

The default value is `undefined`.

`callmgr2`

IP Address or String. The IP address of the Secondary VoIP call managers to assign to the IP phones. This can have the following values:

- An IP address
- `undefined` - The Secondary VoIP server is not defined.

The default value is `undefined`.

`tftpserver`

IP Address or String. The IP address of the Trivial File Transfer Protocol (TFTP) server to assign to the DHCP clients. TFTP enables booting diskless computers over the network.

This can have the following values:

- An IP address
- `undefined` - The TFTP server is not defined.

The default value is `undefined`.

`tftpbootfile`

String. The full path of the boot file to use for booting DHCP clients via TFTP.

This field is only relevant if a TFTP server is defined in the `tftpserver` field.

`xwin-dispmgr`

IP Address or String. The IP address of the X-Windows Display Manager to assign to X-Windows terminals when booting via DHCP.

This can have the following values:

- An IP address
- `undefined` - The XDM server is not defined.

The default value is `undefined`.

`default-gw`

IP Address or String. The IP address to pass to DHCP clients as the default gateway, instead of the current gateway IP address.

This can have the following values:

- An IP address
- `undefined` - The DHCP server will pass the current gateway IP address to DHCP clients as the default gateway's IP address.

The default value is `undefined`.

`avaya-voip-param`	String. The configuration string with which to configure Avaya IP phones.
`nortel-voip-param`	String. The configuration string with which to configure Nortel IP phones.
`thomson-voip-param`	String. The configuration string with which to configure Thomson IP phones.
`wyse-rapport-server`	IP Address or String. The IP address of the Wyse Rapport Web server to assign Wyse thin clients when booting via DHCP. This can have the following values: • An IP address • `undefined` - A Wyse Rapport Web server is not defined. The default value is `undefined`. This setting is only available through the command line.
`wyse-rapport-port`	Integer. The Wyse Rapport Web server's port. This field is only relevant if a Wyse Rapport Web server is defined in the `wyse-rapport-server` field. This setting is only available through the command line.

EXAMPLE 1

The following command adds a DHCP scope for the LAN network and specifies the default domain suffix "mydomain.com".

```
add dhcp scopes network lan domain mydomain.com
```

EXAMPLE 2

The following command modifies scope 1 in the DHCP Scope table, so that the TFTP server is 1.2.3.4:

```
set dhcp scopes 1 tftpserver 1.2.3.4
```

EXAMPLE 3

The following command deletes scope 1 from the DHCP Scope table:

```
delete dhcp scopes 1
```

EXAMPLE 4

The following command displays all DHCP settings for scope 2:

```
show dhcp scopes 2
```

EXAMPLE 5

The following command clears all scopes in the DHCP Scope table:

```
clear dhcp scopes
```

dialup

PURPOSE

The `dialup` variable is used for working with RS232 dialup modem settings in the following ways:

- Setting up an RS232 dialup modem
- Displaying and exporting RS232 dialup modem settings

You can use an RS232 dialup modem as a primary or secondary Internet connection method. This is useful in locations where broadband Internet access is unavailable. When used as a backup Internet connection, the Embedded NGX appliance automatically dials the modem if the primary Internet connection fails. The modem can be automatically disconnected when not in use.

Note: Before setting up the RS232 dialup modem, you must connect it to your Embedded NGX appliance's Serial port. You can use either a regular or ISDN dialup modem.

Note: Your RS232 dialup modem and your Embedded NGX appliance's Serial port must be configured for the same speed.

By default, the appliance's Serial port's speed is 57600 bps. For information on changing the Serial port's speed, *see port serial* on page 509.

Note: After you have finished setting up the modem, you must configure a Dialup Internet connection.
If you want to use the dialup connection as a backup connection, you must configure a LAN or broadband connection as the primary Internet connection, and configure the Dialup connection as the secondary Internet connection. Refer to the User Guide and to ***net wan2*** on page *430*.

For information on setting up a USB dialup modem, see ***usb modems*** on page 670.

SYNTAX

When used with `set`:

set dialup [type *type*] [dialmode *dialmode*] [incoming-ppp *incoming-ppp*] [custominit *custominit*]

When used with `show`:

set dialup [type | dialmode | incoming-ppp | custominit]

FIELDS

`type`

String. The modem type. This can have the following values:

- `Custom` - A custom modem.
  If the modem type is `Custom`, you must include the `custominitstring` field.
- `Hayes Accura 56K`
- `USRobotics Courier I-Modem ISDN/v.34`
- `NetCruiser 56K (Conexant Chipset)`
- `WebExcel 56K (Ambient Chipset)`
- `Generic Modem 1`
- `Generic Modem 2`
- `Generic Modem 3`
- `Generic ISDN (Async > Sync PPP)`
- `Generic ISDN (Sync PPP 64K)`
- `Generic ISDN (Sync PPP 128K Dual channel)`

Reminder: The values are case-sensitive. To enter a string containing spaces, enclose the string in quotation marks.

`dialmode`	String. The dial mode the modem uses. This can have the following values: • `tone` • `pulse` The default value is `tone`.
`incoming-ppp`	String. Indicates whether the modem should answer incoming PPP calls. This allows accessing the appliance out of band for maintenance purposes, in case the primary Internet connection fails. This can have the following values: • `enabled` - The modem will answer incoming PPP calls. • `disabled` - The modem will not answer incoming PPP calls. The default value is `disabled`. The client is assigned an IP address from the OfficeMode network; therefore, the OfficeMode network must be enabled. For information on enabling the OfficeMode network, see ***net officemode*** on page 395.
`custominit`	String. The installation string for the custom modem type. This information is provided automatically if a standard modem type is used.

EXAMPLE 1

The following command sets up a custom modem with the installation string AT&F. The dial mode is tone.

```
set dialup type "Hayes Accura 56K" dialmode tone custominit AT&F
```

EXAMPLE 2

The following command displays all dialup modem settings:

```
show dialup
```

dvmrp

PURPOSE

The `dvmrp` variable is used for working with Distance Vector Multicast Routing Protocol (DVMRP) settings in the following ways:

- Enabling/disabling DVMRP
- Displaying and exporting the DVMRP mode

The Embedded NGX appliance supports DVMRP version 2 multicast routing protocol. DVMRP is useful if you need to use multicast routing in a dense environment.

These settings are only relevant for N series appliances, and they are only available through the command line.

Note: To use DVMRP, your Embedded NGX appliance must be installed with a DVMRP-enabled firmware. Such firmwares do not have a "b" appended to their version number. For example 8.2.21x supports DVMRP, but 8.2.21xb does not.

DVMRP-enabled firmwares do not support BGP.

Note: The DVMRP and PIM-SM routers cannot be used simultaneously.

SYNTAX

When used with `set`:

set dvmrp mode *mode*

When used with `show`:

show dvmrp [mode]

FIELDS

`mode`	String. The DVMRP mode. This can have the following values: • `disable` - DVMRP is disabled. • `internal` - DVMRP is enabled for internal routes only. • `all` - DVMRP is enabled for all routes. This mode supports route-based VPN. The default value is `disable`.

EXAMPLE 1

The following command enables DVMRP for all networks:

```
set dvmrp mode all
```

EXAMPLE 2

The following command displays all DVMRP settings:

```
show dvmrp
```

fw

PURPOSE

The `fw` variable is used for working with firewall settings in the following ways:

- Defining an exposed host

  If you need to allow unlimited incoming and outgoing connections between the Internet and a particular host, you can define an exposed host. An exposed host is not protected by the firewall, and it receives all traffic that was not forwarded to another computer by use of Allow and Forward rules.

- Setting the firewall level
- Displaying and exporting the above firewall settings
- Displaying and exporting all firewall settings, including:
  - Firewall rules
  - Server rules
  - Advanced firewall protections

  For information on displaying and exporting specific firewall rules, server rules, and advanced firewall protections, see ***fw rules*** on page 322, ***fw servers*** on page 332, and ***fw advanced*** on page 319.

Warning: Defining an exposed host is not recommended unless you are fully aware of the security risks. For example, an exposed host may be vulnerable to hacker attacks.

SYNTAX

When used with `set`:

set fw [exposedhost *exposedhost*] [level *level*]

When used with `show`:

show fw [exposedhost | level]

FIELDS

`exposedhost`

IP Address or String. The IP address of the computer you want to define as an exposed host.

This can have the following values:

- An IP address
- `undefined` - An exposed host is not defined.

The default value is `undefined`.

`level`

String. The firewall security level. This can have the following values:

- `low` - Enforces basic control on incoming connections, while permitting all outgoing connections.
  All inbound traffic is blocked to the external Embedded NGX appliance IP address, except for ICMP echoes ("pings"). All outbound connections are allowed.
- `medium` - Enforces strict control on all incoming connections, while permitting safe outgoing connections.
  This is the default level and is recommended for most cases. Leave it unchanged unless you have a specific need for a higher or lower security level.
  All inbound traffic is blocked. All outbound traffic is allowed to the Internet except for Windows file sharing (NBT ports 137, 138, 139 and 445).

- `high` - Enforces strict control on all incoming and outgoing connections. All inbound traffic is blocked. Restricts all outbound traffic except for the following: Web traffic (HTTP, HTTPS), email (IMAP, POP3, SMTP), ftp, newsgroups, Telnet, DNS, IPSEC IKE and VPN traffic.
- `blockall` - Blocks all access between Embedded NGX networks. All inbound and outbound traffic is blocked between the WAN, LAN, DMZ, primary WLAN, VLANs, VAPs, and OfficeMode networks.
  This does not affect traffic to and from the gateway itself.

Note: The definitions of firewall security levels provided here represent the Embedded NGX appliance's default security policy. Security updates downloaded from a Service Center may alter this policy and change these definitions, and may also prevent the changing of this field.

EXAMPLE 1

The following command sets the firewall level to High:

```
set fw level high
```

EXAMPLE 2

The following command displays all firewall settings, including firewall rules and server rules:

```
show fw
```

fw advanced

PURPOSE

The `fw advanced` variable is used for configuring and displaying advanced firewall settings.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set fw advanced [excessive-logging-protection *excessive-logging-protection*] [udp-port-0 *udp-port-0*] [arp-filter *arp-filter*]

When used with `show`:

show fw advanced [excessive-logging-protection | udp-port-0 | arp-filter]

FIELDS

`excessive-logging-protection`

String. Indicates whether protection against excessive logging attacks is enabled.

In an excessive logging attack, an attacker performs a large number of identical attacks against the gateway. These attacks serve either to overload the logging mechanism of the firewall, or to conceal other criminal operations by hiding them among a large number of log messages.

This can have the following values:

- `true` - Protection against excessive logging attacks is enabled.
- `false` - Protection against excessive logging attacks is disabled.

The default value is `true`.

Note: It is highly recommended to leave this setting on the default value.

`udp-port-0`

String. Indicates whether to allow incoming and outgoing traffic on UDP port 0. Blocking such traffic protects against UDP port 0 Denial of Service attacks.

This can have the following values:

- `allow` - Allow traffic on UDP port 0.
- `block` - Block all traffic on UDP port 0.

The default value is `block`.

Note: It is highly recommended to leave this setting on the default value.

`arp-filter`

String. Indicates whether to enable selective Address Resolution Protocol (ARP) table updates for requests originating from the external interfaces.

This can have the following values:

- `enabled` - Enable ARP table updates for requests from external interfaces.
- `disabled` - Disable ARP table updates for requests from external interfaces.

The default value is `disabled`.

Note: Enabling this setting is not recommended for cable Internet connections.

EXAMPLE 1

The following command enables the protection against excessive logging attacks:

```
set fw advanced excessive-logging-protection true
```

EXAMPLE 2

The following command displays the advanced firewall protection settings:

```
show fw advanced
```

fw rules

PURPOSE

The `fw rules` variable is used for working with firewall rules in the following ways:

- Adding new firewall rules
- Modifying firewall rules
- Deleting firewall rules
- Displaying and exporting firewall rules
- Clearing the Firewall Rules table

The Embedded NGX appliance checks the protocol used, the ports range, and the destination IP address, when deciding whether to allow or block traffic. By default, in the Medium security level, the Embedded NGX appliance blocks all connection attempts from the Internet (WAN) to the LAN, and allows all outgoing connection attempts from the LAN to the Internet (WAN). For further information on the default security policy, refer to the User Guide.

User-defined rules have priority over the default rules and provide you with greater flexibility in defining and customizing your security policy. For detailed information on the rule types, refer to the User Guide.

The Embedded NGX appliance processes user-defined rules in the order they appear in the Firewall Rules table, so that rule 1 is applied before rule 2, and so on. This enables you to define exceptions to rules, by placing the exceptions higher up in the Firewall Rules table.

SYNTAX

When used with `add`:

add fw rules action *action* [service *service*] [src *src*] [dest *dest*] [forward-to *forward-to*] [ports *ports*] [protocol *protocol*] [qosclass *qosclass*] [redirectport *redirectport*] [index *index*] [log *log*] [disabled *disabled*] [description *description*] [time *time*]

When used with `set`:

set fw rules *number* [action *action*] [service *service*] [src *src*] [dest *dest*] [forward-to *forward-to*] [ports *ports*] [protocol *protocol*] [qosclass *qosclass*] [redirectport *redirectport*] [index *index*] [log *log*] [disabled *disabled*] [description *description*] [time *time*]

When used with `delete`:

delete fw rules *number*

When used with `show`:

show fw rules [*number*] [action | service | src | dest | forward-to | ports | protocol | qosclass | redirectport | index | log | disabled | description | time]

When used with `clear`:

clear fw rules

FIELDS

`number`	Integer. The firewall rule's row in the Firewall Rules table.
`action`	String. The type of rule you want to create. This can have the following values: • `allowandforward` - An Allow and Forward rule • `allow` - An Allow rule • `block` - A Block rule For detailed information on the rule types, refer to the User Guide.

`service`

Integer or String. The service to which the rule should apply.

This can have the following values:

- `custom` - The rule should apply to a specific non-standard service. You must include the `protocol` and `ports` fields.
- `0` or `any` - The rule should apply to any service.
- `80` or `web`
- `21` or `ftp`
- `23` or `telnet`
- `25` or `smtp`
- `110` or `pop3`
- `137` or `nbt`
- `500` or `vpn`
- `1720` or `h323`
- `1723` or `pptp`
- The name of a network service object

The default value is `0` or `any`.

`src`

IP Address or String. The source of the connections you want to allow/block. This can have the following values:

- An IP address
- An IP address range - To specify a range, use the following format:
  `<Start IP Address>-<End IP Address>`
- `any` - The rule should apply to any source.
- `wan`
- `wan2`
- `lan`
- `dmz`
- `officemode`
- `vpn`
- `notvpn` - Not VPN
- The name of a VPN site
- The name of a network object
- The name of a bridge
- The name of a VLAN
- The name of a VAP
- The name of a WDS link

The default value is `any`.

`dest`

IP Address or String. Select the destination of the connections you want to allow or block. This can have the following values:

- An IP address
- An IP address range - To specify a range, use the following format:
  `<Start IP Address>-<End IP Address>`
- `any` - The rule should apply to any destination.
- `wan`
- `wan2`
- `lan`
- `dmz`
- `officemode`
- `vpn`
- `notvpn` - Not VPN
- The name of a VPN site
- The name of a network object
- The name of a bridge
- The name of a VLAN
- The name of a VAP
- The name of a WDS link

The default value is `any`.

`forward-to`

IP Address or String. The destination to which matching connections should be forwarded.

- An IP address
- The name of a VPN site
- The name of a network object
- `undefined` - No forwarding destination is defined.

The default value is `undefined`.

This field is only relevant when defining an Allow and Forward rule.

`ports`

Integer. The ports to which the rule applies. This can have the following values:

- A port number - The rule will apply to this port only.
- A port range - To specify a range, use the following format:
  `<Start Port Number>-<End Port Number>`

Note: If you do not enter a port or port range, the rule will apply to all ports.

`protocol`

String. The protocol for which the rule should apply. This can have the following values:

- `any` - The rule should apply to any protocol.
- `tcp`
- `icmp`
- `udp`
- `gre`
- `esp`
- `ospf`
- `igmp`
- A protocol number

The default value is `any`.

`qosclass`

String. An existing QoS class to which you want to assign the specified connections.

If Traffic Shaper is enabled, Traffic Shaper will handle these connections as specified in the bandwidth policy for the selected QoS class. If Traffic Shaper is not enabled, this setting is ignored. For information on Traffic Shaper and QoS classes, refer to the User Guide.

This field is only relevant when defining an Allow rule or an Allow and Forward rule.

If you do not include this field, the connections are assigned to the Default QoS class.

`redirectport`

Integer. The port to which you want to redirect the specified connections.

This option is called Port Address Translation (PAT).

This field is only relevant when defining an Allow and Forward rule.

`index`	Integer. The firewall rule's row in the Firewall Rules table. Use this field to move the rule up or down in the Firewall Rules table. The appliance processes rules higher up in the table (lower indexes) before rules lower down in the table (higher indexes). If you do not include this field when adding a rule, the rule is automatically added to the bottom of the Firewall Rules table.
`log`	String. Indicates whether to log the specified blocked or allowed connections. This can have the following values: • `true` - Log the specified connections. • `false` - Do not log the specified connections. By default, accepted connections are not logged, and blocked connections are logged.
`disabled`	String. Indicates whether the rule is disabled. This can have the following values: • `true` - The rule is disabled. • `false` - The rule is enabled. The default value is `true`.
`description`	String. A description of the rule.

`time`

String. The time range during which the rule should be applied.

This can have the following values:

- `always` - The rule is applied at all times.
- A specific time range in the format:
  `hh[:mm][meridian]-hh[:mm][meridian]`
  where:
  `hh` = hours, either in 24-hour or 12-hour clock notation; when using 12-hour clock notation, you must specify the meridian.
  `mm` = minutes
  `meridian` = am or pm; applicable *only* when using 12-hour clock notation.
  For example, both of the following time ranges are acceptable: "3:30pm-6:30pm" and "15:30-18:30". However, "15:30pm-18:30pm" is not acceptable.

EXAMPLE 1

The following command creates an Allow rule for FTP connections from the WAN to the LAN and assigns these connections to the Important QoS class:

```
add fw rules action allow service ftp action allow src wan dest lan
qosclass Important
```

EXAMPLE 2

The following command modifies rule 1 in the Firewall Rule table, so that it becomes a Block rule:

```
set fw rules 1 action block
```

EXAMPLE 3

The following command deletes rule 1 in the Firewall Rule table:

```
delete fw rules 1
```

EXAMPLE 4

The following command displays the destination IP address for rule 1 in the Firewall Rule table:

```
show fw rules 1 dest
```

EXAMPLE 5

The following command deletes all rules in the Firewall Rule table:

```
clear fw rules
```

fw servers

PURPOSE

The `fw servers` variable is used for working with servers in the following ways:

- Configuring servers
- Deleting servers
- Displaying and exporting servers

You configure servers in order to selectively allow incoming network connections into your network. For example, you can set up your own Web server, Mail server or FTP server. This is useful if you want to host public Internet servers in your network.

Note: Configuring servers is equivalent to creating simple Allow and Forward rules for common services, where the destination is This Gateway. For information on creating more complex rules, see ***fw rules*** on page *322*.

SYNTAX

When used with `set`:

set fw servers *service* [**hostip** *hostip*] [**enconly** *encoly*]

When used with `delete`:

delete fw servers *service*

When used with `show`:

show fw servers [*service*] [**hostip** | **enconly**]

FIELDS

`service` — String. The desired service or application. This can have the following values:

- `web`
- `ftp`
- `telnet`
- `pop3`
- `smtp`
- `pptp`
- `ipsec`
- `nbt`
- `h323`

`hostip` — IP Address or String. The IP address of the computer that will run the service (one of your network computers). This can have the following values:

- An IP address
- `undefined` - The service is not configured.

The default value is `undefined`.

`enconly` — String. Indicates whether to allow only connections made through a VPN. This can have the following values:

- `true` - Allow only connections through a VPN.
- `false` - Allow all connections.

The default value is `false`.

Note: If you did not specify a host IP address for the service, changes to this field will not take effect.

EXAMPLE 1

The following command allows FTP connections made through a VPN only:

```
set fw servers ftp hostip 192.168.10.21 enconly true
```

EXAMPLE 2

The following command deletes the defined FTP server:

```
delete fw servers ftp
```

EXAMPLE 3

The following command displays the FTP server's IP address:

```
show fw servers ftp hostip
```

ha

PURPOSE

The ha variable is used for working with High Availability settings in the following ways:

- Configuring High Availability settings
- Displaying and exporting High Availability network settings, including Internet connection tracking settings and High Availability effect settings

  For information on configuring, displaying, and exporting specific Internet connection tracking settings, see ***ha track*** on page 341. For information on configuring, displaying, and exporting specific High Availability effect settings, see ***ha effect*** on page 338.

You can create a High Availability cluster consisting of two or more Embedded NGX appliances. For example, you can install two Embedded NGX appliances on your network, one acting as the "Master", the default gateway through which all network traffic is routed, and one acting as the "Backup". If the Master fails, the Backup automatically and transparently takes over all the roles of the Master. This ensures that your network is consistently protected by a Embedded NGX appliance and connected to the Internet.

The Embedded NGX appliance supports configuring multiple HA clusters on the same network segment. To this end, each cluster must be assigned a unique ID number.

For more information on High Availability, its requirements, and how to set it up, refer to the User Guide.

Note: After configuring High Availability using the ha variable, you must configure a virtual IP address for each internal network or bridge for which you want to enable High Availability. For instructions, see ***net dmz ha*** on page *376*, ***net lan ha*** on page *390*, ***net wlan ha*** on page *445*, ***vlan*** on page *686*, and ***bridges ha*** on page *288*.

If you want to ensure that Passive Gateways are connected to the Internet at all times, configure a virtual IP address for the WAN or WAN2 interface, as well. For instructions, see ***net wan ha*** on page 420 and ***net wan2 ha*** on page 435. The Internet connection must be configured as "LAN - Static IP".

SYNTAX

When used with `set`:

set ha [mode *mode*] [syncinterface *syncinterface*] [priority *priority*] [groupid *groupid*]

When used with `show`:

show ha [mode | syncinterface | priority | groupid]

FIELDS

`mode`

String. The appliance's High Availability mode. This can have the following values:

- `enabled` - High Availability is enabled on this appliance.
- `disabled` - High Availability is not enabled on this appliance.

The default value is `disabled`.

`syncinterface`

String. The network you want to use as the synchronization interface. The Active Gateway sends periodic signals, or "heartbeats", to the network via the synchronization interface.

This can have the following values:

- `lan` - The LAN network.
- `dmz` - The DMZ network.
- The name of a VLAN network
- The name of a bridge
- `undefined` - The synchronization interface is not defined.

The default value is `undefined`.

Note: If High Availability is enabled, then the synchronization interface must be defined.

Note: The synchronization interface must be the same for all gateways in the High Availability cluster, and must always be connected and enabled on all gateways. Otherwise, multiple

	appliances may become active, causing unpredictable problems. The synchronization interface must have a virtual IP address, which can be set using the command set net *x* ha, where *x* is the network name (lan, dmz, or wlan).
`priority`	Integer. The gateway's priority. This determines the gateway's role: the gateway with the highest priority in the cluster is the Active Gateway and uses the virtual IP address, and the rest of the gateways are Passive Gateways. This must be an integer between 1 and 255.
`groupid`	Integer. The ID number of the cluster to which the gateway should belong. This must be an integer between 1 and 255. The default value is 55. This field is only relevant if there are multiple HA clusters on the same network segment. If only one HA cluster exists, there is no need to change the default value.

EXAMPLE 1

The following command enables High Availability on the appliance. The synchronization interface is the LAN network, the gateway's priority is 100, and the gateway is assigned to cluster 56.

```
set ha mode enabled syncinterface lan priority 100 groupid 56
```

EXAMPLE 2

The following command displays the appliance's priority:

```
show ha priority
```

ha effect

PURPOSE

The `ha effect` variable is used for working with High Availability effect settings in the following ways:

- Configuring the desired effect of the gateway's High Availability status on VPN, OSPF, BGP, and RIP
- Displaying and exporting this setting

When High Availability is enabled, you can specify whether the gateways' status within the High Availability cluster should affect VPN tunnels.

For information on configuring High Availability, see ***ha*** on page 335.

SYNTAX

When used with `set`:

set ha effect [**vpn** *vpn*] [**ospf** *ospf*] [**bgp** *bgp*] [**rip** *rip*] [**multicast** *multicast*]

When used with `show`:

show ha effect [**vpn** | **ospf** | **bgp** | **rip**]

FIELDS

vpn	String. Indicates whether the gateway's status within the High Availability cluster should affect existing VPN tunnels. This can have the following values: • `enabled` - When the gateway's status is Passive, all existing VPN tunnels are automatically terminated. • `disabled` - The gateway's status has no effect on VPN tunnels. The default value is `enabled`.

`ospf`

String. Indicates whether the gateway's status within the High Availability cluster should affect Open Shortest Path First (OSPF) dynamic routing. This can have the following values:

- `enabled` - When the gateway's status is Passive, disable OSPF.
- `disabled` - The gateway's status has no effect on OSPF.

The default value is `enabled`.

`bgp`

String. Indicates whether the gateways' status within the High Availability cluster should affect Border Gateway Protocol (BGP) dynamic routing. This can have the following values:

- `enabled` - When the gateway's status is Passive, disable BGP.
- `disabled` - The gateway's status has no effect on BGP.

The default value is `enabled`.

`rip`

String. Indicates whether the gateways' status within the High Availability cluster should affect Routing Information Protocol (RIP) dynamic routing. This can have the following values:

- `enabled` - When the gateway's status is Passive, disable RIP.
- `disabled` - The gateway's status has no effect on RIP.

The default value is `enabled`.

This field is only relevant for N series appliances.

`multicast`	String. Indicates whether the gateways' status within the High Availability cluster should affect Distance Vector Multicast Routing Protocol (DVMRP) and Protocol Independent Multicast - Sparse-Mode (PIM-SM) multicast routing . This can have the following values: • `enabled` - When the gateway's status is Passive, disable multicast routing. • `disabled` - The gateway's status has no effect on multicast routing. The default value is `enabled`. This field is only relevant for N series appliances.

EXAMPLE 1

The following command disables the High Availability effect on VPN tunnels:

```
set ha effect vpn disabled
```

EXAMPLE 2

The following command displays all High Availability effect settings:

```
show ha effect
```

ha track

PURPOSE

The `ha track` variable is used for working with Internet connection tracking settings in the following ways:

- Configuring interface tracking
- Displaying and exporting interface tracking settings

When High Availability is enabled, you can configure Internet connection tracking: each appliance tracks its Internet connection's status and reduces its own priority by a user-specified amount, if its Internet connection goes down. If the Active Gateway's priority drops below another gateway's priority, then the other gateway becomes the Active Gateway.

Note: You can also track the status of the LAN and DMZ ports by using the command `set port lan1 hatrack` and `set port dmz hatrack`. For information, see ***port lan*** on page *506* and ***port dmz*** on page *500*.

For information on configuring High Availability, see ***ha*** on page 335.

SYNTAX

When used with `set`:

set ha track [wan1 *wan1*] [wan2 *wan2*]

When used with `show`:

show ha track [wan1 | wan2]

FIELDS

wan1	Integer. The amount to reduce the gateway's priority if the primary Internet connection goes down. This must be an integer between 0 and 255. The default value is 0.
wan2	Integer. The amount to reduce the gateway's priority if the secondary Internet connection goes down. This must be an integer between 0 and 255. The default value is 0.

EXAMPLE 1

The following command enables Internet connection tracking for the primary Internet connection. The gateway's priority will be reduced by 10 if the primary connection goes down.

```
set ha track wan1 10
```

EXAMPLE 2

The following command displays the gateway's Internet connection tracking settings:

```
show ha track
```

hotspot

PURPOSE

The `hotspot` variable is used for working with Secure HotSpot settings in the following ways:

- Configuring Secure HotSpot settings
- Displaying and exporting Secure HotSpot settings, including quick guest user settings

  For information on configuring, displaying, and exporting specific quick guest user settings, see ***hotspot quick-guest*** on page 348.

You can enable your Embedded NGX appliance as a public Internet access hotspot for specific networks. When users on those networks attempt to access the Internet, they are automatically re-directed to the My HotSpot page http://my.hotspot. On this page, they must read and accept the My HotSpot terms of use, and if My HotSpot is configured to be password-protected, they must log on using their Embedded NGX username and password. The users may then access the Internet or other corporate networks.

Note: HotSpot users are automatically logged out after one hour of inactivity. If you are using RADIUS authentication, you can change the Secure HotSpot session timeout by configuring the RADIUS Session-Timeout Attribute. For information, refer to the User Guide.

For information on enabling Secure HotSpot for specific networks, see ***net dmz*** on page 368, ***net lan*** on page 387, ***net wlan*** on page 442, ***net wan*** on page 399, ***net wan2*** on page 430, and ***vlan*** on page 686.

For information on granting Secure HotSpot access to users, see ***users*** on page 680.

You can choose to exclude specific network objects from HotSpot enforcement. Excluded network objects will be able to access the network without viewing the My HotSpot page. Furthermore, users on HotSpot networks will be able to access the excluded network object without viewing the My HotSpot page. For information on excluding network objects from HotSpot enforcement, see ***netobj*** on page 465.

Important: SecureClient/SecuRemote VPN software users who are authenticated by the Internal VPN Server are automatically exempt from HotSpot enforcement. This allows, for example, authenticated employees to gain full access to the corporate LAN, while guest users are permitted to access the Internet only.

Note: Secure HotSpot enforcement can block traffic passing through the firewall; however, it does not block local traffic on the same network segment (traffic that does not pass through the firewall).

SYNTAX

When used with `set`:

set hotspot [title *title*] [terms *terms*] [auth *auth*] [redirect-url *redirect-url*] [multiplelogin *multiplelogin*] [usehttps *usehttps*] [timeout *timeout*] [use-dns *use-dns*] [enforce-mode *enforce-mode*]

When used with `show`:

show hotspot [title | terms | auth | redirect-url | multiplelogin | usehttps | timeout | use-dns | enforce-mode]

FIELDS

`title`

String. The title on the My HotSpot page.

The default title is "Welcome to My HotSpot".

`terms`

String. The terms to which the user must agree before logging on to My HotSpot.

You can use HTML tags as needed.

`auth`

String. Indicates whether users are required to enter their username and password before logging on to My HotSpot. This can have the following values:

- `none` - No authentication is required.
- `password` - Authentication is required.

The default value is `none`.

`redirect-url`

String. The URL to which users should be redirected after logging on to My HotSpot.

For example, you can redirect authenticated users to your company's Web site or a "Welcome" page.

If you do not set this field, users will not be redirected after logging on.

`multiplelogin`

String. Indicates whether to allow a single user to log on to My HotSpot from multiple computers at the same time. This can have the following values:

- `enabled` - Login from multiple computers is allowed.
- `disabled` - Login from multiple computers is not allowed.

The default value is `disabled`.

`usehttps`

String. Indicates whether users are required to log on to My HotSpot using HTTPS. This can have the following values:

- `true` - Users must log on using HTTPS. If they connect using HTTP, they are automatically re-directed to HTTPS.
- `false` - Users can log on using HTTP. HTTPS is not required.

The default value is `false`.

`timeout`

Integer. The amount of time in seconds that the connection can remain idle. Once this period of time has elapsed, the My HotSpot session is automatically terminated.

The default value is 3600 seconds.

This setting is only available through the command line.

`use-dns`

String. Indicates whether to redirect unauthenticated users to My HotSpot, by using DNS or the gateway's IP address. This can have the following values:

- `true` - Redirect users to My HotSpot using DNS. Users are redirected to http://my.hotspot.
- `false` - Redirect users to My Hotspot using the gateway's IP address. Users are redirected to http://1.2.3.4.

The default value is `true`.

Using DNS is suitable in most cases. However, if users' Web clients are configured with a DNS server that is not located behind the Embedded NGX appliance, redirection will fail. In this case, you must set this value to `false`.

This setting is only available through the command line.

`enforce-mode`

String. The networks that users should be blocked from accessing, prior to logging in to Secure HotSpot, or after failing to authenticate.

This can have the following values:

- `any` - Users cannot access internal networks, the Internet, or VPN.
- `external` - Users can access internal networks, but not the Internet or VPN.
- `vpn` - Users can access internal networks and the Internet, but not VPN.

The default value is `any`.

EXAMPLE 1

The following command defines terms of use for the My HotSpot page and requires users to log on to the page:

```
set hotspot terms "<b>Internet access is limited to 1 hour.</b>" auth
password
```

EXAMPLE 2

The following command displays all Secure HotSpot settings:

```
show hotspot
```

hotspot quick-guest

PURPOSE

The `hotspot quick-guest` variable is used for working with quick guest HotSpot user settings in the following ways:

- Configuring the default expiration period for guest HotSpot users
- Displaying and exporting this setting

For information on configuring Secure HotSpot, see ***hotspot*** on page 343. For information on adding quick guest HotSpot users, refer to the User Guide.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set hotspot quick-guest default-expiration-minutes *default-expiration-minutes*

When used with `show`:

show set hotspot quick-guest [default-expiration-minutes]

FIELDS

`default-expiration-minutes`	Integer. The default expiration period (in minutes) for guest HotSpot users. The default value is 1440 minutes (1 day).

EXAMPLE 1

The following command sets the default expiration period for guest HotSpot users to two days:

```
set hotspot quick-guest default-expiration-minutes 2880
```

EXAMPLE 2

The following command displays the guest HotSpot user settings:

```
show ha effect
```

https

PURPOSE

The `https` variable is used for working with HTTPS in the following ways:

- Enabling and configuring HTTPS access to the Embedded NGX Portal
- Displaying and exporting HTTPS settings

When HTTPS Remote Access is enabled,Embedded NGX appliance users can securely access the Embedded NGX Portal from the Internet, by accessing the URL https://X.X.X.X:981, where X.X.X.X is the Embedded NGX Internet IP address.

Note: The URL https://my.firewall is always accessible from the Internal Network, even when the HTTPS Remote Access is disabled.

SYNTAX

When used with `set`:

set https [mode *mode*] [iprange *iprange*]

When used with `show`:

show https [mode | iprange]

FIELDS

mode

String. Indicates from where HTTPS access to the Embedded NGX Portal should be granted. This can have the following values:

- `internal` - The internal network only.
  This disables remote HTTPS capability.
  Note: You can use HTTPS to access the Embedded NGX Portal from your internal network, by surfing to https://my.firewall.
- `range` - A particular range of IP addresses.
  If you choose this mode, you must include the `iprange` field.
- `any` - Any IP address.
- `vpn` - The internal network and your VPN.

The default value is `internal`.

Warning: If remote HTTPS is enabled, your Embedded NGX appliance settings can be changed remotely, so it is especially important to make sure all Embedded NGX appliance users' passwords are difficult to guess.

iprange

IP Address or String. The desired IP address range. This can have the following values:

- An IP address
- An IP address range. To specify a range, use the following format:
  `<Start IP Address>-<End IP Address>`
- `undefined` - No IP address range is defined.

The default value is `undefined`.

EXAMPLE 1

The following command enables Embedded NGX users to access the Embedded NGX Portal using HTTPS from any IP address:

```
set https mode any
```

EXAMPLE 2

The following command displays the IP address or IP address range from which HTTPS access is granted:

```
show https iprange
```

loadbalancing

PURPOSE

The `loadbalancing` variable is used for working with WAN load balancing settings in the following ways:

- Configuring WAN load balancing settings
- Displaying and exporting WAN load balancing settings

By default, the Embedded NGX appliance routes all traffic to the primary Internet connection, and the secondary Internet connection is used only when the primary connection is down, or when a routing rule specifically states that traffic should be sent through the secondary connection. WAN load balancing automatically distributes traffic between the primary and secondary connections, allowing you to use both connections in parallel and increasing the amount of available bandwidth.

For more information on WAN load balancing, refer to the User Guide.

Note: Before configuring WAN load balancing using the `loadbalancing` variable, you must configure both the primary and secondary Internet connections and assign them load balancing weights. For instructions, see ***net wan loadbalancing*** on page *421* and ***net wan2 loadbalancing*** on page *436*.

SYNTAX

When used with `set`:

set loadbalancing [mode *mode*] [stickiness *stickiness*] [threshold *threshold*]

When used with `show`:

show loadbalancing [mode | stickiness | threshold]

FIELDS

`mode`	String. Indicates whether WAN load balancing is enabled. This can have the following values: • `enabled` - WAN load balancing is enabled. • `disabled` - WAN load balancing is disabled. The default value is `disabled`.

`stickiness`	Integer. The amount of time (in seconds) that a source-destination pair can remain inactive, before it is removed from the load balancing table. When one IP address sends packets to another IP address, the Embedded NGX appliance enters the source-destination pair in a load balancing table and specifies the least-loaded Internet connection as the connection to use for traffic between this pair. The Embedded NGX appliance will route *all* traffic between this pair to the specified Internet connection, so long as the pair remains in the load balancing table. The default value is 3600 seconds. This setting is only available through the command line.
`threshold`	Integer. The minimum amount of bandwidth utilization (in kilobits per second) required to trigger load balancing. The default value is 64 kilobits per second. This setting is only available though the command line.

EXAMPLE 1

The following command enables WAN load balancing:

```
set loadbalancing mode enabled
```

EXAMPLE 2

The following command displays the WAN load balancing settings:

```
show loadbalancing
```

mailfilter

PURPOSE

The `mailfilter` variable is used for working with Email Filtering settings in the following ways:

- Configuring advanced Email Filtering settings
- Displaying and exporting advanced Email Filtering settings
- Displaying and exporting all Email Filtering settings, including:
  - Email Antivirus settings
  - Email Antispam settings
  - Email Filtering protocol settings

  For information on displaying and exporting specific Email Antivirus settings, Email Antispam settings, and protocol settings, see ***mailfilter antivirus*** on page 358, ***mailfilter antispam*** on page 356, and ***mailfilter protocols*** on page 360.

You can specify how the gateway should handle Email Filtering when the service is enabled and the Service Center is unavailable. Email Filtering includes both Email Antivirus and Email Antispam.

Note: Email Filtering is only available if you are connected to a Service Center and subscribed to this service.

SYNTAX

When used with `set`:

set mailfilter onfailure *onfailure*

When used with `show`:

show mailfilter [onfailure]

FIELDS

`onfailure`

String. Indicates how the gateway should handle Email Filtering, when the service is enabled and the Service Center is unavailable.

This can have the following values:

- `fail-closed` - Temporarily block all email traffic. This ensures constant protection from spam and viruses.
- `fail-open` - Temporarily allow all email traffic. This ensures continuous access to email; however, it does not protect against viruses and spam, so use this option cautiously.

The default value is `fail-closed`.

EXAMPLE 1

The following command configures the gateway to allow all email traffic when the Service Center is unavailable:

```
set mailfilter onfailure fail-open
```

EXAMPLE 2

The following command displays all Email Filtering settings, including Email Antivirus, Email Antispam, and protocol settings:

```
show mailfilter
```

mailfilter antispam

PURPOSE

The `mailfilter antispam` variable is used for working with the Email Antispam service in the following ways:

- Enabling/disabling the Email Antispam service
- Displaying and exporting the Email Antispam service mode

When the Email Antispam service is enabled, your email is automatically scanned for the detection of spam. If spam is detected, the email's Subject line is modified to indicate that it is suspected spam. You can create rules to divert such messages to a special folder.

Note: The Email Antispam subscription service differs from VStream Antispam in the following ways:

- Email Antispam is centralized, redirecting traffic through the Service Center for scanning, while VStream Antispam scans for spam in the Embedded NGX gateway itself.
- Email Antispam is specific scans incoming POP3 and outgoing SMTP connections only, while VStream Antispam supports both incoming and outgoing POP3 and SMTP, as well as POP3 and SMTP connections between internal networks.

You can use either antispam solution or both in conjunction. For general information on VStream Antispam, refer to the User Guide. For information on enabling VStream Antispam's engines, see ***antispam blocked-senders*** on page *239*, ***antispam content-based*** on page *245*, and ***antispam ip-reputation*** on page *253*.

Note: Email Antispam is only available if you are connected to a Service Center and subscribed to this service.

Note: If the Embedded NGX appliance is remotely managed, contact your Service Center administrator to change these settings.

For information on temporarily disabling the Email Antispam service, refer to the User Guide. For information about Email Antispam protocols, see ***mailfilter protocols*** on page 360.

SYNTAX

When used with `set`:

set mailfilter antispam mode *mode*

When used with `show`:

show mailfilter antispam [mode]

FIELDS

`mode`	String. The Email Antispam service mode. This can have the following values: • `enabled` - Enables the service for all internal network computers. • `disabled` - Disables the service for all internal network computers. The default value is `disabled`.

EXAMPLE 1

The following command enables the Email Antispam service:

```
set mailfilter antispam mode enabled
```

EXAMPLE 2

The following command displays the Email Antispam mode:

```
show mailfilter antispam
```

mailfilter antivirus

PURPOSE

The `mailfilter antivirus` variable is used for working with the Email Antivirus service in the following ways:

- Enabling/disabling the Email Antivirus service
- Displaying and exporting the Email Antivirus service mode

When the Email Antivirus service is enabled, your email is automatically scanned for the detection and elimination of all known viruses and vandals. If a virus is detected, it is removed and replaced with a warning message.

Note: The Email Antivirus subscription service differs from VStream Antivirus in the following ways:

- Email Antivirus is centralized, redirecting traffic through the Service Center for scanning, while VStream Antivirus scans for viruses in the Embedded NGX gateway itself.
- Email Antivirus is specific to email, scanning incoming POP3 and outgoing SMTP connections only, while VStream Antivirus supports additional protocols, including incoming SMTP and outgoing POP3 connections.

You can use either antivirus solution or both in conjunction. For information on VStream Antivirus, see ***vstream*** on page *764*.

Note: Email Antivirus is only available if you are connected to a Service Center and subscribed to this service.

Note: If the Embedded NGX appliance is remotely managed, contact your Service Center administrator to change these settings.

For information on temporarily disabling the Email Antivirus service, refer to the User Guide. For information about Email Antivirus protocols, see ***mailfilter protocols*** on page 360.

SYNTAX

When used with `set`:

set mailfilter antivirus mode *mode*

When used with `show`:

show mailfilter antivirus [mode]

FIELDS

`mode`	String. The Email Antivirus service mode. This can have the following values: • `enabled` - Enables the service for all internal network computers. • `disabled` - Disables the service for all internal network computers. The default value is `disabled`.

EXAMPLE 1

The following command enables the Email Antivirus service:

```
set mailfilter antivirus mode enabled
```

EXAMPLE 2

The following command displays the Email Antivirus mode:

```
show mailfilter antivirus
```

mailfilter protocols

PURPOSE

The `mailfilter protocols` variable is used for working with Email Filtering protocol settings in the following ways:

- Defining which protocols should be scanned for viruses and spam
- Displaying and exporting Email Filtering protocol settings

You can configure the Embedded NGX appliance to scan mail in POP3 and SMTP protocols.

Note: Email Filtering is only available if you are connected to a Service Center and subscribed to this service.

Note: If the Embedded NGX appliance is remotely managed, contact your Service Center administrator to change these settings.

SYNTAX

When used with `set`:

set mailfilter protocols [**pop3** *pop3*] [**smtp** *smtp*]

When used with `show`:

show mailfilter protocols [**pop3** | **smtp**]

FIELDS

`pop3`	String. Indicates whether incoming email in the POP3 protocol should be scanned. This can have the following values: • `enabled` - Scan all incoming email in the POP3 protocol. • `disabled` - Do not scan incoming email in the POP3 protocol. The default value is `enabled`.
`smtp`	String. Indicates whether outgoing email should be scanned. This can have the following values: • `enabled` - Scan all outgoing email. • `disabled` - Do not scan outgoing email. The default value is `enabled`.

EXAMPLE 1

If Email Filtering is enabled, you can use the following command to enable the service for outgoing email:

```
set mailfilter protocols smtp enabled
```

For information on enabling the Email Filtering service, see antivirus.

EXAMPLE 2

The following command displays all Email Filtering protocol settings:

```
show mailfilter protocols
```

nat rules

PURPOSE

The `nat rules` variable is used for working with custom NAT rules in the following ways:

- Adding custom NAT rules
- Modifying custom NAT rules
- Deleting custom NAT rules
- Displaying and exporting custom NAT rules
- Clearing the Custom NAT Rules table

A NAT rule is a setting used to change the source, destination, and/or service of specific connections. The Embedded NGX appliance enables you to explicitly define the following types of custom NAT rules:

- Static NAT (or One-to-One NAT). Translation of an IP address range to another IP address range of the same size.
- Hide NAT (or Many-to-One NAT). Translation of an IP address range to a single IP address.
- Few-to-Many NAT. Translation of a smaller IP address range to a larger IP address range.
- Many-to-Few NAT. Translation of a larger IP address range to a smaller IP address range.
- Service-Based NAT. Translation of a connection's original service to a different service.

For more information on NAT rules, refer to ***info nat*** on page 147 and the User Guide.

Note: The Embedded NGX appliance automatically creates NAT rules upon the following events:

- Hide NAT is enabled on an internal network
- An Allow and Forward firewall rule is defined
- Static NAT is configured for a network object
- NAT rules are received from the Service Center

Such rules are called *implicitly defined NAT rules*, and you cannot delete or modify them, nor can you display them using the `show nat rules` command. However, you can display both custom NAT rules and implicitly defined NAT rules using the `info nat` command. See ***info nat*** on page *147*.

SYNTAX

When used with `add`:

add nat rules [orig-src *orig-src*] [orig-dst *orig-dst*] [orig-svc *orig-svc*] [nat-src *nat-src*] [nat-dst *nat-dst*] [nat-svc *nat-svc*] [name *name*]

When used with `set`:

set nat rules *number* [orig-src *orig-src*] [orig-dst *orig-dst*] [orig-svc *orig-svc*] [nat-src *nat-src*] [nat-dst *nat-dst*] [nat-svc *nat-svc*] [name *name*]

When used with `delete`:

delete nat rules *number*

When used with `show`:

show nat rules [*number*] [orig-src | orig-dst | orig-svc | nat-src | nat-dst | nat-svc | name]

When used with `clear`:

clear nat rules

FIELDS

number

Integer. The rule's row in the Custom NAT Rules table.

orig-src

IP Address or String. The original source of the connections you want to translate. This can have the following values:

- An IP address
- An IP address range - To specify a range, use the following format:
  `<Start IP Address>-<End IP Address>`
- `any` - The rule should apply to any source.
- `wan`
- `lan`
- `dmz`
- `vpn`
- `notvpn` - Not VPN
- The name of a VPN site
- The name of a network object
- The name of a bridge
- The name of a VLAN
- The name of a VAP
- The name of a WDS link

The default value is `any`.

orig-dst

IP Address or String. The original destination of the connections you want to translate. This can have the following values:

- An IP address
- An IP address range - To specify a range, use the following format:
  `<Start IP Address>-<End IP Address>`
- `any` - The rule should apply to any destination.
- `wan`

- `lan`
- `dmz`
- `vpn`
- `notvpn` - Not VPN
- The name of a VPN site
- The name of a network object
- The name of a bridge
- The name of a VLAN
- The name of a VAP
- The name of a WDS link

The default value is `any`.

`orig-svc`

String. The original service used for the connections you want to translate. This can have the following values:

This can have the following values:

- The name of a network service object
- `any` - The rule should apply to any service.

The default value is `any`.

`nat-src`

IP Address or String. The translated source of the connections. This can have the following values:

- An IP address
- An IP address range - To specify a range, use the following format: `<Start IP Address>-<End IP Address>`
- `original` - The original source should not be translated.
- The name of a network object

The default value is `original`.

`nat-dst`	IP Address or String. The translated destination of the connections. This can have the following values: • An IP address • An IP address range - To specify a range, use the following format: `<Start IP Address>-<End IP Address>` • `original` - The original destination should not be translated. • The name of a network object The default value is `original`.
`nat-svc`	String. The new service to which the original service should be translated. This can have the following values: • The name of a network service object • `original` - The original service should not be translated. The default value is `original`.
`name`	String. The NAT rule's name. You may choose any name.

Example 1

The following command adds a custom NAT rule that translates all connections from 212.2.2.1 to any destination, so that they appear to originate from 213.2.2.1:

```
add nat rules orig-src 212.2.2.1 orig-dst any nat-src 213.2.2.1 nat-dst original
```

EXAMPLE 2

The following command changes the name of custom NAT rule 2 to "hideLAN":

```
set nat rules 2 name hideLAN
```

EXAMPLE 3

The following command deletes custom NAT rule 2:

```
delete nat rules 2
```

EXAMPLE 4

The following command displays the settings for all custom NAT rules:

```
show nat rules
```

EXAMPLE 5

The following command clears all NAT rules in the Custom NAT Rules table:

```
clear nat rules
```

net dmz

PURPOSE

The `net dmz` variable is used for working with Demilitarized Zone (DMZ) network settings in the following ways:

- Configuring your Embedded NGX appliance's DMZ network settings, including:
  - Hide Network Address Translation (NAT)
  - The DMZ network's default gateway
  - The DMZ network's internal network range
  - DHCP (Dynamic Host Configuration Protocol) settings
  - Secure HotSpot access
  - The DMZ network's bridge assignment and settings
- Displaying and exporting the above DMZ network settings
- Displaying and exporting all DMZ network settings, including High Availability, OSPF, and RIP settings.

  For information on configuring, displaying, and exporting specific DMZ High Availability settings, see ***net dmz ha*** on page 376. For information on configuring, displaying, and exporting specific DMZ OSPF settings, see ***net dmz ospf*** on page 378 and ***net dmz ospf md5*** on page 381. For information on configuring, displaying, and exporting specific DMZ RIP settings, see ***net dmz rip*** on page 383 and ***net dmz rip authentication*** on page 385.

In addition to the LAN network, you can define a second internal network called a DMZ (demilitarized zone) network. By default, all traffic is allowed from the LAN network to the DMZ network, and no traffic is allowed from the DMZ network to the LAN network. You can easily customize this behavior by creating firewall user rules. For information on defining rules, see ***fw rules*** on page 322. For information on the default security policy for DMZs, refer to the User Guide.

Note: Some appliance models have a dedicated DMZ port to which you must connect all DMZ computers. In these models, you must assign the DMZ/WAN2 port to the DMZ. For information, see port.

In appliance models that do not have a dedicated DMZ port, the DMZ is a logical second network behind the Embedded NGX appliance, and you must connect DMZ computers to LAN ports.

Note: The DHCP server only serves computers that are configured to obtain an IP address automatically. If a computer is not configured to obtain an IP address automatically, it is recommended to assign it an IP address outside of the DHCP address range. If you do assign it an IP address within the DHCP address range, the DHCP server will not assign this IP address to another computer.

SYNTAX

When used with `set`:

set net dmz [mode *mode*] [hidenat *hidenat*] [address *address*] [netmask *netmask*] [dhcpserver *dhcpserver*] [dhcprange *dhcprange*] [dhcprelayip1 *dhcprelayip1*] [dhcprelayip2 *dhcprelayip2*] [hotspot *hotspot*] [bridge-to *bridge-to*] [bridge-range *bridge-range*] [bridge-stp-priority *bridge-stp-priority*] [bridge-stp-cost *bridge-stp-cost*] [bridge-antispoofing *bridge-antispoofing*]

show net dmz [mode | hidenat | address | netmask | dhcpserver | dhcprange | dhcprelayip1 | dhcprelayip2 | hotspot | bridge-to | bridge-range | bridge-stp-priority | bridge-stp-cost | bridge-antispoofing]

FIELDS

`mode`

String. The DMZ network mode. This can have the following values:

- `enabled` - The DMZ network is enabled.
- `disabled` - The DMZ network is disabled.
- `bridged` - The DMZ network is assigned to a bridge.

The default value is `disabled`.

`hidenat`

String. Indicates whether to use Hide NAT.

Hide NAT enables you to share a single public Internet IP address among several computers, by “hiding” the private IP addresses of the internal DMZ computers behind the DMZ network's single Internet IP address.

This field can have the following values:

- `enabled` - Hide NAT is enabled.
- `disabled` - Hide NAT is disabled.

The default value is `enabled`.

Note: If Hide NAT is disabled, you must obtain a range of Internet IP addresses from your ISP. Hide NAT is enabled by default.

Note: Static NAT and Hide NAT can be used together.

`address`

IP Address. The IP address of the DMZ network's default gateway.

Note: The DMZ network must not overlap the LAN network.

`netmask`

IP Address. The DMZ’s internal network range.

`dhcpserver`

String. Indicates whether the Embedded NGX DHCP server is enabled. This can have the following values:

- `enabled` - The Embedded NGX DHCP server is enabled.
- `disabled` - The Embedded NGX DHCP server is disabled.
- `relay` - DHCP relay is enabled.

The default value is `enabled`.

By default, the Embedded NGX appliance operates as a DHCP server. This allows the Embedded NGX appliance to automatically configure all the devices on the DMZ network

with their network configuration details.

If you already have a DHCP server in the DMZ's internal network, and you want to use it instead of the Embedded NGX DHCP server, you must disable the Embedded NGX DHCP server, since you cannot have two DHCP servers or relays on the same network segment.

If you want to use a DHCP server on the Internet or via a VPN, instead of the Embedded NGX DHCP server, you can configure DHCP relay. When in DHCP relay mode, the Embedded NGX appliance relays information from the desired DHCP server to the devices on the DMZ network.

`dhcprange`

String. Indicates how the DHCP server should obtain the DHCP address range.

The DHCP address range is the range of IP addresses that the DHCP server can assign to network devices. IP addresses outside of the DHCP address range are reserved for statically addressed computers.

This field can have the following values:

- `automatic` - The Embedded NGX DHCP server automatically sets the DHCP address range.
- A DHCP address range - Relevant only if the Embedded NGX DHCP server is enabled.
  To specify a range, use the following format:
  `<Start IP Address>-<End IP Address>`

The default value is `automatic`.

`dhcprelayip1`

IP Address or String. The IP address of the primary DHCP relay server. This can have the following values:

- An IP address
- `undefined` - No primary DHCP relay server is defined.

The default value is `undefined`.

This field is only relevant if DHCP relay is enabled.

`dhcprelayip2`

IP Address or String. The IP address of the secondary DHCP relay server. This can have the following values:

- An IP address
- `undefined` - No secondary DHCP relay server is defined.

The default value is `undefined`.

This field is only relevant if DHCP relay is enabled.

`hotspot`

String. Indicates whether to enable Secure HotSpot for the DMZ network. This can have the following values:

- `enabled` - Secure HotSpot is enabled for the DMZ.
- `disabled` - Secure HotSpot is disabled for the DMZ.

The default value is `disabled`.

`bridge-to`

String. The bridge to which the DMZ is assigned. This can have the following values:

- `none` - The DMZ is not assigned to a bridge.
- The name of a bridge

The default value is `none`.

`bridge-range`

String. The range of IP addresses that should be allowed on the DMZ network. This can have the following values:

- `undefined` - The no range is defined.
- The name of a bridge

The default value is `undefined`.

Note: When assigning IP addresses to machines in a bridged network segment, the Embedded NGX DHCP server allocates only addresses within the allowed IP address range.

To enable clients to move between bridged networks without changing IP addresses, configure identical IP address ranges for the desired networks, thus allowing the IP addresses to be used on either of the bridged networks.

Note: Configuring overlapping or identical allowed IP address ranges will decrease the effectiveness of anti-spoofing between the bridged networks.

`bridge-stp-priority`	Integer. The port priority of the DMZ network. This field is only relevant if STP is enabled for the bridge. The port's priority is combined with the port's logical number to create the port's ID. The port with the lowest ID is elected as the root port, which forwards frames out of the bridge. The other ports in the bridge calculate the least-cost path to the root port, in order to eliminate loops in the topology and provide fault tolerance. To increase the chance of this port being elected as the root port, select a lower priority. Note: If you select the same priority for all ports, the root port will be elected based on the port's logical number. This must be an integer between 0 and 240, in increments of 16. The default value is 128.
`bridge-stp-cost`	Integer. The port cost of the DMZ network. This field is only relevant if STP is enabled for the bridge. STP uses the available port with the lowest cost to forward frames to the root port. All other ports are blocked. It is recommended to set a lower value for faster links. The default value is 100.

`bridge-antispoofing`

String. Indicates whether anti-spoofing is enabled on the bridged DMZ network. This can have the following values:

- `enabled` - Anti-spoofing is enabled for the DMZ. Only IP addresses within the allowed IP range (specified in the `bridge-range` field) can be source IP addresses for packets on this network
- `disabled` - Anti-spoofing is disabled for the DMZ.

The default value is `enabled`.

EXAMPLE 1

The following command enables Hide NAT for the DMZ network:

```
set net dmz hidenat enabled
```

EXAMPLE 2

The following command assigns the DMZ network to the "Bridge1" bridge.

```
set net dmz mode bridged bridge-to Bridge1
```

EXAMPLE 3

The following command displays the DMZ network's DHCP range:

```
show net dmz dhcprange
```

net dmz ha

PURPOSE

The `net dmz ha` variable is used for working with DMZ High Availability settings in the following ways:

- Configuring DMZ High Availability settings
- Displaying and exporting DMZ High Availability settings

You can create a High Availability cluster consisting of two or more Embedded NGX appliances. For more information on High Availability, see ***ha*** on page 335.

SYNTAX

When used with `set`:

set net dmz ha virtualip *virtualip*

When used with `show`:

show net dmz ha [**virtualip**]

FIELDS

`virtualip`	IP Address or String. The default gateway IP address. This can have the following values: • An IP address - This can be any unused IP address in the DMZ network, and must be the same for both gateways. • `undefined` - High Availability is not configured for this network. The default value is `undefined`.

EXAMPLE 1

The following command sets the DMZ network's virtual IP address:

```
set net dmz ha virtualip 192.168.10.14
```

EXAMPLE 2

The following command displays the appliance's DMZ High Availability settings:

```
show net dmz ha
```

net dmz ospf

PURPOSE

The `net dmz ospf` variable is used for working with OSPF settings for the DMZ in the following ways:

- Configuring the OSPF settings for the DMZ
- Displaying and exporting OSPF settings for the DMZ, including authentication settings

  For information on configuring, displaying, and exporting specific authentication settings, see ***net dmz ospf authentication*** on page 381.

These settings are only relevant if OSPF is enabled. For information, see ***ospf*** on page 470.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set net dmz ospf [cost *cost*] [passive-interface *passive-interface*] [hello-interval *hello-interval*] [dead-interval *dead-interval*] [retransmit-interval *retransmit-interval*] [transmit-delay *transmit-delay*]

When used with `show`:

show net dmz ospf [cost | passive-interface | hello-interval | dead-interval | retransmit-interval | transmit-delay]

FIELDS

`cost`	Integer. The cost of this sending a packet on this interface. Routers send a packet to the route that matches the packet's destination and has the lowest cost. The default value is 0.

`passive-interface`	String. Indicates whether to define this interface as a passive interface. A passive interface is included in the AS topology, but it does not generate or accept OSPF traffic. This can have the following values: • `enabled` - Define this interface as a passive interface. • `disabled` - Do not define this interface as a passive interface. The default value is `disabled`.
`hello-interval`	Integer. The interval of time (in seconds) between transmissions of hello packets on this interface. The default value is 10 seconds.
`dead-interval`	Integer. The interval of time (in seconds) after which the OSPF neighbor will be considered "dead", if it does not send hello packets. The default value is 40 seconds.
`retransmit-interval`	Integer. The interval of time (in seconds) after which the gateway will send an LSA to a neighbor, if the neighbor does not respond to the previous transmission. The default value is 5 seconds.
`transmit-delay`	Integer. The amount of time (in seconds) required to transmit an LSA packet. This value is added to the LSA packet's age before transmission. When specifying this value, take into account the interface's transmission and propagation delays. Slower Internet connections will require a higher value. The default value is 1 second.

EXAMPLE 1

The following command sets the DMZ's OSPF cost:

```
set net dmz ospf cost 10
```

EXAMPLE 2

The following command displays the DMZ's OSPF settings:

```
show net dmz ospf
```

net dmz ospf authentication

PURPOSE

The `net dmz ospf authentication` variable is used for working with OSPF authentication settings for the DMZ in the following ways:

- Configuring OSPF authentication settings for the DMZ
- Displaying and exporting OSPF authentication settings for the DMZ

These settings are only relevant if OSPF is enabled. For information, see ***ospf*** on page 470.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set net dmz ospf authentication [simple-text-password *simple-text-password*] [md5-key *md5-key*] [md5-password *md5-password*] [mode *mode*]

When used with `show`:

show net dmz ospf authentication [simple-text-password | md5-key | md5-password | mode]

FIELDS

`simple-text-password`	String. The password to use for clear-text authentication. Passwords need not be the identical throughout an OSPF area, but they must be the same for OSPF neighbors.
`md5-key`	Integer. The key ID to use for MD5 authentication.
`md5-password`	String. The password to use for MD5 authentication. Passwords need not be the identical throughout an OSPF area, but they must be the same for OSPF neighbors.

`mode`	String. The authentication scheme to use for OSPF connections. This can have the following values: • `none` - Do not use authentication. • `md5` - Use the MD5 authentication scheme. • `simple-text` - Use the clear-text authentication scheme. The default value is `none`.

EXAMPLE 1

The following command enables MD5 authentication for OSPF connections:

```
set net dmz ospf authentication md5-key 1 md5-password thepassword mode
md5
```

EXAMPLE 2

The following command displays the DMZ's OSPF MD5 authentication settings:

```
show net dmz ospf authentication
```

net dmz rip

PURPOSE

The `net dmz rip` variable is used for working with RIP settings for the DMZ in the following ways:

- Configuring the RIP settings for the DMZ
- Displaying and exporting RIP settings for the DMZ, including authentication settings

  For information on configuring, displaying, and exporting specific authentication settings, see ***net dmz rip authentication*** on page 385.

These settings are only relevant if RIP is enabled. For information, see ***rip*** on page 541.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set net dmz rip passive-interface *passive-interface*

When used with `show`:

show net dmz rip [passive-interface]

FIELDS

`passive-interface`	String. Indicates whether to define the DMZ as a passive interface. A passive interface does not generate or accept RIP traffic. This can have the following values: • `enabled` - Define this interface as a passive interface. • `disabled` - Do not define this interface as a passive interface. The default value is `disabled`.

EXAMPLE 1

The following command configures the DMZ as a passive interface for RIP traffic:

```
set net dmz rip passive-interface enabled
```

EXAMPLE 2

The following command displays the DMZ's RIP settings:

```
show net dmz rip
```

net dmz rip authentication

PURPOSE

The `net dmz rip authentication` variable is used for working with RIP authentication settings for the DMZ in the following ways:

- Configuring RIP authentication settings for the DMZ
- Displaying and exporting RIP authentication settings for the DMZ

These settings are only relevant if RIP is enabled. For information, see ***rip*** on page 541.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set net dmz rip authentication [simple-text-password *simple-text-password*] [md5-key *md5-key*] [md5-password *md5-password*] [mode *mode*]

When used with `show`:

show net dmz rip authentication [simple-text-password | md5-key | md5-password | mode]

FIELDS

`simple-text-password`	String. The password to use for clear-text authentication.
`md5-key`	Integer. The key ID to use for MD5 authentication.
`md5-password`	String. The password to use for MD5 authentication.
`mode`	String. The authentication scheme to use for RIP connections. This can have the following values: • `none` - Do not use authentication. • `md5` - Use the MD5 authentication scheme. • `simple-text` - Use the clear-text authentication scheme. The default value is `none`.

EXAMPLE 1

The following command enables MD5 authentication for RIP connections:

```
set net dmz rip authentication md5-key 1 md5-password thepassword mode
md5
```

EXAMPLE 2

The following command displays the DMZ's RIP MD5 authentication settings:

```
show net dmz rip authentication
```

net lan

PURPOSE

The `net lan` variable is used for working with your Local Area Network (LAN) settings in the following ways:

- Configuring your Embedded NGX appliance's LAN settings, including:
  - Hide Network Address Translation (NAT)
  - Your Embedded NGX appliance's internal IP address
  - The range of IP addresses in your internal network
  - DHCP settings
  - Secure HotSpot access
  - The LAN network's bridge assignment and settings
- Displaying and exporting the above LAN settings
- Displaying and exporting all LAN settings, including High Availability, OSPF, and RIP settings.

  For information on configuring, displaying, and exporting specific LAN High Availability settings, see ***net lan ha*** on page 390. For information on configuring, displaying, and exporting specific LAN OSPF settings, see ***net lan ospf*** on page 391 and ***net lan ospf md5*** on page 392. For information on configuring, displaying, and exporting specific LAN RIP settings, see ***net lan rip*** on page 393 and ***net lan rip authentication*** on page 394.

Note: The DHCP server only serves computers that are configured to obtain an IP address automatically. If a computer is not configured to obtain an IP address automatically, it is recommended to assign it an IP address outside of the DHCP address range. If you do assign it an IP address within the DHCP address range, the DHCP server will not assign this IP address to another computer.

Note: After changing LAN settings, you must do the following:

- If your computer is configured to obtain its IP address automatically (using DHCP), and either the Embedded NGX DHCP server or another DHCP server is enabled, restart your computer. Your computer obtains an IP address in the new range.
- Otherwise, manually reconfigure your computer to use the new address range using the TCP/IP settings. For information on configuring TCP/IP, refer to the User Guide.

SYNTAX

When used with `set`:

set net lan [mode *mode*] [hidenat *hidenat*] [address *address*] [netmask *netmask*] [dhcpserver *dhcpserver*] [dhcprange *dhcprange*] [dhcprelayip1 *dhcprelayip1*] [dhcprelayip2 *dhcprelayip2*] [hotspot *hotspot*] [bridge-to *bridge-to*] [bridge-range *bridge-range*] [bridge-stp-priority *bridge-stp-priority*] [bridge-stp-cost *bridge-stp-cost*] [bridge-antispoofing *bridge-antispoofing*]

When used with `show`:

show net lan [mode | hidenat | address | netmask | dhcpserver | dhcprange | dhcprelayip1 | dhcprelayip2 | hotspot | bridge-to | bridge-range | bridge-stp-priority | bridge-stp-cost | bridge-antispoofing]

FIELDS

`address`	IP Address. The Embedded NGX appliance's internal IP address.
`netmask`	IP Address. The subnet mask that applies to the appliance's internal IP address. Note: The internal network range is defined both by the Embedded NGX appliance's internal IP address and by the subnet mask. For example, if the Embedded NGX appliance's internal IP address is 192.168.100.7, and you set the subnet mask to 255.255.255.0, the network's IP address range will be 192.168.100.1 – 192.168.100.254. The default internal network range is 192.168.10.*.

For all other fields, see ***net dmz*** on page 368.

EXAMPLE 1

The following command enables Hide NAT for the LAN:

```
set net lan hidenat enabled
```

EXAMPLE 2

The following command assigns the LAN network to the "Bridge1" bridge.

```
set net lan mode bridged bridge-to Bridge1
```

EXAMPLE 3

The following command displays the LAN DHCP range:

```
show net lan dhcprange
```

net lan ha

See ***net dmz ha*** on page 376.

net lan ospf

See ***net dmz ospf*** on page 378.

net lan ospf authentication

See ***net dmz ospf authentication*** on page 381.

net lan rip

See ***net dmz rip*** on page 383.

net lan rip authentication

See ***net dmz rip authentication*** on page 385.

net officemode

PURPOSE

The `net officemode` variable is used for working with OfficeMode network settings in the following ways:

- Configuring your Embedded NGX appliance's OfficeMode network settings, including:
  - Hide Network Address Translation (NAT)
  - The OfficeMode network's default gateway
  - The OfficeMode network's internal network range
  - DHCP (Dynamic Host Configuration Protocol) settings
- Displaying and exporting the above OfficeMode network settings

By default, VPN Clients connect to the VPN Server using an Internet IP address locally assigned by an ISP. This may lead to the following problems:

- VPN Clients on the same network will be unable to communicate with each other via the Embedded NGX Internal VPN Server. This is because their IP addresses are on the same subnet, and they therefore attempt to communicate directly over the local network, instead of through the secure VPN link.
- Some networking protocols or resources may require the client's IP address to be an internal one.

OfficeMode solves these problems by enabling the Embedded NGX DHCP Server to automatically assign a unique local IP address to the VPN client, when the client connects and authenticates. The IP addresses are allocated from a pool called the *OfficeMode network*.

Note: OfficeMode requires Check Point SecureClient to be installed on the VPN clients. It is not supported by Check Point SecuRemote.

When OfficeMode is not supported by the VPN client, traditional mode will be used instead.

Note: The DHCP server only serves computers that are configured to obtain an IP address automatically. If a computer is not configured to obtain an IP address automatically, it is recommended to assign it an IP address outside of the DHCP address range. If you do assign it an IP address within the DHCP address range, the DHCP server will not assign this IP address to another computer.

SYNTAX

When used with `set`:

set net officemode [mode *mode*] [hidenat *hidenat*] [address *address*] [netmask *netmask*] [dhcpserver *dhcpserver*] [dhcprange *dhcprange*]

When used with `show`:

show net officemode [mode | hidenat | address | netmask | dhcpserver | dhcprange]

FIELDS

`mode`

String. The OfficeMode network mode. This can have the following values:

- `enabled` - The OfficeMode network is enabled.
- `disabled` - The OfficeMode network is disabled.

The default value is `disabled`.

`hidenat`

String. Indicates whether to use Hide NAT.

Hide NAT enables you to share a single public Internet IP address among several computers, by “hiding” the private IP addresses of the internal OfficeMode computers behind the OfficeMode network's single Internet IP address.

This field can have the following values:

- `enabled` - Hide NAT is enabled.
- `disabled` - Hide NAT is disabled.

The default value is `enabled`.

Note: If Hide NAT is disabled, you must obtain a range of

Internet IP addresses from your ISP. Hide NAT is enabled by default.

Note: Static NAT and Hide NAT can be used together.

`address` — IP Address. The IP address of the OfficeMode network's default gateway.

Note: The OfficeMode network must not overlap the LAN network.

`netmask` — IP Address. The OfficeMode's internal network range.

`dhcpserver` — String. Indicates whether the Embedded NGX DHCP server is enabled. This can have the following values:

- `enabled` - The Embedded NGX DHCP server is enabled.
- `disabled` - The Embedded NGX DHCP server is disabled.
- `relay` - DHCP relay is enabled.

The default value is `enabled`.

By default, the Embedded NGX appliance operates as a DHCP server. This allows the Embedded NGX appliance to automatically configure all the devices on the OfficeMode network with their network configuration details.

If you already have a DHCP server in the OfficeMode's internal network, and you want to use it instead of the Embedded NGX DHCP server, you must disable the Embedded NGX DHCP server, since you cannot have two DHCP servers or relays on the same network segment.

If you want to use a DHCP server on the Internet or via a VPN, instead of the Embedded NGX DHCP server, you can configure DHCP relay. When in DHCP relay mode, the Embedded NGX appliance relays information from the desired

DHCP server to the devices on the OfficeMode network.

`dhcprange`

String. Indicates how the DHCP server should obtain the DHCP address range.

The DHCP address range is the range of IP addresses that the DHCP server can assign to network devices. IP addresses outside of the DHCP address range are reserved for statically addressed computers.

This field can have the following values:

- `automatic` - The Embedded NGX DHCP server automatically sets the DHCP address range.
- A DHCP address range - Relevant only if the Embedded NGX DHCP server is enabled.
  To specify a range, use the following format:
  `<Start IP Address>-<End IP Address>`

The default value is `automatic`.

EXAMPLE 1

The following command enables Hide NAT for the OfficeMode network:

```
set net officemode hidenat enabled
```

EXAMPLE 2

The following command displays the OfficeMode network's DHCP range:

```
show net officemode dhcprange
```

net wan

PURPOSE

The `net wan` variable is used for doing the following:

- Configuring your Embedded NGX appliance's primary Internet connection
- Displaying and exporting the primary Internet connection's settings, including:
  - ATM settings
  - Connection delay settings
  - High Availability settings
  - WAN load balancing settings
  - OSPF settings
  - RIP settings
  - Connection probing settings

  For information on configuring, displaying, and exporting specific WAN ATM settings, see ***net wan atm*** on page 416. For information on configuring, displaying, and exporting specific connection delay settings, see ***net wan demand-connect*** on page 418. For information on configuring, displaying, and exporting specific WAN High Availability settings, see ***net wan ha*** on page 420. For information on configuring, displaying, and exporting specific WAN load balancing settings, see ***net wan loadbalancing*** on page 421. For information on configuring, displaying, and exporting specific WAN OSPF settings, see ***net wan ospf*** on page 423 and ***net wan ospf authentication*** on page 424. For information on configuring, displaying, and exporting specific WAN RIP settings, see ***net wan rip*** on page 428 and ***net wan rip authentication*** on page 429. For information on configuring, displaying, and exporting specific connection probing settings, see ***net wan probe*** on page 425.

For information on configuring a secondary connection, see ***net wan2*** on page 430.

SYNTAX

When used with `set`:

set net wan mode *mode* [gateway *gateway*] [address *address*] [netmask *netmask*] [password *password*] [username *username*] [pptpserver *pptpserver*] [pptpclientip *pptpclientip*] [pptpclientmask *pptpclientmask*] [pptpservice *pptpservice*] [pptpgateway *pptpgateway*] [accelerate-pptp *accelerate-pptp*] [ppoeservice *ppoeservice*] [mtu *mtu*] [externalip *externalip*] [phonenumber *phonenumber*] [clonedmac *clonedmac*] [usedhcp *usedhcp*] [staticwins *staticwins*] [avoidgateway *avoidgateway*] [connectonlyactive *connectonlyactive*] [staticdns *staticdns*] [disabled *disabled*] [dns1 *dns1*] [dns2 *dns2*] [wins *wins*] [uprate *uprate*] [downrate *downrate*] [connectondemand *connectondemmand*] [idletimeout *idletimeout*] [port *port*] [bypassvpn *bypassvpn*] [bridge-to *bridge-to*] [bridge-stp-priority *bridge-stp-priority*] [bridge-stp-cost *bridge-stp-cost*] [vlan-tag *vlan-tag*] [hotspot *hotspot*]

When used with `show`:

show net wan [mode | gateway | address | netmask | password | username | pptpserver | pptpclientip | pptpclientmask | pptpservice | pppoeservice | pptpgateway | accelerate-pptp | mtu | phonenumber | externalip | clonedmac | usedhcp | staticwins | avoidgateway | connectonlyactive | staticdns | disabled | dns1 | dns2 | wins | uprate | downrate | connectondemand | idletimeout | port | bypassvpn | bridge-to | bridge-stp-priority | bridge-stp-cost | vlan-tag | hotspot]

FIELDS

`mode`

String. The Internet connection type. This can have the following values:

- `lan` - LAN. Relevant when configuring an Ethernet-based connection.
- `cable` - Cable modem. Relevant when configuring an Ethernet-based connection.
- `pppoe` - PPoE. Relevant when configuring an Ethernet-based connection or a direct ADSL connection.
- `pptp` - PPTP. Relevant when configuring an Ethernet-based connection.
- `bpa` - Telstra. Relevant when configuring an Ethernet-based connection.
- `l2tp` - L2TP. Relevant when configuring an Ethernet-based connection.
- `none` - No connection.
- `dialup` - Dialup. Relevant when configuring a dialup connection on the Serial port (using a connected RS232 modem) or on a USB port (using a connected USB modem).
- `pppoa` - PPPoA. Relevant when configuring a direct ADSL connection.
- `eoa` - EoA. Relevant when configuring a direct ADSL connection.
- `ipoa` - IPoA. Relevant when configuring a direct ADSL connection.
- `bridged` - Bridged. Relevant when assigning an Ethernet-based connection or a direct ADSL connection to an existing bridge. For information on adding bridges, see ***bridges*** on page 284.

The specified Internet connection method must be appropriate to the port selected in the `port` field.

`gateway`

IP Address. The IP address of your ISP's default gateway. This can have the following values:

- An IP address
- `undefined` - The default gateway is not defined.

The default value is `undefined`.

This field is only relevant for LAN connections with a static IP address.

`address`

IP Address. The static IP address of your Embedded NGX appliance. This can have the following values:

- An IP address
- `undefined` - The static IP address is not defined.

The default value is `undefined`.

This field is only relevant for LAN connections with a static IP address.

`netmask`

IP Address. The subnet mask that applies to the static IP address of your Embedded NGX appliance. This can have the following values:

- An IP address
- `undefined` - The subnet mask is not defined.

The default value is `undefined`.

This field is only relevant for LAN connections with a static IP address.

`password`

String. Your password.

`username`

String. Your user name.

`pptpserver`	IP Address. If you selected PPTP, this is the IP address of the PPTP server as given by your ISP. If you selected Telstra (BPA), this is the IP address of the Telstra authentication server as given by Telstra.
`pptpclientip`	IP Address. The static IP address of your Embedded NGX appliance. This can have the following values: • An IP address • `undefined` - The static IP address is not defined. The default value is `undefined`. This field is only relevant for the PPTP connection type.
`pptpclientmask`	IP Address. The subnet mask that applies to the static IP address of your Embedded NGX appliance. This can have the following values: • An IP address • `undefined` - The subnet mask is not defined. The default value is `undefined`. This field is only relevant for the PPTP connection type.
`pptpservice`	String. Your PPTP service name. If your ISP has not provided you with a service name, leave this field empty. This field is only relevant when using PPTP or PPPoE connection type.
`pptpgateway`	IP Address. The IP address of the PPTP default gateway.

`accelerate-pptp`

String. Indicates whether to increase the PPTP bandwidth to 9 Mbps.

This can have the following values:

- `enabled` - Increase PPTP bandwidth.
- `disabled` - Do not increase PPTP bandwidth.

The default value is `disabled`.

This field is only relevant for the PPTP connection type.

Important: If your ISP transmits data in compressed format, enabling this setting will be detrimental to your Internet connection performace. It is therefore recommended to consult with your ISP before enabling this setting.

`pppoeservice`

String. Your PPPoE service name.

If your ISP has not provided you with a service name, leave this field empty.

This field is only relevant for the PPTP or PPPoE connection type.

`mtu`

Integer or String. The maximum transmission unit size. This can have the following values:

- A unit size
- `automatic` - The MTU is set automatically.

The default value is `automatic`.

As a general recommendation you should leave this field set to `automatic`. If however you wish to modify the default MTU, it is recommended that you consult with your ISP first and use MTU values between 1300 and 1500.

`pppauthmethod`

String. The authentication method to use for PPP connections. This can have the following values:

- `auto` - If possible, use CHAP; otherwise, use PAP.
- `pap`
- `chap`

The default value is `auto`.

This field is only relevant for the PPP-based connections.

`phonenumber`

Integer. The phone number that the modem should dial, as given by your ISP.

This field is only relevant for the Dialup connection type.

`externalip`

IP Address. The external IP address. This can have the following values:

- The IP address of the PPTP or PPPoE client as given by your ISP.
- `undefined` - The external IP is not defined.

The default value is `undefined`.

If you selected PPPoE, this field is optional, and you do not have to fill it in unless your ISP has instructed you to do so.

`clonedmac`

MAC Address or String. Indicates whether to clone a MAC address. You must clone a MAC address if your ISP restricts connections to specific, recognized MAC addresses. This field can have the following values:

- A MAC address - The MAC address will be cloned. The MAC address must be six groups of two hexadecimal characters, with semicolons between the groups. For example: 00:08:d1:52:81:e2.
- `undefined` - No MAC address will be cloned.

The default value is `undefined`.

`usedhcp`

String. Indicates whether the Embedded NGX appliance should obtain an IP address automatically using DHCP. This can have the following values:

- `enabled` - Obtain an IP address automatically using DHCP.
- `disabled` - Do not obtain an IP address automatically using DHCP.
  If the connection type is LAN, you must provide values for the `gateway`, `address`, and `netmask` fields.
  If the connection type is PPTP, you must provide values for the `pptpclientmask` and `pptpclientip` fields.

The default value is `enabled`.

`staticwins`

String. Indicates whether the Embedded NGX appliance should automatically configure the WINS server. This can have the following values:

- `enabled` - The Embedded NGX appliance will not automatically configure the WINS server.
  You must provide a value for the `wins` field.
- `disabled` - The Embedded NGX appliance will automatically configure the WINS server.

`avoidgateway`

String. Indicates whether to automatically create a default route when an Internet connection is established. This can have the following values:

- `false` - A default route is created automatically, meaning that the traffic to all non-internal networks will be routed via this connection.
- `true` - A default route is not created automatically, and you can create the routes manually, using static routes. For information on using static routes, see ***netobj*** on page 465.

The default value is `false`.

This setting is only available through the command line.

`connectonlyactive`

String. Indicates whether the gateway should connect to the Internet only when it is the Active Gateway in the High Availability cluster. This can have the following values:

- `true` - The gateway will connect to the Internet only when it is the Active Gateway. This is called WAN High Availability.
- `false` - The gateway will connect to the Internet even if it is a Passive Gateway.

The default value is `false`.

This field is only relevant if High Availability is configured. For information on High Availability, see ***ha*** on page 335.

`staticdns`

String. Indicates whether the Embedded NGX appliance should automatically configure DNS servers. This can have the following values:

- `enabled` - The Embedded NGX appliance will not automatically configure DNS servers. You must provide values for the `dns1` and `dns2` fields.
- `disabled` - The Embedded NGX appliance will automatically configure the DNS servers.

`disabled`

String. Indicates whether the connection is disabled. This can have the following values:

- `true` - The connection is disabled.
- `false` - The connection is enabled.

The default value is `false`.

This field is useful if, for example, you are going on vacation and do not want to leave your computer connected to the Internet. Also, if you have two Internet connections, you can force the Embedded NGX appliance to use a particular connection, by disabling the other connection.

Note: The Internet connection's Enabled/Disabled status is persistent through Embedded NGX appliance reboots.

`dns1`

IP Address or String. The primary DNS server IP address. This can have the following values:

- An IP address
- `undefined` - This server is not defined.

The default value is `undefined`.

`dns2`

IP Address or String. The secondary DNS server IP address. This can have the following values:

- An IP address
- `undefined` - This server is not defined.

The default value is `undefined`.

`wins`

IP Address or String. The WINS server IP address. This can have the following values:

- An IP address
- `undefined` - This server is not defined.

The default value is `undefined`.

`uprate`

Integer or String. Indicates whether to enable Traffic Shaper for outgoing traffic. This can have the following values:

- A rate (in bytes/second) - The rate should be slightly lower than your Internet connection's maximum measured upstream speed.
  It is recommended to try different rates in order to determine which one provides the best results.
  For information on using Traffic Shaper, see ***qos classes*** on page 515.
- `unlimited` - Traffic Shaper is not enabled for outgoing traffic.

The default is `unlimited`.

`downrate`

Integer or String. Indicates whether to enable Traffic Shaper for incoming traffic. This can have the following values:

- A rate (in bytes/second) - The rate should be slightly lower than your Internet connection's maximum measured downstream speed in the field provided.
  It is recommended to try different rates in order to determine which one provides the best results.
- `unlimited` - Traffic Shaper is not enabled for outgoing traffic.

The default is `unlimited`.

Note: Traffic Shaper cannot control the number or type of packets it receives from the Internet; it can only affect the rate of incoming traffic by dropping received packets. This makes the shaping of inbound traffic less accurate than the shaping of outbound traffic. It is therefore recommended to enable traffic shaping for incoming traffic only if necessary. For information on using Traffic Shaper, see ***qos classes*** on page 515.

`connectondemand`

String. Indicates whether the appliance should connect to the Internet on demand.

- `disable` - The appliance is constantly connected to the Internet.
- `immediate` - The appliance should only establish a connection if no other connection exists, and the Embedded NGX appliance is not acting as a Backup appliance.
  If another connection opens, or if the Embedded NGX appliance becomes a Backup appliance, the appliance will disconnect.
  For information on configuring the appliance as a Backup or Master, refer to the User Guide.
- `activity` - The appliance should only establish a connection if no other connection exists, and there is outgoing activity (that is, packets need to be transmitted to the Internet).
  If another connection opens, or if the connection times out, the appliance will disconnect.

The default value is `disable`.

This field is useful when configuring a backup connection. For information, see refer to the User Guide.

This field is only relevant when using PPTP, PPPoE, PPPoA, or Dialup connection types.

`idletimeout`

Integer. The amount of time (in minutes) that the connection can remain idle. Once this period of time has elapsed, the appliance will disconnect.

The default value is 15.

This field is only relevant when using PPTP, PPPoE, PPPoA, or Dialup connection types.

`port`

String. The Embedded NGX appliance port on which to configure the connection. This can have the following values:

- `none` - No connection.
- `wan` - The WAN port. This allows configuring an Ethernet-based connection.
- `dmz` - The DMZ/WAN2 port. This allows configuring an Ethernet-based connection.
- `dsl` - The DSL port. This allows configuring an ADSL connection or an Ethernet-based connection. It is relevant for models with a built-in ADSL modem.
- `rs232` - The Serial port. This allows configuring a dialup connection via an RS232 modem.
- `usbmodem1` - A USB port. This allows configuring a dialup connection via a USB port.
- `lan<number>` - A LAN port, where number indicates the LAN port's number. For example, `lan4` represents LAN port 4. This allows configuring an Ethernet-based connection.

`bypassvpn`

String. Indicates whether to bypass VPN encryption for all connections made through this interface.

This can have the following values:

- `enabled` - Bypass VPN encryption for this interface.
- `disabled` - Do not bypass VPN encryption. All VPN connections through this interface will be encrypted.

The default value is `disabled`.

This setting is only available through the command line.

`bridge-to`

String. The bridge to which the connection is assigned. This can have the following values:

- `none` - The connection is not assigned to a bridge.
- The name of a bridge

The default value is `none`.

`bridge-stp-priority`

Integer. The port priority of the connection.

This field is only relevant if STP is enabled for the bridge.

The port's priority is combined with the port's logical number to create the port's ID. The port with the lowest ID is elected as the root port, which forwards frames out of the bridge. The other ports in the bridge calculate the least-cost path to the root port, in order to eliminate loops in the topology and provide fault tolerance.

To increase the chance of this port being elected as the root port, select a lower priority.

Note: If you select the same priority for all ports, the root port will be elected based on the port's logical number.

This must be an integer between 0 and 240, in increments of 16. The default value is 128.

`bridge-stp-cost`

Integer. The port cost of the connection.

This field is only relevant if STP is enabled for the bridge.

STP uses the available port with the lowest cost to forward frames to the root port. All other ports are blocked.

It is recommended to set a lower value for faster links.

The default value is 100.

`vlan-tag`

Integer. The WAN network's VLAN tag.

You must configure this field when the WAN port is configured as a VLAN trunk. For information on VLANs, see ***vlan*** on page 686.

This field is only available through the command line.

`hotspot`

String. Indicates whether to enable Secure HotSpot for the WAN network. This can have the following values:

- `enabled` - Secure HotSpot is enabled for the WAN.
- `disabled` - Secure HotSpot is disabled for the WAN.

The default value is `disabled`.

This setting is only available through the command line.

EXAMPLE 1

The following command configures the Embedded NGX appliance for a PPTP primary Internet connection on the WAN port:

```
set net wan mode pptp user JohnSmith.net.il@myisp password 123456
usedhcp disabled pptpserver 10.0.0.138 pptpservice RELAY_PPP1

pptpclientip 10.200.1.1 pptpclientmask 255.0.0.0 staticdns disabled
disabled false port wan
```

EXAMPLE 2

The following command configures the Embedded NGX appliance for a LAN primary Internet connection with DHCP on the WAN port:

```
set net wan mode lan disabled false port wan
```

EXAMPLE 3

The following command configures the Embedded NGX appliance for a PPPoE primary Internet connection:

```
set net wan mode pppoe user JohnSmith.net.il@myisp password 123456
staticdns enabled disabled false
```

EXAMPLE 4

The following command configures the Embedded NGX appliance for a PPTP primary Internet connection with DHCP:

```
set net wan mode pptp user JohnSmith password 123456 usedhcp enabled
pptpserver 212.143.205.253 staticdns disabled disabled false
```

EXAMPLE 5

The following command configures the Embedded NGX appliance for a PPPoA primary Internet connection on the DSL port:

```
set net wan mode pppoa user JohnSmith password 123456 staticdns
enabled disabled false port dsl
```

EXAMPLE 6

The following command configures the Embedded NGX for an Ethernet-based primary Internet connection on the WAN port, and assigns the connection to the "Bridge1" bridge:

```
set net wan mode bridged disabled false port wan bridge-to Bridge1
```

EXAMPLE 7

The following command displays the Embedded NGX appliance's cloned MAC address:

```
show net wan clonedmac
```

net wan atm

PURPOSE

The `net wan atm` variable is used for working with ADSL Asynchronous Transfer Mode (ATM) settings in the following ways:

- Configuring ATM settings for ADSL
- Displaying and exporting ATM settings

These settings are relevant for direct ADSL connections only. For information on configuring a direct ADSL connection, see ***net wan*** on page 399.

These settings are only relevant for models with a built-in ADSL modem.

SYNTAX

When used with `set`:

set net wan atm [vpi *vpi*] [vci *vci*] [encapsulation *encapsulation*]

When used with `show`:

show net wan atm [vpi | vci | encapsulation]

FIELDS

`vpi`	Integer. The VPI number to use for the ATM virtual path, as specified by your ISP. For a list of settings for various ISPs, see ***ADSL Settings*** on page 813.
`vci`	Integer. The VCI number to use for the ATM virtual circuit, as specified by your ISP. For a list of settings for various ISPs, see ***ADSL Settings*** on page 813.

`encapsulation`	String. The encapsulation type to use for the DSL line, as specified by your ISP. This can be one of the following: • `llc` • `vcmux` For a list of settings for various ISPs, see ***ADSL Settings*** on page 813.

EXAMPLE 1

The following command sets the WAN network's ATM settings:

```
set net wan atm vpi 1 vci 1 encapsulation llc
```

EXAMPLE 2

The following command displays the WAN network's ATM settings:

```
show net wan atm
```

net wan demand-connect

PURPOSE

The `net wan demand-connect` variable is used for working with connection delay settings for Internet connections on the WAN port in the following ways:

- Configuring connection delay settings
- Displaying and exporting connection delay settings

These settings are relevant only when using a PPTP, PPPoE, PPPoA, or Dialup connection for which connect-on-demand is enabled. For information on enabling connect-on-demand, see ***net wan*** on page 399 and refer to the `connectondemand` field.

SYNTAX

When used with `set`:

set net wan demand-connect delay *delay*

When used with `show`:

show net wan demand-connect [delay]

FIELDS

`delay`	Integer. The amount of time (in seconds) that the appliance should wait to re-connect to the Internet, if the connection goes down. If you have an unstable Internet connection that tends to go down and then return almost immediately, this setting allows you to avoid unnecessary and costly dialing during outage periods, by deferring re-connection for a few seconds. The default value is 0 seconds.

EXAMPLE 1

The following command sets the connection delay for the Internet connection currently using the WAN port:

```
set net wan demand-connect delay 10
```

EXAMPLE 2

The following command displays the connection delay for the Internet connection currently using the WAN port:

```
show net wan demand-connect
```

net wan ha

See ***net dmz ha*** on page 376.

net wan loadbalancing

PURPOSE

The `net wan loadbalancing` variable is used for working with WAN load balancing settings for Internet connections on the WAN port in the following ways:

- Configuring the connection's WAN load balancing weight
- Displaying and exporting this setting

When WAN load balancing is enabled, the Embedded NGX appliance automatically distributes traffic between the primary and secondary connections. By default, the load distribution between Internet connections is symmetric; however, you can configure non-symmetric load balancing by assigning a different load balancing weight to each Internet connection.

Note: To ensure full utilization of both Internet connections, the ratio between the connections' load balancing weights should reflect the ratio between the connections' bandwidths.

For instructions on enabling WAN load balancing, see ***loadbalancing*** on page 352. For more information on WAN load balancing, refer to the User Guide.

SYNTAX

When used with `set`:

set wan loadbalancing weight *weight*

When used with `show`:

show wan loadbalancing [weight]

FIELDS

`weight`	Integer. A value indicating the amount of traffic that should be routed though this connection relative to the other connection. For example, if you assign the primary connection a weight of 100, and you assign the secondary connection a weight of 50, twice as much traffic will be routed through the primary connection as through the secondary connection. This must be an integer between 1 and 100. The default value is 50.

EXAMPLE 1

The following command sets the load balancing weight for the Internet connection currently using the WAN port:

```
set net wan loadbalancing weight 75
```

EXAMPLE 2

The following command displays the load balancing weight for the Internet connection currently using the WAN port:

```
show net wan loadbalancing
```

net wan ospf

See ***net dmz ospf*** on page 378.

net wan ospf authentication

See ***net dmz ospf authentication*** on page 381.

net wan probe

PURPOSE

The `net wan probe` variable is used for working with connection probing settings for Internet connections on the WAN port in the following ways:

- Configuring connection probing settings
- Displaying and exporting connection probing settings

Note: Both the primary and secondary Internet connection can use the WAN port, depending on your Embedded NGX appliance's configuration. Therefore connection probing for the WAN port can affect the primary and secondary Internet connections. In contrast, connection probing for the WAN2 port will not affect the primary Internet connection, since this connection can only use the WAN port.

SYNTAX

When used with `set`:

set wan probe [probenexthop *probenexthop*] [method *method*] [dest1 *dest1*] [dest2 *dest2*] [dest3 *dest3*]

When used with `show`:

show wan probe [probenexthop | method | dest1 | dest2 | dest3]

FIELDS

`probenexthop`	String. Indicates whether to automatically detect loss of connectivity to the default gateway. If you selected LAN, this is done by sending ARP requests to the default gateway. If you selected PPTP, PPPoE, or Dialup, this is done by sending PPP echo reply (LCP) messages to the PPP peer. By default, if the default gateway does not respond, the Internet connection is considered to be down. If it is determined that the Internet connection is down, and two Internet connections are defined, a failover will be performed to the second Internet connection, ensuring continuous Internet

connectivity.

This field can have the following values:

- `enabled` - Check for loss of connectivity to the default gateway.
- `disabled` - Do not check for loss of connectivity to the default gateway.

This default value is `enabled`.

`method`

String. Indicates whether to perform connection probing and which method to use.

While the `probenexthop` option checks the availability of the next hop router, which is usually at your ISP, connectivity to the next hop router does not always indicate that the Internet is accessible. For example, if there is a problem with a different router at the ISP, the next hop will be reachable, but the Internet might be inaccessible. Connection probing is a way to detect Internet failures that are more than one hop away.

This field can have the following values:

- `none` - Do not perform Internet connection probing. Next hop probing will still be used, if the `probenexthop` option is enabled.
- `icmp` - Ping anywhere from one to three servers specified by IP address or DNS name in the `dest1`, `dest2`, and `dest3` fields. If for 45 seconds none of the defined servers respond to pinging, the Internet connection is considered to be down.
  Use this method if you have reliable servers that can be pinged, that are a good indicator of Internet connectivity, and that are not likely to fail simultaneously (that is, they are not at the same location).

- `dns` - Probe the primary and secondary DNS servers. If for 45 seconds neither gateway responds, the Internet connection is considered to be down.
  Use this method if the availability of your DNS servers is a good indicator for the availability of Internet connectivity.
- `rdp` - Send RDP echo requests to up to three Check Point VPN gateways specified by IP address or DNS name in the `dest1`, `dest2`, and `dest3` fields. If for 45 seconds none of the defined gateways respond, the Internet connection is considered to be down.
  Use this option if you have Check Point VPN gateways, and you want loss of connectivity to these gateways to trigger ISP failover to an Internet connection from which these gateways are reachable.

The default value is `none`.

`dest1, dest 2, dest 3`

String. If you chose the `icmp` connection probing method, this field specifies the IP addresses or DNS names of the desired servers. If you chose the `rdp` connection probing method, this field specifies the IP addresses or DNS names of the desired VPN gateways.

EXAMPLE 1

The following command enables next hop probing and DNS connection probing for the Internet connection currently using the WAN port:

```
set net wan probe probenexthop enabled method dns
```

EXAMPLE 2

The following command displays all connection probing settings for the Internet connection currently using the WAN port:

```
show net wan probe
```

net wan rip

See ***net dmz rip*** on page 383.

net wan rip authentication

See ***net dmz rip authentication*** on page 385.

net wan2

PURPOSE

The `net wan2` variable is used for doing the following:

- Configuring your Embedded NGX appliance's secondary Internet connection
- Displaying and exporting the secondary Internet connection's settings, including:
  - ATM settings
  - Connection delay settings
  - High Availability settings
  - WAN load balancing settings
  - OSPF settings
  - Connection probing settings

  For information on configuring, displaying, and exporting specific WAN ATM settings, see ***net wan2 atm*** on page 433. For information on configuring, displaying, and exporting specific connection delay settings, see ***net wan2 demand-connect*** on page 434. For information on configuring, displaying, and exporting specific WAN High Availability settings, see ***net wan2 ha*** on page 435. For information on configuring, displaying, and exporting specific WAN load balancing settings, see ***net wan2 loadbalancing*** on page 436. For information on configuring, displaying, and exporting specific WAN2 OSPF settings, see ***net wan2 ospf*** on page 437 and ***net wan2 ospf md5*** on page 438. For information on configuring, displaying, and exporting specific connection probing settings, see ***net wan2 probe*** on page 439.

When you configure both a primary and a secondary Internet connection, the secondary connection acts as a backup, so that if the primary connection fails, the Embedded NGX appliance remains connected to the Internet.

Note: You can configure different DNS servers for the primary and secondary connections. The Embedded NGX appliance acts as a DNS relay and routes requests from computers within the network to the appropriate DNS server for the active Internet connection.

For information on setting up your appliance for different types of secondary Internet connections, refer to the User Guide.

SYNTAX

See ***net wan*** on page 399.

FIELDS

See ***net wan*** on page 399.

EXAMPLE 1

The following command configures the Embedded NGX appliance for a dialup secondary Internet connection via an RS232 modem:

```
set net wan2 mode dialup username JohnS.myisp.com password 123456
phonenumber 96909111 disabled false port rs232
```

EXAMPLE 2

The following command configures the Embedded NGX appliance for a dialup secondary Internet connection via a USB modem:

```
set net wan2 mode dialup username JohnS.myisp.com password 123456
phonenumber 96909111 disabled false port usbmodem1
```

EXAMPLE 3

The following command configures the Embedded NGX appliance for a LAN secondary Internet connection with a static IP address:

```
set net wan2 mode lan usedhcp disabled address 212.150.8.74 gateway
212.150.8.65 netmask 255.255.255.224 staticdns disabled dns1
212.150.48.169 disabled false
```

EXAMPLE 4

The following command configures the Embedded NGX appliance for a PPPoE secondary Internet connection with a static IP address:

```
set net wan2 mode pppoe gateway undefined address undefined netmask
undefined password 123456  username JohnSmith.net.il@myisp mtu
automatic usedhcp disabled staticdns disabled dns1 undefined dns2
undefined wins undefined uprate 5000 downrate unlimited disabled false
```

EXAMPLE 5

The following command configures the Embedded NGX for an Ethernet-based secondary Internet connection on the WAN2 port, and assigns the connection to the "Bridge1" bridge:

```
set net wan2 mode bridged disabled false port wan2 bridge-to Bridge1
```

EXAMPLE 6

The following command displays the secondary Internet connection's uprate:

```
show net wan2 uprate
```

net wan2 atm

See ***net wan atm*** on page 416.

net wan2 demand-connect

See ***net wan demand-connect*** on page 418.

net wan2 ha

See ***net dmz ha*** on page 376.

net wan2 loadbalancing

See ***net wan loadbalancing*** on page 421.

net wan2 ospf

See ***net dmz ospf*** on page 378.

net wan2 ospf authentication

See ***net dmz ospf authentication*** on page 381.

net wan2 probe

See ***net wan probe*** on page 425.

net wan2 rip

See ***net dmz rip*** on page 383.

net wan2 rip authentication

See ***net dmz rip authentication*** on page 385.

net wlan

PURPOSE

The `net wlan` variable is used for working with the primary wireless network (WLAN) settings in the following ways:

- Configuring your Embedded NGX appliance's primary WLAN settings, including:
  - Hide Network Address Translation (NAT)
  - The primary WLAN's default gateway
  - The primary WLAN’s internal network range
  - DHCP (Dynamic Host Configuration Protocol) settings
  - Secure HotSpot access
  - The primary WLAN's bridge assignment and settings
- Displaying and exporting the above primary WLAN settings
- Displaying and exporting all primary WLAN settings, including primary WLAN High Availability and wireless connection settings.

  For information on configuring, displaying, and exporting specific primary WLAN High Availability settings, see ***net wlan ha*** on page 445. For information on configuring wireless connection settings for the primary WLAN network, see ***net wlan wireless*** on page 446.

When using wireless Embedded NGX models, you can define a wireless internal network called the primary WLAN. The primary WLAN is the main wireless network, and it controls all other wireless network's statuses: wireless networks can be enabled only if the primary WLAN is enabled, and disabling the primary WLAN automatically disables all other wireless network. In addition, all wireless networks inherit certain settings from the primary WLAN.

For information on default security policy rules controlling traffic to and from the primary WLAN, refer to the User Guide.

These settings are only relevant for models supporting a wireless interface.

Note: It is recommended to configure the primary WLAN via Ethernet and not via a wireless connection, because the wireless connection could be broken after making a change to the configuration.

Note: The DHCP server only serves computers that are configured to obtain an IP address automatically. If a computer is not configured to obtain an IP address automatically, it is recommended to assign it an IP address outside of the DHCP address range. If you do assign it an IP address within the DHCP address range, the DHCP server will not assign this IP address to another computer.

SYNTAX

When used with `set`:

set net wlan [mode *mode*] [hidenat *hidenat*] [address *address*] [netmask *netmask*] [dhcpserver *dhcpserver*] [dhcprange *dhcprange*] [dhcprelayip1 *dhcprelayip1*] [dhcprelayip2 *dhcprelayip2*] [hotspot *hotspot*] [bridge-to *bridge-to*] [bridge-range *bridge-range*] [bridge-stp-priority *bridge-stp-priority*] [bridge-stp-cost *bridge-stp-cost*] [bridge-antispoofing *bridge-antispoofing*]

When used with `show`:

show net wlan [mode | hidenat | address | netmask | dhcpserver | dhcprange | dhcprelayip1 | dhcprelayip2 | hotspot | bridge-to | bridge-range | bridge-stp-priority | bridge-stp-cost | bridge-antispoofing]

FIELDS

See ***net dmz*** on page 368.

EXAMPLE 1

The following command enables Hide NAT for the primary WLAN:

```
set net wlan hidenat enabled
```

EXAMPLE 2

The following command assigns the primary WLAN to the "Bridge1" bridge.

```
set net wlan mode bridged bridge-to Bridge1
```

EXAMPLE 3

The following command displays the primary WLAN's DHCP range:

```
show net wlan dhcprange
```

net wlan ha

See ***net dmz ha*** on page 376.

net wlan wireless

PURPOSE

The `net wlan wireless` variable is used for working with the primary WLAN's wireless connection settings in the following ways:

- Configuring your primary WLAN's wireless connection settings, including:
  - The primary WLAN's SSID
  - The security protocol
  - Advanced security settings
- Displaying and exporting the above wireless connection settings
- Displaying and exporting all primary WLAN wireless connection settings, including the WEP, WPA, and WPA-Personal settings.

  For information on configuring, displaying, and exporting specific WEP settings, see ***net wlan wireless wep*** on page 456. For information on configuring, displaying, and exporting specific WPA settings, see ***net wlan wireless wpa*** on page 459. For information on configuring, displaying, and exporting specific WPA-Personal settings, see ***net wlan wireless wpapsk*** on page 463.

In order for the primary WLAN's wireless connection settings to take effect, you must configure the primary WLAN and global wireless connection settings. For information on enabling and configuring the primary WLAN, see ***net wlan*** on page 442. For information on configuring global wireless connection settings, including the operation mode, security settings, and wireless transmitter settings, see ***wireless*** on page 800.

These settings are only relevant for models supporting a wireless interface.

SYNTAX

When used with `set`:

set net wlan wireless [netname *netname*] [hidenetname *hidenetname*] [macfilter *macfilter*] [datarate *datarate*] [fragthreshold *fragthreshold*] [rtsthreshold *rtsthreshold*] [station-to-station *station-to-station*] [beacon-interval *beacon-interval*] [dtim-period *dtim-period*] [xr *xr*] [wmm *wmm*] [security *security*] [wds *wds*]

When used with `show`:

show net wlan wireless [netname | hidenetname | macfilter | datarate | fragthreshold | rtsthreshold | station-to-station | beacon-interval | dtim-period | xr | wmm | security | wds]

FIELDS

`netname`

String. The network name (SSID) that identifies your wireless network.

This name will be visible to wireless stations passing near your access point, unless you enable the hidenetname option.

It can be up to 32 alphanumeric characters long and is case-sensitive.

`hidenetname`

String. Indicates whether the network's SSID is hidden. This can have the following values:

- `yes` - The SSID is hidden. Only devices to which your SSID is known can connect to your network.
- `no` - The SSID is not hidden. Any device within range can detect your network name and attempt to connect to your network.

The default value is `no`.

Note: Hiding the SSID does not provide strong security, because by a determined attacker can still discover your SSID. Therefore, it is not recommended to rely on this setting alone for security.

`macfilter`

String. Indicates whether MAC address filtering is enabled.

This can have the following values:

- `enabled` - MAC address filtering is enabled. Only MAC addresses that you added as network objects can connect to your network. For information on network objects, see ***netobj*** on page 465.
- `disabled` - MAC address filtering is disabled.

The default value is `disabled`.

Note: MAC address filtering does not provide strong security, since MAC addresses can be spoofed by a determined attacker. Therefore, it is not recommended to rely on this setting alone for security.

`datarate`

Integer or String. The transmission rate. This can have the following values:

- `auto` - The Embedded NGX appliance automatically selects a rate.
- A specific rate: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54, 72, 96, or 108
- For Safe@Office 1000NW and UTM-1 Edge NW, the following values are also available: mcs0, mcs1, mcs2, mcs3, mcs4, mcs5, mcs6, mcs7, mcs8, mcs9, mcs10, mcs11, mcs12, mcs13, mcs14, and mcs15

The default value is `auto`.

`fragthreshold`

Integer. The smallest IP packet size (in bytes) that requires that the IP packet be split into smaller fragments.

If you are experiencing significant radio interference, set the threshold to a low value (around 1000), to reduce error penalty and increase overall throughput.

Otherwise, set the threshold to a high value (around 2000), to reduce overhead.

The default value is 2346.

`rtsthreshold`

Integer. The smallest IP packet size for which a station must send an RTS (Request To Send) before sending the IP packet.

If multiple wireless stations are in range of the access point, but not in range of each other, they might send data to the access point simultaneously, thereby causing data collisions and failures. RTS ensures that the channel is clear before the each packet is sent.

If your network is congested, and the users are distant from one another, set the RTS threshold to a low value (around 500).

Setting a value equal to the fragmentation threshold effectively disables RTS.

The default value is 2346.

`station-to-station`	String. Indicates whether wireless stations on this network can communicate with each other. This can have the following values: • `allow` - Allow stations to communicate with each other. This is the default. • `block` - Block traffic between wireless stations.
`beacon-interval`	Integer. The interval of time in milliseconds between beacon transmissions. The access point broadcasts beacons, to inform wireless stations of its availability. To enable wireless clients to detect the access point more quickly, set a smaller interval between beacons. To increase network throughput and conserve power at the wireless stations, set a larger interval between beacons. The default value is 100 milliseconds. This setting is only available through the command line.

`dtim-period`

Integer. The interval between beacons that include a Delivery Traffic Indication Message (DTIM).

Before sending multicast or broadcast messages, the access point sends a beacon that includes a DTIM, to indicate to wireless stations that they should listen for data. The access point then sends a new DTIM every specified interval.

To improve multicast and broadcast data transmission, set a smaller interval between DTIMs. To conserve power and bandwidth at the wireless stations, set a larger interval between DTIMs.

The default value is 1, meaning that a DTIM is sent with every beacon.

This setting is only available through the command line.

`xr`

String. Indicates whether Extended Range (XR) mode is enabled. XR mode allows up to three times the range of a regular 802.11g access point, when communicating with stations that support XR.

This can have the following values:

- `enabled` - XR mode is enabled. XR will be automatically negotiated with XR-enabled wireless stations and used as needed.
- `disabled` - XR mode is disabled.

The default value is `enabled`.

This attribute is *not* relevant for the following appliance models: Safe@Office 1000NW and UTM-1 Edge NW.

`wmm`

String. Indicates whether to use the Wireless Multimedia (WMM) standard to prioritize traffic from WMM-compliant multimedia applications.

This can have the following values:

- `enabled` - WMM is enabled. The Embedded NGX appliance will prioritize multimedia traffic according to four access categories (Voice, Video, Best Effort, and Background). This allows for smoother streaming of voice and video when using WMM aware applications.
- `disabled` - WMM is disabled.

The default value is `disabled`.

`security`

String. The security protocol to use. This can have the following values:

- `none`
- `wep`
- `802.1x`
- `wpa` - Use WPA-Enterprise.
- `wpapsk` - Use WPA-Personal.

The default value is `none`.

For detailed information on the supported security protocols, refer to the User Guide.

If you choose `wep`, you must configure at least one WEP key. For information on configuring WEP settings, see ***net wlan wireless wep*** on page 456. The wireless stations must be configured with the same key as well.

If you chose `wpa` or `wpapsk`, you can configure additional security settings, such as key management and data encryption settings. See ***net wlan wireless wpa*** on page 459.

If you choose `wpapsk`, you must configure a passphrase. For information on configuring the passphrase, see ***net wlan wireless wpapsk*** on page 463. The wireless stations must be configured with this passphrase as well.

`wds`

String. Indicates whether to enable Wireless Distribution System (WDS) with WPA2 encryption, so as to extend the primary WLAN's coverage area.

This can have the following values:

- `enabled` - WDS is enabled. The Embedded NGX appliance acts as a WDS root and accepts connections from other WDS access points. You must add WDS links between the desired access points.
- `disabled` - WDS is disabled.

The default value is `disabled`.

For detailed information on setting up a WDS, refer to the User Guide.

This setting is only available through the command line.

It is only relevant for the following appliances: Safe@Office 1000NW and UTM-1 Edge NW.

EXAMPLE 1

The following command configures a wireless connection where the SSID is MyOffice, the SSID is hidden, and the security protocol used is WPA-Personal.

```
set net wlan wireless netname MyOffice hidenetname yes security
wpapsk
```

EXAMPLE 2

The following command displays the primary WLAN's SSID:

```
show net wlan wireless netname
```

net wlan wireless wep

PURPOSE

The `net wlan wireless wep` variable is used for working with the primary WLAN's WEP settings in the following ways:

- Configuring WEP keys
- Displaying and exporting WEP keys

These settings are only relevant when the primary WLAN is configured, and the selected security protocol is WEP. For information on enabling and configuring the primary WLAN, see ***net wlan*** on page 442. For information on setting the security protocol, see ***net wlan wireless*** on page 446.

These settings are only relevant for models supporting a wireless interface.

SYNTAX

When used with `set`:

set net wlan wireless wep [**defkey** *defkey*] [**key1** *key1*] [**key2** *key2*] [**key3** *key3*] [**key4** *key4*]

When used with `show`:

show net wlan wireless wep [**defkey** | **key1** | **key2** | **key3** | **key4**]

FIELDS

`defkey`

Integer. The number of the WEP key to use for transmission. The value must be between 1 and 4.

The default value is `1`.

The selected key must be entered in the same key slot (1-4) on the station devices, but the key need not be selected as the transmit key on the stations.

Note: You can use all four keys to receive data.

`key1 - key4`

String. A WEP key.

The key is composed of hexadecimal characters 0-9 and A-F, and is not case-sensitive.

The key length can be any of the following:

- 64 Bits. The key length is 10 characters.
- 128 Bits. The key length is 26 characters.
- 152 Bits. The key length is 32 characters.

Note: Some wireless card vendors call these lengths 40/104/128, respectively.

For the highest security, choose a long passphrase that is hard to guess.

Note: WEP is generally considered to be insecure, regardless of the selected key length.

EXAMPLE 1

The following command configures two WEP keys, and specifies that the second WEP key should be used for transmission:

```
set net wlan wireless wep defkey 2 key1 4FC0046169 key2 D8462C0BA9
```

EXAMPLE 2

The following command displays the WEP settings:

```
show net wlan wireless wep
```

net wlan wireless wpa

PURPOSE

The `net wlan wireless wpa` variable is used for working with the primary WLAN's WPA settings in the following ways:

- Configuring the WPA settings, including:
  - Restricting access to wireless clients that support WPA2
  - Key management settings
  - Data encryption settings
  - The authentication server to use for authenticating wireless clients
- Displaying and exporting WPA settings

These settings are only relevant when a primary WLAN is configured, and the selected security protocol is WPA-Enterprise or WPA-Personal. For information on enabling and configuring the primary WLAN, see ***net wlan*** on page 442. For information on setting the security protocol, see ***net wlan wireless*** on page 446.

These settings are only relevant for models supporting a wireless interface.

SYNTAX

When used with `set`:

set net wlan wireless wpa [wpa2only *wpa2only*] [group-key-update-interval *group-key-update-interval*] [master-key-update-interval *master-key-update-interval*] [cipher-suites *cipher-suites*] [authentication-server *authentication-server*]

When used with `show`:

show net wlan wireless wpa [wpa2only | group-key-update-interval | master-key-update-interval | cipher-suites]

FIELDS

`wpa2only`

String. Indicates whether wireless stations should be required to connect using WPA2 only.

The WPA2 security method uses the more secure Advanced Encryption Standard (AES) cipher, instead of the RC4 cipher used by WPA and WEP. When using WPA-Enterprise or WPA-Personal security methods, the Embedded NGX enables you to restrict access to the primary WLAN to wireless stations that support the WPA2 security method.

This can have the following values:

- `yes` - Only wireless stations using WPA2 can access the primary WLAN.
- `no` - Wireless stations using either WPA or WPA2 can access the primary WLAN.

The default value is `no`.

`group-key-update-interval`

Integer or String. The interval (in seconds) for changing the encryption keys. This can have the following values:

- `disabled` - Do not change encryption keys.
- A specific interval - A shorter interval ensures higher security.

The default value is 1800 seconds.

This setting is only available through the command line.

`master-key-update-interval`	Integer or String. The interval (in seconds) for deleting and renewing the Pair-wise Master Key (PMK) used for authentication. This can have the following values: • `disabled` - Do not delete and renew the PMK. • A specific interval The default value is 86400 seconds. This setting is only available through the command line.
`cipher-suites`	String. The cipher suite to use for data encryption. This can have the following values: • `aes-ccmp` - Use AES/CCMP. • `tkip` - Use TKIP (Temporal Key Integrity Protocol). • `auto` - The Embedded NGX appliance automatically selects the cipher suite to use. (Recommended) The default value is `auto`.
`authentication-server`	String. The authentication server to use for authenticating wireless clients. This can have the following values: • `radius` - A RADIUS server • `local` - The Embedded NGX EAP authenticator The default value is `radius`. If you select `radius`, you must configure a RADIUS server. See ***radius servers*** on page 527. If you select `local`, you must set up the network for use with the Embedded NGX EAP authenticator. For information, refer to the User Guide. This field is only relevant when using WPA-Enterprise.

EXAMPLE 1

The following command configures the primary WLAN to allow only wireless station using WPA2 to connect:

```
set net wlan wireless wpa wpa2only yes
```

EXAMPLE 2

The following command displays all WPA settings:

```
show net wlan wireless wpa
```

net wlan wireless wpapsk

PURPOSE

The `net wlan wireless wpapsk` variable is used for working with the primary WLAN's WPA-Personal settings in the following ways:

- Configuring the WPA-Personal passphrase
- Displaying and exporting the WPA-Personal passphrase

These settings are only relevant when the primary WLAN is configured, and the selected security protocol is WPA-Personal. For information on enabling and configuring the primary WLAN, see ***net wlan*** on page 442. For information on setting the security protocol, see ***net wlan wireless*** on page 446.

These settings are only relevant for models supporting a wireless interface.

SYNTAX

When used with `set`:

set net wlan wireless wpapsk passphrase *passphrase*

When used with `show`:

show net wlan wireless wpapsk [passphrase]

FIELDS

`passphrase`	String. The passphrase for accessing the network. This must be between 8 and 63 characters. It can contain spaces and special characters, and is case-sensitive. For the highest security, choose a long passphrase that is hard to guess.

EXAMPLE 1

The following command configures the WPA-Personal passphrase:

```
set net wlan wireless wpapsk passphrase D@34462Crf3-4%-ehj
```

EXAMPLE 2

The following command displays the WPA-Personal passphrase:

```
show net wlan wireless wpapsk
```

netobj

PURPOSE

The `netobj` variable is used for working with network objects in the following ways:

- Adding network objects
- Modifying network object settings
- Deleting network objects
- Displaying and exporting network object settings
- Clearing the Network Objects table

You can add individual computers or networks as network objects. This enables you to configure various settings for the computer or network represented by the network object.

You can configure the following settings for a network object:

- Static NAT (or One-to-One NAT)

  Static NAT allows the mapping of Internet IP addresses or address ranges to hosts inside the internal network. This is useful if you want a computer in your private network to have its own Internet IP address. For example, if you have both a mail server and a Web server in your network, you can map each one to a separate Internet IP address.

- Assign the network object's IP address to a MAC address

  You can guarantee that a particular computer's IP address remains constant, by reserving the IP address for use by the computer's MAC address only. This is called *DHCP reservation*, and it is useful if you are hosting a public Internet server on your network.

- Web Filtering enforcement

  You can specify whether or not to enforce the Web Filtering service and Web rules for the network object. Network objects that are excluded from such enforcement will be able to access the Internet without restriction. For information on Web Filtering, see ***webfilter*** on page 796. For information on Web rules, see ***webfilter rule*** on page 790.

- Secure HotSpot enforcement

  You can specify whether or not to exclude the network object from Secure HotSpot enforcement. Excluded network objects will be able to access the network without viewing the My HotSpot page. Furthermore, users on HotSpot networks will be able to access the excluded network object without viewing the My HotSpot page. For information on configuring Secure HotSpot, see ***hotspot*** on page 343.

- 802.1x port-based security enforcement

  When DHCP reservation is used, you can specify whether or not to exclude a computer from 802.1x port-based security enforcement. Excluded computers will be able to connect to the Embedded NGX appliance's ports and access the network without authenticating. For information on 802.1x port-based security, see ***port dmz security*** on page 502 and ***port lan security*** on page 508.

For more information on these settings, refer to the User Guide.

SYNTAX

When used with `add`:

add netobj name *name* type *type* ip *ip* [staticnat *staticnat*] [mac *mac*] [hotspotexclude *hotspotexclude*] [dot1xexclude *dot1xexclude*]

When used with `set`:

set netobj *number* [name *name*] [type *type*] [ip *ip*] [staticnat *staticnat*] [mac *mac*] [hotspotexclude *hotspotexclude*] [dot1xexclude *dot1xexclude*]

When used with `delete`:

delete netobj *number*

When used with `show`:

show netobj *number* [name | type | ip | staticnat | mac | hotspotexclude | dot1xexclude]

When used with `clear`:

clear netobj

FIELDS

number — Integer. The network object's row in the Network Objects table.

`name` — String. The network object's name.

`type` — String. The type of network object. This can have the following values:

- `computer`
- `network`

- `ip` — IP Address. The IP address of the network object. This can have the following values:
  - If the network object is a computer, this is the IP address of the local computer.
  - If the network object is a network, this is the network's IP address range. To specify a range, use the following format: `<Start IP Address>-<End IP Address>`

`staticnat` — IP Address or String. Indicates whether to perform Static NAT. This can have the following values:

- The Internet IP address to which you want to map the network object's IP address - Relevant only if the network object is a computer.
- The Internet IP address range to which you want to map the network object's IP address range - Relevant only if the network object is a network. To specify a range, use the following format: `<Start IP Address>-<End IP Address>`
- `undefined` - Static NAT is not performed.

The default value is `undefined`.

`mac`

MAC Address or String. Indicates whether to perform DHCP reservation. This can have the following values:

- The MAC address you want to assign to the network object's IP address. This must be six groups of two hexadecimal characters, with semicolons between the groups. For example: 00:08:d1:52:81:e2.
- `undefined` - DHCP reservation is not performed.

This field is only relevant for network objects that are computers.

The default value is `undefined`.

`hotspotexclude`

String. Indicates whether to exclude the network object from HotSpot enforcement. This can have the following values:

- `enabled` - The network object is excluded from HotSpot enforcement.
- `disabled` - HotSpot rules will be enforced for the network object.

The default value is `disabled`.

`ufpexclude`

String. Indicates whether to exclude this computer from the Web Filtering service and Web rule enforcement. This can have the following values:

- `enabled` - The network object is excluded from the Web FIltering service and Web rule enforcement.
- `disabled` - The Web Filtering service and Web rules will be enforced for the network object.

The default value is `disabled`.

`dot1xexclude` — String. Indicates whether to exclude this computer from the 802.1x port-based security enforcement. This can have the following values:

- `enabled` - The network object is excluded from 802.1x port-based security enforcement.
- `disabled` - 802.1x port-based security will be enforced for the network object.

The default value is `disabled`.

EXAMPLE 1

The following command adds a network object called "office", that represents a single computer:

```
add netobj name office type computer ip 192.168.10.21
```

EXAMPLE 2

The following command modifies network object 1 in the Network Objects table, so that DHCP reservation is performed, and the network object is excluded from HotSpot enforcement:

```
set netobj 1 mac 00:0c:6e:41:5d:6a hotspotexclude enabled
```

EXAMPLE 3

The following command deletes network object 1 in the Network Objects table:

```
delete netobj 1
```

EXAMPLE 4

The following command displays the Static NAT settings for network object 1 in the Network Objects table:

```
show netobj 1 staticnat
```

EXAMPLE 5

The following command deletes all network objects in the Network Objects table:

```
clear netobj
```

ospf

PURPOSE

The `ospf` variable is used for working with Open Shortest Path First (OSPF) settings in the following ways:

- Setting the OSPF mode
- Specifying the OSPF router identifier
- Setting the BGP log level
- Displaying and exporting the above OSPF settings
- Displaying and exporting all OSPF settings, including:
  - OSPF areas
  - OSPF networks
  - Routing information distribution settings
  - Default route generation settings

  For information on configuring, displaying, and exporting specific OSPF areas, see ***ospf area*** on page 473. For information on configuring, displaying, and exporting specific OSPF networks, see ***ospf network*** on page 479. For information on configuring, displaying, and exporting specific routing information distribution settings, see ***ospf redistribute connected*** on page 481 and ***ospf redistribute kernel*** on page 483. For information on configuring, displaying, and exporting specific default route generation settings, see ***ospf default-information*** on page 477.

The Embedded NGX appliance supports OSPF version 2, a dynamic routing protocol that distributes routing information between routers in a single autonomous system (AS). Each router in the AS distributes its local state (that is, the router's usable interfaces and reachable neighbors) to the other routers in the AS, and uses the link-state advertisements (LSAs) of the other routers to build and maintain a database describing the entire AS topology. This enables the routers to do the following:

- Automatically choose the best (least-cost) route for sending packets.
- Send packets to a single destination via multiple interfaces simultaneously.
- Reroute traffic around failures for high resiliency.

OSPF can be used together with route-based VPNs. For information on configuring route-based VPNs, see ***vpn sites*** on page 740.

Note: The Embedded NGX OSPF implementation is fully interoperable with the Check Point Advanced Routing Suite, as well as with any other RFC-compliant OSPF implementation.

Note: To use OSPF, your Embedded NGX appliance must be installed with an OSPF-enabled firmware. Such firmwares do not have a "b" appended to their version number. For example 8.0.21x supports OSPF, but 8.0.21xb does not.

OSPF-enabled firmwares do not support BGP.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set ospf [mode *mode*] [router-id *router-id*] [log-level *log-level*]

When used with `show`:

show ospf [mode | router-id | log-level]

FIELDS

`mode`

String. The OSPF mode. This can have the following values:

- `disable` - OSPF is disabled.
- `internal` - Enables OSPF for all internal networks.
- `all` - Enables OSPF for all networks.

The default value is `internal`.

`router-id`	IP Address or String. The OSPF router identifier. This can have the following values: • An IP address • `undefined` - No OSPF router is defined. The IP address with the highest numeric value will be used as the router ID. The default value is `undefined`.
`log-level`	String. The level of OSPF logs that should be written to the Embedded NGX appliance's Event Log. This can have the following values: • `low` • `medium` • `high` The default value is `low`.

EXAMPLE 1

The following command enables OSPF for all internal networks:

```
set ospf mode internal
```

EXAMPLE 2

The following command displays all OSPF settings:

```
show ospf
```

ospf area

PURPOSE

The `ospf area` variable is used for working with OSPF areas in the following ways:

- Adding OSPF areas
- Modifying OSPF areas
- Deleting OSPF areas
- Displaying and exporting OSPF area settings
- Clearing the OSPF Area table

An AS is divided into areas, each of which contains a number of networks. Each area has its own authentication settings.

These settings are only available through the command line.

SYNTAX

When used with `add`:

add ospf area id *id* [stub *stub*] [nssa *nssa*]

When used with `set`:

set ospf area *number* [id *id*] [stub *stub*] [nssa *nssa*]

When used with `delete`:

delete ospf area *number*

When used with `show`:

show ospf area *number* [id | stub | nssa]

When used with `clear`:

clear ospf area

FIELDS

number	Integer. The area's row in the OSPF Area table.
`id`	IP Address. The OSPF area's IP address.
`stub`	String. Indicates whether to configure the area as a stub area. Networks in a stub area accept and distribute link-state advertisements *within* the OSPF area only. Therefore, configuring an area as a stub reduces the AS topology database size for routers in the stub area. This can have the following values: • `true` - Configure the area as a stub. • `false` - Do not configure the area as a stub. The default value is `false`.
`nssa`	String. Indicates whether to configure the area as a Not-So-Stubby Area (NSSA). Like stubs, NSSAs do not accept link-state advertisements from other OSPF areas, nor do they distribute link-state advertisements to other OSPF areas. However, NSSAs import link-state advertisements from sources that are external to the AS. Configuring an area as NSSA minimizes the number of route updates and database synchronizations between OSPF routers. This can have the following values: • `true` - Configure the area as an NSSA. • `false` - Do not configure the area as an NSSA. The default value is `false`.

EXAMPLE 1

The following command adds an OSPF area:

```
add ospf area id 1.2.3.4
```

EXAMPLE 2

The following command modifies area 1 in the OSPF Areas table, so that it is configured as a stub:

```
set ospf area 1 stub true
```

EXAMPLE 3

The following command deletes area 1 in the OSPF Areas table:

```
delete ospf area 1
```

EXAMPLE 4

The following command displays all OSPF areas:

```
show ospf area
```

EXAMPLE 5

The following command deletes all areas in the OSPF Areas table:

```
clear ospf area
```

ospf default-information

PURPOSE

The `ospf default-information` variable is used for working with OSPF (Open Shortest Path First) settings in the following ways:

- Configuring the default route generation settings
- Displaying and exporting default route generation settings

These settings are only available through the command line.

SYNTAX

When used with `set`:

set ospf default-information [originate *originate*] [metric *metric*] [metric-type *metric-type*]

When used with `show`:

show ospf default-information [originate | metric | metric-type]

FIELDS

`originate`	String. Indicates whether to enable the router to generate default external routes. This can have the following values: • `true` - Enable default route generation. • `false` - Disable default route generation. The default value is `false`.
`metric`	Integer. The OSPF cost for default routes. The default value is 0.

`metric-type`	Integer. The external link type associated with the default route. This can have the following values: • `1` - Type 1 external route • `2` - Type 2 external route The default value is 2.

EXAMPLE 1

The following command enables default route generation:

```
set ospf default-information originate true metric 10 metric-type 1
```

EXAMPLE 2

The following command displays default route generation settings:

```
show ospf default-information
```

ospf network

PURPOSE

The `ospf network` variable is used for working with OSPF networks in the following ways:

- Adding OSPF networks
- Modifying OSPF networks
- Deleting OSPF networks
- Displaying and exporting OSPF networks
- Clearing the OSPF Networks table

To enable OSPF for a specific network, you must add the network as an OSPF network and assign it to an OSPF area.

These settings are only available through the command line.

SYNTAX

When used with `add`:

add ospf network address *address* mask *mask* area *area*

When used with `set`:

set ospf network *number* [address *address*] [mask *mask*] [area *area*]

When used with `delete`:

delete ospf network *number*

When used with `show`:

show ospf network *number* [address | mask | area]

When used with `clear`:

clear ospf network

FIELDS

number	Integer. The network 's row in the OSPF Networks table.
address	IP Address. The network's IP address.
mask	IP Address. The network's subnet mask.
area	IP Address. The OSPF area's IP address.

Example 1

The following command adds an OSPF network:

```
add ospf network address 1.2.3.4 mask 255.255.255.255 area 2.3.4.5
```

EXAMPLE 2

The following command assigns network 1 in the OSPF Networks table to a different area:

```
set ospf network 1 area 3.4.5.6
```

EXAMPLE 3

The following command deletes network 1 in the OSPF Networks table:

```
delete ospf network 1
```

EXAMPLE 4

The following command displays all OSPF networks:

```
show ospf network
```

EXAMPLE 5

The following command deletes all networks in the OSPF Networks table:

```
clear ospf network
```

ospf redistribute connected

PURPOSE

The `ospf redistribute connected` variable is used for working with OSPF (Open Shortest Path First) settings in the following ways:

- Configuring OSPF routing information distribution settings for directly connected networks
- Displaying and exporting OSPF routing information distribution settings for directly connected networks

These settings are only available through the command line.

SYNTAX

When used with `set`:

set ospf redistribute connected [enabled *enabled*] [metric *metric*] [metric-type *metric-type*]

When used with `show`:

show ospf redistribute connected [enabled | metric | metric-type]

FIELDS

`enabled`	String. Indicates whether to enable redistribution of OSPF routing information for connected networks. This can have the following values: • `true` - Enable redistribution. • `false` - Disable redistribution. The default value is `false`.
`metric`	Integer. The OSPF cost for redistributed routes. The default value is 0.

`metric-type`	Integer. The exterior metric type for redistributed routes. The Embedded NGX appliance supports metric types 1 and 2.

EXAMPLE 1

The following command enables redistributing routing information for connected networks:

```
set ospf redistribute connected enabled true metric 10 metric-type 1
```

EXAMPLE 2

The following command displays all redistribution settings for connected networks:

```
show ospf redistribute connected
```

ospf redistribute kernel

PURPOSE

The `ospf redistribute kernel` variable is used for working with OSPF (Open Shortest Path First) settings in the following ways:

- Configuring OSPF routing information distribution settings for routes updated in the Embedded NGX Portal
- Displaying and exporting OSPF routing information distribution settings for routes updated in the Embedded NGX Portal

These settings are only available through the command line.

SYNTAX

When used with `set`:

set ospf redistribute kernel [enabled *enabled*] [metric *metric*] [metric-type *metric-type*]

When used with `show`:

show ospf redistribute kernel [enabled | metric | metric-type]

FIELDS

`enabled`	String. Indicates whether to enable redistribution of OSPF routing information for routes updated in the Embedded NGX Portal. This can have the following values: • `true` - Enable redistribution. • `false` - Disable redistribution. The default value is `false`.
`metric`	Integer. The OSPF cost for redistributed routes. The default value is 0.
`metric-type`	Integer. The exterior metric type for redistributed routes. The Embedded NGX appliance supports metric types 1 and 2.

EXAMPLE 1

The following command enables redistributing routing information for for routes updated in the Embedded NGX Portal:

```
set ospf redistribute kernel enabled true metric 10 metric-type 1
```

EXAMPLE 2

The following command displays all redistribution settings for for routes updated in the Embedded NGX Portal:

```
show ospf redistribute kernel
```

pim-sm

PURPOSE

The `pim-sm` variable is used for working with Protocol Independent Multicast - Sparse-Mode (PIM-SM) multicast routing protocol settings in the following ways:

- Enabling/disabling PIM-SM
- Displaying and exporting the PIM-SM mode

The Embedded NGX appliance supports PIM-SM version 2, a multicast routing protocol that distributes routing information between routers in a single PIM domain. PIM-SM is useful if you need to use multicast routing in a sparse environment.

These settings are only relevant for N series appliances, and they are only available through the command line.

Note: To use PIM-SM, your Embedded NGX appliance must be installed with a PIM-SM-enabled firmware.

Note: The DVMRP and PIM-SM routers cannot be used simultaneously.

Note: You cannot enable the PIM-SM multicast routing protocol, when CISCO IOS DOS PIM protection is enabled in SmartDefense. To disable SmartDefense PIM protection, see ***smartdefense network-security ip-icmp cisco-ios*** on page *615*.

SYNTAX

When used with `set`:

set pim-sm mode *mode*

When used with `show`:

show pim-sm [mode]

FIELDS

`mode`	String. The PIM-SM mode. This can have the following values: • `disable` - PIM-SM is disabled. • `internal` - PIM-SM is enabled for internal routes only. • `all` - PIM-SM is enabled for all routes. The default value is `disable`. Route-based VPN is supported for `internal` modes.

EXAMPLE 1

The following command enables PIM-SM for all networks:

```
set pim-sm mode all
```

EXAMPLE 2

The following command displays all PIM-SM settings:

```
show pim-sm
```

port adsl

PURPOSE

The `port adsl` variable is used for working with the appliance's DSL port in the following ways:

- Modifying the DSL port's settings, including the DSL standard
- Displaying and exporting the above DSL port settings
- Displaying and exporting all DSL port settings, including:
  - Annex C settings
  - Automatic Seamless Rate Adaptation (SRA) settings
  - RX bin settings
  - TX bin settings

  For information on configuring, displaying, and exporting specific Annex C settings, see ***port adsl annexc*** on page 492. For information on configuring, displaying, and exporting cpecific automatic SRA settings, see ***port adsl auto-sra*** on page 494. For information on configuring, displaying, and exporting specific RX bin settings, see ***port adsl rxbin*** on page 496. For information on configuring, displaying, and exporting specific TX bin settings, see ***port adsl txbin*** on page 498.

These settings are only relevant for models with a built-in ADSL modem, and aside from the DSL standard setting, they are only available through the command line.

SYNTAX

When used with `set`:

set port adsl [standard *standard*] [framer-type *framer-type*] [trellis *trellis*] [expand *expand*] [txatten *txatten*] [coding-gain *coding-gain*] [maxbits-per-bin *maxbits-per-bin]* [fast-retrain *fast-retrain*] [esc-fast-retrain *esc-fast-retrain*] [bitswap *bitswap*] [upbitswap *upbitswap*] [ecfdm *ecfdm*] [power-mng *power-mng*]

When used with `show`:

show port adsl [standard | framer-type | trellis | expand | txatten | coding-gain | maxbits-per-bin | fast-retrain | esc-fast-retrain | bitswap | upbitswap | ecfdm | power-mng]

FIELDS

`standard`

String. The standard to support for the DSL line, as specified by your ISP. This can have the following values:

- `adsl2` - ADSL2
- `adsl2plus` - ADSL2+
- `gdmt` - G.DMT
- `glite` - G.Lite
- `multimode` - Automatically detect G.DMT or T1.413
- `t1413` - T.1413

The default value is `adsl2plus`.

For a list of settings for various ISPs, see ***ADSL Settings*** on page 813.

`framer-type`

Integer or String. The DSL line's overhead framing structure, from full overhead to reduced overhead.

This can have the following values:

- `0`
- `1`
- `2`
- `3`
- `3et`

The default value is `3et`.

This field is not relevant for the G.lite standard.

`trellis`

String. Indicates whether to use Trellis coding on the DSL interface. This can have the following values:

- `enabled` - Use Trellis coding.
- `disabled` - Do not use Trellis coding.

The default value is `enabled`.

`expand`

String. Indicates whether to use Expanded Exchange Sequence (EES). EES is useful for compatibility testing. This can have the following values:

- `enabled` - Use EES.
- `disabled` - Do not use EES.

The default value is `enabled`.

This field is only valid for the T1.413 standard.

`txatten`

Integer. The transmit power attenuation in dB.

This can have the following values: 0, 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12.

The default value is 0.

`coding-gain`

Integer or String. The gain due to Trellis/RS coding (coding gain). This can have the following values:

- auto - The coding gain changes automatically.
- An integer from 0-7 - Restrict the coding gain to a specific value (in dB).

The default value is `auto`.

`maxbits-per-bin`

Integer. The maximum number of receive bits per bin.

The default value is 14.

`fast-retrain`

String. Indicates whether to use fast retrain capability.

This can have the following values:

- `enabled` - Use fast retrain capability.
- `disabled` - Do not use fast retrain capability.

The default value is `disabled`.

This field is relevant only for the G.lite standard.

`esc-fast-retrain` String. Indicates whether to enable escape to fast retrain capability. This can have the following values:

- `enabled` - Enable escape to fast retrain capability.
- `disabled` - Disable escape to fast retrain capability.

The default value is `disabled`.

`bitswap` String. Indicates whether to use bit swapping for downstream traffic. This can have the following values:

- `enabled` - Use bit swapping for downstream traffic.
- `disabled` - Do not use bit swapping for downstream traffic.

The default value is `enabled`.

`upbitswap` String. Indicates whether to use bit swapping for upstream traffic. This can have the following values:

- `enabled` - Use bit swapping for upstream traffic.
- `disabled` - Do not use bit swapping for upstream traffic.

The default value is `enabled`.

`ecfdm` String. The echo cancellation and frequency division multiplexing mode to use. This can have the following values:

- `ec` - Echo cancellation mode
  `fdm` - Frequency division multiplexing mode with echo cancellation
- `fdmhp` - Frequency division multiplexing mode without echo cancellation
- `fdmnaf` - Frequency division multiplexing mode without analog filter

The default value is `ec`.

`power-mng`	String. The power management level 2 mode for online reconfiguration (OLR). This can have the following values: • `disable` - Power management is disabled. • `level2` - Power management level 2. • `level3` - Power management level 3. The default value is `level3`.

EXAMPLE 1

The following command sets the DSL line's standard:

```
set port adsl standard adsl2
```

EXAMPLE 2

The following command displays the DSL port's settings:

```
show port adsl
```

port adsl annexc

PURPOSE

The `port adsl annexc` variable is used for working with Annex C settings in the following ways:

- Configuring Annex C settings
- Displaying and exporting Annex C settings

These settings are only relevant for models with a built-in ADSL modem, and they are only available through the command line.

SYNTAX

When used with `set`:

set port adsl annexc [mode-item *mode-item*] [pilot-req *pilot-req*] [ttrr-offset *ttrr-offset*]

When used with `show`:

show port adsl annexc [mode-item | pilot-req | ttrr-offset]

FIELDS

`mode-item`	String. The bitmap transmission mode. This can have the following values: • `fbm` - Far End Cross Talk Bit Map (FBM) • `dbm` - Dual Bit Map (DBM) The default value is `fbm`.
`pilot-req`	Integer. Indicates whether to enable reception of Pilot Tone during the next period in the FEXT bitmap mode. This can have the following values: • `enabled` - Allow receiving pilot tone requests. • `disabled` - Do not allow pilot tone requests. The default value is `enabled`.

`ttrr-offset`	Integer. The offset from TTR_C (the timing reference used in ATU-C) to TTR_R (timing reference used in ATU-R). This can have the following values: • `offset0` • `offset42` The default value is `offset42`.

EXAMPLE 1

The following command sets the Annex C settings:

```
set port adsl annexc mode-item fbm pilot-req enabled ttrr-offset
offset42
```

EXAMPLE 2

The following command displays all Annex C settings:

```
show port adsl annexc
```

port adsl auto-sra

PURPOSE

The `port adsl auto-sra` variable is used for working with automatic SRA settings in the following ways:

- Configuring automatic SRA settings
- Displaying and exporting automatic SRA settings

Automatic Seamless Rate Adaptation (SRA) transparently changes the data rate of existing connections, to compensate for channel conditions. This helps prevent service interruptions.

These settings are only relevant for models with a built-in ADSL modem, and they are only available through the command line.

SYNTAX

When used with `set`:

set port adsl auto-sra [**mode** *mode*] [**crc** *crc*] [**fec** *fec*] [**up-shift** *up-shift*] [**down-shift** *down-shift*]

When used with `show`:

show port adsl auto-sra [**mode** | **crc** | **fec** | **up-shift** | **down-shift**]

FIELDS

`mode`	String. The automatic SRA (ADSL2/2+ Seamless Rate Adaptation) triggering mode. This can have the following values: • `enabled` - Automatic SRA triggering is enabled. • `disabled` - Automatic SRA triggering is disabled. The default value is `enabled`.

`crc`	Integer. The acceptable Cyclic Redundancy Check (CRC) error rate, expressed as the number of seconds within which one CRC error may occur. The default value is 1800 seconds.
`fec`	Integer. The acceptable Forward Error Correction (FEC) error rate, expressed as the number of seconds within which one FEC error may occur. The default value is 60 seconds.
`up-shift`	Integer. The observation period in seconds for margin up shift. The default value is 3600 seconds.
`down-shift`	Integer. The observation period in seconds for margin down shift. The default value is 600 seconds.

EXAMPLE 1

The following command enables automatic SRA:

```
set port adsl auto-sra mode enabled
```

EXAMPLE 2

The following command displays all automatic SRA settings:

```
show port adsl auto-sra
```

port adsl rxbin

PURPOSE

The `port adsl rxbin` variable is used for working with receive (RX) bin (frequency range) settings in the following ways:

- Configuring RX bin settings
- Displaying and exporting RX bin settings

These settings are only relevant for models with a built-in ADSL modem, and they are only available through the command line.

SYNTAX

When used with `set`:

set port adsl rxbin [auto-adjust *auto-adjust*] [start *start*] [end *end*]

When used with `show`:

show port adsl rxbin [auto-adjust | start | end]

FIELDS

`auto-adjust`	String. Indicates whether to enable automatic bin adjustment for receive signals. This can have the following values: • `enabled` - Automatic bin adjustment is enabled. • `disabled` - Automatic bin adjustment is disabled. The default value is `disabled`.
`start`	Integer. The lowest bin number allowed for receive signals. The default value is 32.
`end`	Integer. The highest bin number allowed for receive signals. The default value is 511.

EXAMPLE 1

The following command sets the RX bin settings:

```
set port adsl rxbin auto-adjust enabled start 32 end 511
```

EXAMPLE 2

The following command displays all RX bin settings:

```
show port adsl rxbin
```

port adsl txbin

PURPOSE

The `port adsl txbin` variable is used for working with transmit (TX) bin (frequency range) settings in the following ways:

- Configuring TX bin settings
- Displaying and exporting TX bin settings

These settings are only relevant for models with a built-in ADSL modem, and they are only available through the command line.

SYNTAX

When used with `set`:

set port adsl txbin [auto-adjust *auto-adjust*] [start *start*] [end *end*]

When used with `show`:

show port adsl txbin [auto-adjust | start | end]

FIELDS

`auto-adjust`	String. Indicates whether to enable automatic bin adjustment for transmit signals. This can have the following values: • `enabled` - Automatic bin adjustment is enabled. • `disabled` - Automatic bin adjustment is disabled. The default value is `enabled`.
`start`	Integer. The lowest bin number allowed for transmit signals. The default value is 6.
`end`	Integer. The highest bin number allowed for transmit signals. The default value is 31.

EXAMPLE 1

The following command sets the TX bin settings:

```
set port adsl txbin auto-adjust enabled start 6 end 31
```

EXAMPLE 2

The following command displays all TX bin settings:

```
show port adsl txbin
```

port dmz

PURPOSE

The `port dmz` variable is used for working with the appliance's DMZ/WAN2 port in the following ways:

- Modifying the DMZ/WAN2 port's settings
- Displaying and exporting the DMZ/WAN2 port's settings, including 802.1x port-based security settings

  For information on configuring, displaying, and exporting specific 802.1x port-based security settings, see ***port dmz security*** on page 502.

SYNTAX

When used with `set`:

set port dmz [network *network*] [hatrack *hatrack*] [link *link*]

When used with `show`:

show port dmz [network | hatrack | link]

FIELDS

`network`

String. The DMZ/WAN2 port's assignment. This can have the following values:

- `dmz` - The DMZ network. For information on configuring the DMZ, see ***net dmz*** on page 368.
- `internet` - A WAN Internet connection (either primary or secondary).
  For information on configuring the primary Internet connection, refer to the User Guide and to ***net wan*** on page 399. For information on configuring a secondary Internet connection, refer to ***net wan2*** on page 430.
- `trunk` - A VLAN trunk. For information on VLANs and VLAN trunks, see ***vlan*** on page 686.
- An existing port-based VLAN - For information on port-based VLANs, see ***vlan*** on page 686.
- `none` - The port is disabled.

- `from-radius` - A VLAN that is dynamically assigned by a RADIUS server, as part of an 802.1x port-based security scheme. For information on setting up 802.1x port-based security for this port, see ***port dmz security*** on page 502.

The default value is `dmz`.

`hatrack`

Integer. The amount to reduce the gateway's priority if the DMZ/WAN2 port's Ethernet link is lost.

The default value is 0.

`link`

String. The DMZ/WAN2 port's link speed and duplex. This can have the following values:

- `automatic` - The port automatically detects the link speed and duplex
- `10/full`
- `10/half`
- `100/full`
- `100/half`

The default value is `automatic`.

EXAMPLE 1

The following command assigns the DMZ/WAN2 port to a secondary WAN connection:

```
set port dmz network wan2
```

EXAMPLE 2

The following command displays the DMZ/WAN2 port's assignment:

```
show port dmz
```

port dmz security

PURPOSE

The `port dmz security` variable is used for working with the DMZ/WAN2 port's security settings in the following ways:

- Configuring 802.1x port-based security for the DMZ/WAN2 port
- Displaying and exporting the DMZ/WAN2 port's security settings

The Embedded NGX appliance supports the IEEE 802.1x standard for secure authentication of users and devices that are directly attached to Embedded NGX appliance's LAN and DMZ ports, as well as the wireless LAN. Authentication can be performed either by an external RADIUS server, or by the Embedded NGX appliance's built-in EAP authenticator. For information on the Embedded NGX EAP authenticator, refer to the User Guide.

When an 802.1x security scheme is implemented for a port, users attempting to connect to that port are required to authenticate using their network user name and password. The Embedded NGX appliance sends the user's credentials to the configured authentication server, and if authentication succeeds, a connection is established. If the user fails to authenticate, the port is physically isolated from other ports on the gateway.

If desired, you can specify how users should be handled after successful or failed authentication. Users who authenticate successfully on a specific port are assigned to the network with which that port is associated. When using a RADIUS server for authentication, you can assign authenticated users to specific network segments, by configuring dynamic VLAN assignment on the RADIUS server. Upon successful authentication, the RADIUS server sends RADIUS option 81 [Tunnel-Private-Group-ID] to the Embedded NGX appliance, indicating to which network segment the user should be assigned.

The Embedded NGX appliance also enables you to automatically assign users to a “Quarantine” network when authentication fails. All Quarantine network security and network rules will apply to those users.

You can choose to exclude specific network objects from 802.1x port-based security enforcement. Excluded network objects will be able to connect to the Embedded NGX appliance's ports and access the network without authenticating. For information on excluding network objects from 802.1x port-based security enforcement, see ***netobj*** on page 465.

For more information on setting up 802.1x port-based security, refer to the User Guide.

SYNTAX

When used with `set`:

set port dmz security [mode *mode*] [eap-reauth-period *eap-reauth-period*] [quarantine-network *quarantine-network*] [multiple-host *multiple-host*] [authentication-server *authentication-server*] [eap-timeout *eap-timeout*]

When used with `show`:

show port dmz security [mode | eap-reauth-period | quarantine-network | mutiple-host | authentication-server | eap-timeout]

FIELDS

`mode`

String. The port's security mode. This can have the following values:

- `disabled` - No security scheme is in use.
- `dot1x` - An 802.1x security scheme is enabled.

The default value is `disabled`.

`eap-reauth-period`

Integer or String. The interval of time in seconds after which the authenticated user must re-authenticate. This can have the following values:

- `none` - The user does not have to re-authenticate.
- A number

The default value is 3600 seconds.

This setting is only available through the command line.

`quarantine-network`	String. The name of the Quarantine network. This can have the following values: • `dmz` • Any existing VLAN. For information on adding VLANs, see ***vlan*** on page 686. • `none` - No Quarantine network is defined. The default value is `none`.
`mutiple-host`	String. Indicates whether to allow multiple clients to connect to this port via a hub or switch. This can have the following values: • `enabled` - Multiple clients can connect to this port. Each client must authenticate separately. If authentication fails for one host, then all clients on the port will be blocked. • `disabled` - Only one client can connect to this port at a time. The default value is `disabled`. Note: Enabling this option makes 802.1x port-based security less secure. Therefore, it is recommended to enable this option only in locations where the number of ports are a limiting factor, and where an external 802.1x-capable switch cannot be installed.

`authentication-server`	String. The authentication server to use for authenticating clients on this port. This can have the following values: • `radius` - A RADIUS server • `local` - The Embedded NGX EAP authenticator The default value is `radius`. If you select `radius`, you must configure a RADIUS server. See ***radius servers*** on page 527. If you select `local`, you must set up the network for use with the Embedded NGX EAP authenticator. For information, refer to the User Guide.
`eap-timeout`	Integer. The amount of time (in seconds) after which the client's session will time out, if it does not send an EAP response to the authentication server. The default value is 30 seconds. This setting is only available through the command line.

EXAMPLE 1

The following command enables 802.1x security for the DMZ/WAN2 port, and sets the VLAN1 network to be the Quarantine network:

```
set port dmz security mode dot1x quarantine-network VLAN1
```

EXAMPLE 2

The following command displays the DMZ/WAN2 port's security settings:

```
show port dmz security
```

port lan

PURPOSE

The `port lan` variable is used for working with the appliance's LAN ports in the following ways:

- Modifying the desired LAN port's settings
- Displaying and exporting the desired LAN port's settings, including 802.1x port-based security settings

  For information on configuring, displaying, and exporting specific 802.1x port-based security settings, see ***port lan security*** on page 508.

SYNTAX

When used with `set`:

set port lan*number* [network *network*] [hatrack *hatrack*] [link *link*]

When used with `show`:

show port lan*number* [network | hatrack | link]

FIELDS

`number`	Integer. The LAN port's number.
`network`	String. The port's assignment. This can have the following values: • `lan` - The LAN network • `internet` - A WAN Internet connection (either primary or secondary). For information on configuring the primary Internet connection, refer to the User Guide and to ***net wan*** on page 399. For information on configuring a secondary Internet connection, refer to ***net wan2*** on page 430. • An existing port-based VLAN - For information on port-based VLANs, see ***vlan*** on page 686. • `none` - The port is disabled. • `from-radius` - A VLAN that is dynamically

assigned by a RADIUS server, as part of an 802.1x port-based security scheme. For information on setting up 802.1x port-based security for this port, see ***port dmz security*** on page 502.

The default value is `lan`.

`hatrack`

Integer. The amount to reduce the gateway's priority if the LAN port's Ethernet link is lost.

The default value is 0.

`link`

String. The LAN port's link speed and duplex. This can have the following values:

- `automatic` - The port automatically detects the link speed and duplex
- `10/full`
- `10/half`
- `100/full`
- `100/half`

The default value is `automatic`.

EXAMPLE 1

The following command assigns the LAN1 port to a VLAN network called Marketing:

```
set port lan1 network Marketing
```

EXAMPLE 2

The following command displays the LAN4 port's assignment:

```
show port lan4
```

port lan security

PURPOSE

The `port lan security` variable is used for working with the appliance's LAN ports' security settings in the following ways:

- Configuring 802.1x port-based security for the desired LAN port
- Displaying and exporting the desired LAN port's security settings

For an overview of 802.1x port-based security, see ***port dmz security*** on page 502.

SYNTAX

When used with `set`:

set port lan*number* security [mode *mode*] [eap-reauth-period *eap-reauth-period*] [quarantine-network *quarantine-network*] [multiple-host *multiple-host*] [authentication-server *authentication-server*] [eap-timeout *eap-timeout*]

When used with `show`:

show port lan*number* security [mode | eap-reauth-period | quarantine-network | mutiple-host | authentication-server | eap-timeout]

FIELDS

`number`	Integer. The LAN port's number.

For additional fields, see ***port dmz security*** on page 502.

EXAMPLE 1

The following command enables 802.1x security for the LAN1 port, and sets the VLAN1 network to be the Quarantine network:

```
set port lan1 security mode dot1x quarantine-network vlan1
```

EXAMPLE 2

The following command displays the LAN4 port's security settings:

```
show port lan4 security
```

port serial

PURPOSE

The `port serial` variable is used for working with the appliance's Serial (RS232) port in the following ways:

- Modifying the Serial port's assignment
- Modifying the Serial port's speed
- Displaying and exporting the Serial port's assignment and speed

SYNTAX

When used with `set`:

set port serial [mode *mode*] [speed *speed*] [flow-control *flow-control*]

When used with `show`:

show port serial [mode] [speed] [flow-control]

FIELDS

`mode`

String. The Serial port's assignment. This can have the following values:

- `dialup` - A dialup modem. For information on configuring a dialup modem, see ***dialup*** on page 310.
- `console` - A serial console. For information on using a serial console, refer to the User Guide.
- `terminal-server` - The internal terminal server. For information on using the terminal server, see ***terminal-server*** on page 666.
- `disabled` - The Serial port is disabled.

The default value is `dialup`.

`speed`	Integer. The Serial port's speed (in bits per second). This can have the following values: • `9600` • `19200` • `38400` • `57600` • `115200` • `230400` The Serial port's speed must match that of the attached dialup modem or serial console. The default value is 57600.
`flow-control`	String. The method of flow control supported by the attached device. This can have the following values: • `rts-cts` - Hardware-based flow control, using the Serial port's RTS/CTS lines. • `xon-xoff` - Software-based flow control, using XON/XOFF characters. The default value is `rts-cts`.

EXAMPLE 1

The following command assigns the Serial port for use with a serial console:

```
set port serial mode console
```

EXAMPLE 2

The following command displays the Serial port's speed:

```
show port serial speed
```

port wan

PURPOSE

The `port dmz` variable is used for working with the appliance's WAN port in the following ways:

- Modifying the WAN port's settings
- Displaying and exporting the WAN port's settings

SYNTAX

When used with `set`:

set port wan [link *link*] [network *network*]

When used with `show`:

show port wan [link | network]

FIELDS

`link`

String. The WAN port's link speed and duplex. This can have the following values:

- `automatic` - The port automatically detects the link speed and duplex
- `10/full`
- `10/half`
- `100/full`
- `100/half`

The default value is `automatic`.

`network`	String. The port's assignment. This can have the following values: • `internet` - A WAN Internet connection (either primary or secondary). For information on configuring the primary Internet connection, refer to the User Guide and to ***net wan*** on page 399. For information on configuring a secondary Internet connection, refer to ***net wan2*** on page 430. • `none` - The port is disabled. The default value is `internet`.

EXAMPLE 1

The following command sets the WAN port's speed and duplex to automatic:

```
set port wan link automatic
```

EXAMPLE 2

The following command displays the WAN port's assignment:

```
show port wan network
```

printers

PURPOSE

The `printers` variable is used for working with network printers in the following ways:

- Modifying printer port numbers
- Displaying and exporting printer port numbers

Some Embedded NGX models include a built-in print server, enabling you to connect up to four USB-based printers to the appliance and share them across the network. The appliance automatically detects printers as they are plugged in, and they immediately become available for printing.

Usually, no special configuration is required on the Embedded NGX appliance. However, you may sometimes need to change the port number after completing printer setup. For example, you may want to replace a malfunctioning network printer, with another existing network printer, without reconfiguring the client computers. To do this, you must change the replacement printer's port number to the malfunctioning printer's port number, using the `printers` variable.

These settings are only relevant for models supporting a print server.

SYNTAX

When used with `set`:

set printers *number* port *port*

When used with `show`:

show printers [*number* [port]]

FIELDS

number	The printer's row in the Printers table.
port	Integer. The network printer's TCP port number. Note: Printer port numbers may not overlap, and must be high ports.

EXAMPLE 1

The following command assigns TCP port 9100 to printer 1:

```
set printer 1 port 9100
```

EXAMPLE 2

The following command displays all printers and their port numbers:

```
show printers
```

qos classes

PURPOSE

The `qos classes` variable is used for working with Traffic Shaper settings in the following ways:

- Adding QoS classes
- Modifying QoS classes
- Deleting QoS classes
- Displaying and exporting QoS class settings
- Clearing the Quality of Service Classes table

Traffic Shaper is a bandwidth management solution that allows you to set bandwidth policies to control the flow of communication.

Traffic Shaper classifies traffic in user-defined Quality of Service (QoS) classes and divides available bandwidth among the classes according to weight. If a specific QoS class is not using all of its bandwidth, the leftover bandwidth is divided among the remaining QoS classes, in accordance with their relative weights.

Your Embedded NGX appliance offers different degrees of traffic shaping, depending on its model:

- Simplified Traffic Shaper. Includes a fixed set of four predefined classes. You can assign network traffic to each class, but you cannot modify the classes, delete them, or create new classes.
- Advanced Traffic Shaper. Includes a set of four predefined classes, but enables you to modify the classes, delete them, and create new classes. You can define up to eight classes.

Some models do not include Traffic Shaper.

For further information about Traffic Shaper, refer to the User Guide.

Note: Traffic Shaper must be enabled for the direction of traffic specified in the rule. For information on enabling Traffic Shaper, refer to the User Guide.

Traffic Shaper cannot control the number or type of packets it receives from the Internet; it can only affect the rate of incoming traffic by dropping received packets. This makes the shaping of inbound traffic less accurate than the shaping of outbound traffic. It is therefore recommended to enable traffic shaping for incoming traffic only if necessary.

Note: To use Traffic Shaper, you must create Allow or Allow and Forward rules that assign different types of connections to QoS classes. See ***fw rules*** on page *322*.
For example, if Traffic Shaper is enabled for outgoing traffic, and you create an Allow rule associating all outgoing VPN traffic with the Urgent QoS class, then Traffic Shaper will handle outgoing VPN traffic as specified in the bandwidth policy for the Urgent class.
If you do not assign a connection type to a class, Traffic Shaper automatically assigns the connection type to the built-in "Default" class.

SYNTAX

When used with `add`:

add qos classes name *name* weight *weight* [uplimit *uplimit*] [downlimit *downlimit*] [delayclass *delayclass*] [dscp *dscp*] [upguarantee *upguarantee*] [downguarantee *downguarantee*]

When used with `set`:

set qos classes *number* [name *name*] [uplimit *uplimit*] [downlimit *downlimit*] [weight *weight*] [delayclass *delayclass*] [dscp *dscp*] [upguarantee *upguarantee*] [downguarantee *downguarantee*]

When used with `delete`:

delete qos classes *number*

When used with `show`:

show qos classes [*number*] [name | uplimit | downlimit | weight | delayclass | dscp | upguarantee | downguarantee]

When used with `clear`:

clear qos classes

FIELDS

`number`	Integer. The QoS class's row in the Traffic Shaper table.
`name`	String. The class's name. For example, if you are creating a class for high priority Web connections, you can name the class "High Priority Web".
`uplimit`	Integer or String. The maximum rate (in bytes/second) of outgoing traffic belonging to this class. This can have the following values: • A rate • `unlimited` - The maximum rate of outgoing traffic belonging to this class is unlimited. The default value is `unlimited`.
`downlimit`	Integer or String. The maximum rate (in bytes/second) of incoming traffic belonging to this class. This can have the following values: • A rate • `unlimited` - The maximum rate of incoming traffic belonging to this class is unlimited. The default value is `unlimited`.
`weight`	Integer. A value indicating the class's importance relative to the other defined classes. For example, if one class's weight is 100, and another class's weight is 50, the first class will be allocated twice the amount of bandwidth as the second when the lines are congested.

`delayclass`

String. The degree of precedence to give this class in the transmission queue. This can have one of the following values:

- `bulk` - Traffic that is not sensitive to long delays. For example, SMTP traffic (outgoing email).
- `normal` - Normal traffic
- `interactive` - Traffic that is highly sensitive to delay. For example, IP telephony, videoconferencing, and interactive protocols that require quick user response, such as telnet.

Traffic Shaper serves delay-sensitive traffic with a lower latency. That is, Traffic Shaper attempts to send packets with an `interactive` level before packets with a `normal` or `bulk` level.

The default value is `normal`.

`dscp`

Integer. The class's DiffServ Code Point (DSCP). The DSCP must be between 0 and 63.

If you include this field, packets belonging to this class will be marked with a DSCP. The marked packets will be given priority on the public network according to their DSCP.

To use this option, your ISP or private WAN must support DiffServ. You can obtain the correct DSCP value from your ISP or private WAN administrator.

The default value is 0.

`upguarantee`

Integer or String. The guaranteed minimum bandwidth (in bytes/second) for outgoing traffic belonging to this class. This can have the following values:

- A rate
- `none` - The bandwidth for outgoing traffic belonging to this class is calculated according to the class's weight.

The default value is `none`.

`downguarantee`

Integer or String. The guaranteed minimum bandwidth (in bytes/second) for incoming traffic belonging to this class. This can have the following values:

- A rate
- `none` - The bandwidth for incoming traffic belonging to this class is calculated according to the class's weight.

The default value is `none`.

EXAMPLE 1

The following command adds a QoS class named Crucial, with a relative weight of 50:

```
add qos classes name Crucial weight 50
```

EXAMPLE 2

The following command modifies QoS class 1 in the Quality of Service Classes table, so that it is classified as interactive traffic:

```
set qos classes 1 delayclass interactive
```

EXAMPLE 3

The following command deletes QoS class 1 in the Quality of Service Classes table:

```
delete qos classes 1
```

EXAMPLE 4

The following command displays the maximum rate of outgoing traffic for QoS class 1 in the Quality of Service Classes table:

```
show qos classes 1 downlimit
```

EXAMPLE 5

The following command deletes all QoS classes in the Quality of Service Classes table:

```
clear qos classes
```

radius

PURPOSE

The `radius` variable is used for working with RADIUS settings in the following ways:

- Configuring the NAS IP address
- Configuring the Embedded NGX appliance's behavior upon RADIUS authentication failure
- Configuring the interval for sending accounting information to RADIUS servers
- Displaying and exporting the above RADIUS settings
- Displaying and exporting all RADIUS settings including:
  - RADIUS servers
  - RADIUS permissions

  For information configuring, displaying, and exporting specific RADIUS server and RADIUS permission settings, see ***radius servers*** on page 527 and ***radius permissions*** on page 524.

You can use RADIUS to authenticate both Embedded NGX appliance users and Remote Access VPN Clients trying to connect to the Embedded NGX appliance. When a user accesses the Embedded NGX Portal and tries to log on, the Embedded NGX appliance sends the entered user name and password, along with the gateway's Network Access Server (NAS) IP address, to the RADIUS server. The server then checks whether the RADIUS database contains a matching user name and password pair. If so, then the user is logged on.

SYNTAX

When used with `set`:

set radius [nas-ip-address *nas-ip-address*] [on-access-reject *on-access-reject*] [account-interval *account-interval*]

When used with `show`:

show radius [nas-ip-address | on-access-reject | account-interval]

FIELDS

`nas-ip-address`

IP Address or String. The NAS IP address to use for RADIUS requests.

The NAS IP address serves as a unique identifier for the gateway, when making RADIUS requests. By default, the NAS IP address is the IP address of the gateway interface on which the user is trying to authenticate. If this IP address is not unique, (such as when Hide NAT is enabled), you can specify a different NAS IP address using this field.

This can have the following values:

- An IP address
- `auto` - The IP address of the interface on which the user is trying to authenticate.

The default value is `auto`.

This setting is only available through the command line.

`on-access-reject`

String. Specifies how the Embedded NGX appliance's should behave when RADIUS authentication fails.

This can have the following values:

- `reject-user` - Deny the user access.
- `try-next` - Authenticate to the secondary RADIUS server. If a secondary RADIUS server is not defined, or if authentication to the secondary RADIUS server fails, deny the user access.

The default value is `reject-user`.

This setting is only available through the command line.

`account-interval`

Integer or String. The interval at which the Embedded NGX appliance should send accounting information to the RADIUS server during a user session.

This can have the following values:

- `disabled` - The Embedded NGX appliance will only send accounting information to the RADIUS server at the beginning and end of a session.
- The interval in seconds - The Embedded NGX appliance will send accounting information to the RADIUS server throughout a session, every specified number of seconds.

This field is only relevant when RADIUS accounting is enabled. For information on enabling RADIUS accounting, see ***radius servers*** on page 527.

EXAMPLE 1

The following command sets the NAS IP address:

```
set radius nas-ip-address 192.168.10.21
```

EXAMPLE 2

The following command displays all RADIUS settings

```
show radius
```

radius permissions

PURPOSE

The `radius permissions` variable is used for working with RADIUS permissions in the following ways:

- Setting permissions for all users authenticated by the defined RADIUS servers
- Displaying and exporting RADIUS permissions

SYNTAX

When used with `set`:

set radius permissions [adminaccess *adminaccess*] [vpnaccess *vpnaccess*] [filteroverride *filteroverride*] [hotspotaccess *hotspotaccess*] [rdpaccess *rdpaccess*] [users-manager *users-manager*]

When used with `show`:

show radius permissions [adminaccess | vpnaccess | filteroverride | hotspotaccess | rdpaccess | users-manager]

FIELDS

`adminaccess`

String. The level of access to the Embedded NGX Portal to assign to all users authenticated by the RADIUS server. This can have the following values:

- `none` - The user cannot access the Embedded NGX Portal.
- `readonly` - The user can log on to the Embedded NGX Portal, but cannot modify system settings.
- `users-manager` - The user can log on to the Embedded NGX Portal and add, edit, or delete "No Access"-level users. However, the user cannot modify other system settings.
- `readwrite` - The user can log on to the Embedded NGX Portal and modify system settings.

The default level is `none`.

`vpnaccess`

String. Indicates whether to allow all users authenticated by the RADIUS server to remotely access your network via VPN. This can have the following values:

- `true` - Authenticated users can remotely access your network via VPN.
- `false` - Authenticated users cannot remotely access your network via VPN.

This field is only relevant if the Embedded NGX Remote Access VPN Server is enabled. See ***vpn server*** on page 727.

`filteroverride`

String. Indicates whether to allow all users authenticated by the RADIUS server to override Web Filtering. This can have the following values:

- `true` - Authenticated users can override Web Filtering.
- `false` - Authenticated users cannot override Web Filtering.

This option is only relevant if the Web Filtering service is defined. See webfilter mode.

`hotspotaccess`

String. Indicates whether to allow all users authenticated by the RADIUS server to access the My HotSpot page. This can have the following values:

- `true` - Authenticated users can access the My HotSpot page.
- `false` - Authenticated users cannot access the My HotSpot page.

This option is only relevant if Secure HotSpot is enabled. See ***hotspot*** on page 343.

`rdpaccess`

String. Indicates whether to allow all users authenticated by the RADIUS server to remotely access computers' desktops, using the Remote Desktop feature. This can have the following values:

- `true` - Authenticated users can log on to the my.firewall portal, view the Active Computers page, and remotely access computers' desktops.
  Note: Authenticated users can perform these actions, even if their level of administrative access (`adminaccess`) is `none`.
- `false` - Authenticated users cannot remotely access computers' desktops.

This option is only relevant if Remote Desktop is enabled. See ***remote-desktop*** on page 534.

`users-manager`

String. Indicates whether to allow all users authenticated by the RADIUS server to log in to the Embedded NGX Portal and add, edit, or delete "No Access"-level users, but not modify other system settings. This can have the following values:

- `true` - Authenticated users can log in to the Embedded NGX Portal and add, edit, or delete "No Access"-level users.
- `false` - Authenticated users cannot log in to the Embedded NGX Portal and add, edit, or delete "No Access"-level users.

EXAMPLE 1

The following command enables users authenticated by the RADIUS server to override Web Filtering and modify system settings:

```
set radius permissions adminaccess readwrite filteroverride true
```

EXAMPLE 2

The following command displays all RADIUS permissions:

```
show radius permissions
```

radius servers

PURPOSE

The `radius servers` variable is used for working with RADIUS servers in the following ways:

- Adding RADIUS servers
- Modifying RADIUS server settings
- Displaying and exporting RADIUS server settings
- Clearing the servers in the RADIUS table

SYNTAX

When used with `add`:

add radius servers address *address* secret *secret* [port *port*] [realm *realm*] [timeout *timeout*] [tries *tries*] [accounting *accounting*] [accounting-port *accounting-port*]

When used with `set`:

set radius servers *number* [address *address*] [secret *secret*] [port *port*] [realm *realm*] [timeout *timeout*] [tries *tries*] [accounting *accounting*] [accounting-port *accounting-port*]

When used with `show`:

show radius servers [*number*] [address | secret | port | realm | timeout | tries | accounting | accounting-port]

When used with `clear`:

clear radius servers

FIELDS

`number`	Integer. The RADIUS server's number.
`address`	IP Address. The IP address of the computer that runs the RADIUS service (one of your network computers).
`secret`	String. The shared secret to use for secure communication with the RADIUS server.
`port`	Integer. The port number on the RADIUS server's host computer. The default is 1812.
`realm`	String. The realm to append to RADIUS requests. The realm will be appended to the username as follows: <username>@<realm> For example, if you set the realm to "myrealm", and the user "JohnS" attempts to log on to the Embedded NGX Portal, the Embedded NGX appliance will send the RADIUS server an authentication request with the username "JohnS@myrealm". This field is only relevant if your organization uses RADIUS realms.
`timeout`	Integer. The interval of time in seconds between attempts to communicate with the RADIUS server. The default value is 3.
`tries`	Integer. The number of attempts that should be made to communicate with the RADIUS server before determining that it is unreachable.

`accouting`	String. Indicates whether RADIUS accouting is enabled. This can have the following values: • `enabled` - RADIUS accouting is enabled. • `disabled` - RADIUS accounting is disabled. The default value is `disabled`.
`accounting-port`	Integer. The port number on the RADIUS server's host computer to use for RADIUS accounting purposes. The default port number is 1813.

EXAMPLE 1

The following command adds a RADIUS server located at 192.168.10.21, with the shared secret "mysharedsecret" and the RADIUS realm "mycompany":

```
add radius servers address 192.168.10.21 secret mysharedsecret realm
mycompany
```

No port number is specified, so the default port (1812) will be used.

EXAMPLE 2

The following command specifies that RADIUS server 1 should use port 1814:

```
set radius servers 1 port 1814
```

EXAMPLE 3

The following command displays the IP address of RADIUS server 1 in the RADIUS table:

```
show radius servers 1 address
```

EXAMPLE 4

The following command deletes all network objects in the Network Objects table:

```
clear radius servers
```

remote-cli

PURPOSE

The `remote-cli` variable is used for working with remote CLI access settings in the following ways:

- Enabling remote CLI access
- Configuring the remote CLI access shared secret
- Displaying and exporting the above remote CLI access settings
- Displaying and exporting all remote CLI access settings including the remote CLI white list

  For information configuring, displaying, and exporting remote CLI white list settings, see ***remote-cli white-list*** on page 532.

If the Embedded NGX has a USB modem attached, you can run CLI commands by sending text messages from your cellular phone. For information on setting up and using this feature, see ***Sending CLI Commands via Text Messages*** on page 12.

SYNTAX

When used with `set`:

set remote-cli [mode *mode*] [shared-secret *shared-secret*]

When used with `show`:

show remote-cli [mode | shared-secret]

FIELDS

`mode`	String. Indicates whether remote CLI access is enabled. This can have the following values: • `enabled` - Remote CLI access is enabled. • `disabled` - Remote CLI access is disabled. The default value is `disabled`.

`shared-secret`	String. The shared secret to use for secure communication between the cellular phone and the USB modem. In each text message sent to the USB modem, the shared secret must precede the CLI command, as described in ***Sending Text Messages*** on page 12.

EXAMPLE 1

The following command enables remote CLI access:

```
set remote-cli mode enabled
```

EXAMPLE 2

The following command displays all remote CLI access settings:

```
show remote-cli
```

remote-cli white-list

PURPOSE

The `remote-cli white-list` variable is used for working with remote CLI white list settings in the following ways:

- Configuring whether to use the remote CLI white list
- Configuring the remote CLI white list
- Displaying and exporting the above remote CLI white list settings

If remote CLI access is enabled, you can configure a list of up to 10 cellular phones from which the USB modem should receive CLI commands sent via text message. For information on enabling remote CLI access, see ***remote-cli*** on page 530.

SYNTAX

When used with `set`:

set remote-cli white-list [accept-all *accept-all*] [phone-number1 *phone-number1*] [phone-number2 *phone-number2*] [phone-number3 *phone-number3*] [phone-number4 *phone-number4*] [phone-number5 *phone-number5*] [phone-number6 *phone-number6*] [phone-number7 *phone-number7*] [phone-number8 *phone-number8*] [phone-number9 *phone-number9*] [phone-number10 *phone-number10*]

When used with `show`:

show remote-cli white-list [accept-all | phone-number1 | phone-number2 | phone-number3 | phone-number4 | phone-number5 | phone-number6 | phone-number7 | phone-number8 | phone-number9 | phone-number10]

FIELDS

`accept-all`

String. Indicates whether to accept CLI commands from any cellular phone, ignoring the configured remote CLI white list.

This can have the following values:

- `enabled` - Accept CLI commands from all cellular phones, and do not use the configured remote CLI white list.
- `disabled` - Accept CLI commands only from the cellular phones included in the remote CLI white list.

The default value is `disabled`.

`phone-number1 /`
`phone-number2 /`
`phone-number3 /`
`phone-number4 /`
`phone-number5 /`
`phone-number6 /`
`phone-number7 /`
`phone-number8 /`
`phone-number9 /`
`phone-number10`

String. A cellular phone number from which the USB modem should accept CLI commands sent via text message.

EXAMPLE 1

The following command enables remote CLI access:

```
set remote-cli white-list mode enabled
```

EXAMPLE 2

The following command displays all remote CLI white list settings:

```
show remote-cli white-list
```

remote-desktop

PURPOSE

The `remote-desktop` variable is used for working with Remote Desktop settings in the following ways:

- Enabling Remote Desktop
- Optimizing Remote Desktop sessions
- Displaying and exporting the above Remote Desktop settings
- Displaying and exporting all Remote Desktop settings including:
  - Device redirection settings
  - Display settings

  For information configuring, displaying, and exporting specific device redirection settings, see ***remote-desktop device-redirect*** on page 536. For information configuring, displaying, and exporting Remote Desktop display settings, see ***remote-desktop display*** on page 539.

Your Embedded NGX appliance includes an integrated client for Microsoft Terminal Services, allowing you to remotely access the desktop of each of your computers from anywhere, via the Embedded NGX Portal. You can even redirect your printers or ports to a remote computer, so that you can print and transfer files with ease.

For information on setting up and using Remote Desktop, refer to the User Guide.

SYNTAX

When used with `set`:

set remote-desktop [mode *mode*] [optimize-performance *optimize-performance*]

When used with `show`:

show remote-desktop [mode | optimize-performance]

FIELDS

`mode`	String. Indicates whether Remote Desktop is enabled. This can have the following values: • `enabled` - Remote Desktop is enabled. • `disabled` - Remote Desktop is disabled. The default value is `disabled`.
`optimize-performance`	String. Indicates whether Remote Desktop is optimized for slow links. This can have the following values: • `true` - Remote Desktop is optimized for slow links. Bandwidth-consuming options, such as wallpaper and menu animations, will be disabled. • `false` - Remote Desktop is not optimized for slow links. The default value is `true`.

EXAMPLE 1

The following command enables Remote Desktop access:

```
set remote-desktop mode enabled
```

EXAMPLE 2

The following command displays the Remote Desktop optimization setting:

```
show remote-desktop optimize-performance
```

remote-desktop device-redirect

PURPOSE

The `remote-desktop device-redirect` variable is used for working with Remote Desktop device redirection settings in the following ways:

- Configuring Remote Desktop device redirection settings
- Displaying and exporting Remote Desktop device redirection settings

SYNTAX

When used with `set`:

set remote-desktop device-redirect [com-ports *com-ports*] [drives *drives*] [printers *printers*] [smartcards *smartcards*]

When used with `show`:

show remote-desktop device-redirect [com-ports | drives | printers | smartcards]

FIELDS

`com-ports`

String. Indicates whether to allow the host computer to access COM ports on the client computer. This enables remote users to access their local COM ports when logged on to the host computer.

This can have the following values:

- `true` - The host computer can access COM ports on the client computer.
- `false` - The host computer cannot access COM ports on the client computer.

The default value is `true`.

`drives`

String. Indicates whether to allow the host computer to access hard drives on the client computer. This enables remote users to access their local hard drives when logged on to the host computer.

This can have the following values:

- `true` - The host computer can access hard drives on the client computer.
- `false` - The host computer cannot access hard drives on the client computer.

The default value is `true`.

`printers`

String. Indicates whether to allow the host computer to access printers on the client computer. This enables remote users to access their local printers when logged on to the host computer.

This can have the following values:

- `true` - The host computer can access printers on the client computer.
- `false` - The host computer cannot access printers on the client computer.

The default value is `true`.

`smartcards`

String. Indicates whether to allow the host computer to access smartcards on the client computer. This enables remote users to access their local smartcards when logged on to the host computer.

This can have the following values:

- `true` - The host computer can access smartcards on the client computer.
- `false` - The host computer cannot access smartcards on the client computer.

The default value is `false`.

EXAMPLE 1

The following command enables redirecting COM port access for Remote Desktop sessions:

```
set remote-desktop device-redirect com-ports true
```

EXAMPLE 2

The following command displays all Remote Desktop device redirection settings:

```
show remote-desktop device-redirect
```

remote-desktop display

PURPOSE

The `remote-desktop display` variable is used for working with Remote Desktop display settings in the following ways:

- Configuring Remote Desktop display settings
- Displaying and exporting Remote Desktop display settings

SYNTAX

When used with `set`:

set remote-desktop display fullscreen *fullscreen*

When used with `show`:

show remote-desktop display [fullscreen]

FIELDS

`fullscreen`	String. Indicates whether to open Remote Desktop sessions on the whole screen. This can have the following values: • `true` - Open Remote Desktop session on the whole screen. • `false` - Do not open Remote Desktop session on the whole screen. The default value is `false`.

EXAMPLE 1

The following command configures Remote Desktop to open sessions on the whole screen:

```
set remote-desktop display fullscreen true
```

EXAMPLE 2

The following command displays the Remote Desktop display setting:

```
show remote-desktop display
```

rip

PURPOSE

The `rip` variable is used for working with Routing Information Protocol (RIP) settings in the following ways:

- Enabling/disabling RIP
- Setting the RIP log level
- Displaying and exporting the above RIP settings
- Displaying and exporting all RIP settings, including:
  - RIP networks
  - Routing information distribution settings

  For information on configuring, displaying, and exporting specific RIP networks, see ***rip network*** on page 543. For information on configuring, displaying, and exporting specific routing information distribution settings, see ***rip redistribute connected*** on page 545 and ***rip redistribute kernel*** on page 547.

The Embedded NGX appliance supports RIP version 2 dynamic routing protocol. RIP is suitable for use in smaller networks.

These settings are only relevant for N series appliances, and they are only available through the command line.

SYNTAX

When used with `set`:

set rip [**mode** *mode*] [**log-level** *log-level*]

When used with `show`:

show rip [**mode** | **log-level**]

FIELDS

`mode`	String. The RIP mode. This can have the following values: • `disable` - RIP is disabled. • `internal` - RIP is enabled for internal routes only. • `all` - RIP is enabled for all routes. The default value is `disable`.
`log-level`	String. The level of RIP logs that should be written to the Embedded NGX appliance's Event Log. This can have the following values: • `low` • `medium` • `high` The default value is `low`.

EXAMPLE 1

The following command enables RIP for all networks:

```
set rip mode all
```

EXAMPLE 2

The following command displays all RIP settings:

```
show rip
```

rip network

PURPOSE

The `rip network` variable is used for working with RIP networks in the following ways:

- Adding RIP networks
- Modifying RIP networks
- Deleting RIP networks
- Displaying and exporting RIP networks
- Clearing the RIP Networks table

To enable RIP for a specific network, you must add the network as a RIP network.

These settings are only relevant for N series appliances, and they are only available through the command line.

SYNTAX

When used with `add`:

add rip network address *address* mask *mask*

When used with `set`:

set rip network *number* [address *address*] [mask *mask*]

When used with `delete`:

delete rip network *number*

When used with `show`:

show rip network *number* [address | mask]

When used with `clear`:

clear rip network

FIELDS

number	Integer. The network 's row in the RIP Networks table.
address	IP Address. The network's IP address.
mask	IP Address. The network's subnet mask.

EXAMPLE 1

The following command adds a RIP network:

```
add rip network address 1.2.3.4 mask 255.255.255.255
```

EXAMPLE 2

The following command modifies the subnet mask of network 1 in the RIP Networks table:

```
set rip network 1 mask 255.255.255.0
```

EXAMPLE 3

The following command deletes network 1 from the RIP Networks table:

```
delete rip network 1
```

EXAMPLE 4

The following command displays all RIP networks:

```
show rip network
```

EXAMPLE 5

The following command deletes all networks in the RIP Networks table:

```
clear rip network
```

rip redistribute connected

PURPOSE

The `rip redistribute connected` variable is used for working with RIP settings in the following ways:

- Configuring RIP routing information distribution settings for directly connected networks
- Displaying and exporting RIP routing information distribution settings for directly connected networks

These settings are only relevant for N series appliances, and they are only available through the command line.

SYNTAX

When used with `set`:

set rip redistribute connected [enabled *enabled*] [metric *metric*]

When used with `show`:

show rip redistribute connected [enabled | metric]

FIELDS

`enabled`	String. Indicates whether to enable redistribution of RIP routing information for connected networks. This can have the following values: • `true` - Enable redistribution. • `false` - Disable redistribution. The default value is `false`.
`metric`	Integer. The RIP cost for redistributed routes. The default value is 0.

EXAMPLE 1

The following command enables redistributing routing information for connected networks:

```
set rip redistribute connected enabled true metric 10
```

EXAMPLE 2

The following command displays all redistribution settings for connected networks:

```
show rip redistribute connected
```

rip redistribute kernel

PURPOSE

The `rip redistribute kernel` variable is used for working with RIP settings in the following ways:

- Configuring RIP routing information distribution settings for routes updated in the Embedded NGX Portal
- Displaying and exporting RIP routing information distribution settings for routes updated in the Embedded NGX Portal

These settings are only relevant for N series appliances, and they are only available through the command line.

SYNTAX

When used with `set`:

set rip redistribute kernel [enabled *enabled*] [metric *metric*]

When used with `show`:

show rip redistribute kernel [enabled | metric]

FIELDS

`enabled`	String. Indicates whether to enable redistribution of RIP routing information for routes updated in the Embedded NGX Portal. This can have the following values: • `true` - Enable redistribution. • `false` - Disable redistribution. The default value is `false`.
`metric`	Integer. The RIP cost for redistributed routes. The default value is 0.

EXAMPLE 1

The following command enables redistributing routing information for for routes updated in the Embedded NGX Portal:

```
set rip redistribute kernel enabled true metric 10
```

EXAMPLE 2

The following command displays all redistribution settings for for routes updated in the Embedded NGX Portal:

```
show rip redistribute kernel
```

routes

PURPOSE

The `routes` variable is used for working with static routes in the following ways:

- Adding static routes
- Modifying static route settings
- Deleting static routes
- Displaying and exporting static route settings
- Clearing the Static Routes table

A static route is a setting that explicitly specifies the route to use for packets, according to *one* of the following criteria:

- The packet's source IP address and/or destination IP address
- The network service used to send the packet

Packets that match the criteria for a specific static route are sent to the route's defined destination, or *next hop*, which can be a specific gateway's IP address or an Internet connection. Packets with a source, destination, or network service that do not match any defined static route are routed to the default gateway.

For more information on static routes, refer to the User Guide.

SYNTAX

When used with `add`:

add routes gateway *gateway* metric *metric* [network *network*] [netmask *netmask*] [source *source*] [srcmask *srcmask*]

When used with `set`:

set routes *number* [gateway *gateway*] [metric *metric*] [network *network*] [netmask *netmask*] [source *source*] [srcmask *srcmask*]

When used with `delete`:

delete routes *number*

When used with `show`:

show routes [*number*] [gateway | metric | network | netmask | source | srcmask]

When used with `clear`:

clear routes

FIELDS

number	Integer. The route's row in the Static Routes table.
`network`	IP Address or String. The IP address of the destination network. This can have the following values: • An IP address • `undefined` - The route applies to all destination networks.
`netmask`	IP Address or String. The subnet mask of the destination network. This can have the following values: • A subnet mask • `undefined` - The route applies to all destination network subnet masks.
`gateway`	IP Address or String . The next hop to which to route packets matching this static route's criteria. This can be any of the following: • The IP address of the desired gateway (next hop router) • `wan` - The Internet connection on the WAN1 interface. • `wan2` - The Internet connection on the WAN2 interface. • A VPN site
`metric`	Integer. The static route's metric. The gateway sends a packet to the route that matches the packet's destination and has the lowest metric.

`source` — IP Address or String. The IP address of the source network.

This can have the following values:

- An IP address
- `undefined` - The route applies to all source networks.

`srcmask` — IP Address or String. The subnet mask of the source network.

This can have the following values:

- An subnet mask
- `undefined` - The route applies to all source network subnet masks.

`service` — String. The service used to send packets (service routing). This can have the following values:

- `any` - This route applies to packets sent using any service.
- A network service object

Note: When defining a static route for a specific service, the `source` and `network` fields must be set to `undefined`.

EXAMPLE 1

The following command adds the static route with a metric of 90:

```
add routes network 192.168.253.1 netmask 255.255.255.0 gateway
212.143.205.233 metric 90
```

EXAMPLE 2

The following command changes the metric of route 2 to 80:

```
set routes 2 metric 80
```

EXAMPLE 3

The following command deletes route 2:

```
delete routes 2
```

EXAMPLE 4

The following command displays the settings for all routes:

```
show routes
```

EXAMPLE 5

The following command clears the Static Routes table:

```
clear routes
```

smartdefense ai cifs file-sharing

PURPOSE

The `smartdefense ai cifs file-sharing` variable is used for working with file sharing settings in the following ways:

- Configuring CIFS file sharing defense settings
- Displaying and exporting CIFS file sharing defense settings, including worm patterns

  For information on configuring, displaying, and exporting specific worm patterns settings, see ***smartdefense ai cifs file-sharing patterns*** on page 555.

Microsoft operating systems and Samba clients rely on Common Internet File System (CIFS), a protocol for sharing files and printers. However, this protocol is also widely used by worms as a means of propagation.

SYNTAX

When used with `set`:

set smartdefense ai cifs file-sharing [enforce *enforce*] [log *log*]

When used with `show`:

show smartdefense ai cifs file-sharing [enforce | log]

FIELDS

`enforce`	String. Indicates whether to enable CIFS worm blocking. This can have the following values: • `enabled` - CIFS worm blocking is enabled. • `disabled` - CIFS worm blocking is disabled. The default value is `disabled`.

`log`	String. Indicates whether to log CIFS worm attacks. This can have the following values: • `disabled` - Do not log attacks. • `enabled` - Log attacks The default value is `disabled`.

EXAMPLE 1

The following command enables CIFS worm blocking and logging:

```
set smartdefense ai cifs file-sharing enforce enabled log log
```

EXAMPLE 2

The following command displays all CIFS file sharing defense settings, including worm patterns:

```
show smartdefense ai cifs file-sharing
```

smartdefense ai cifs file-sharing patterns

PURPOSE

The `smartdefense ai cifs file-sharing patterns` variable is used for working with CIFS worm patterns in the following ways:

- Adding worm patterns
- Modifying worm patterns
- Deleting worm patterns
- Displaying and exporting worm patterns
- Clearing the CIFS Worm Patterns table

Worm patterns are matched against file names (including file paths but excluding the disk share name) that the client is trying to read or write from the server. If a match is detected, SmartDefense takes action according to the file sharing settings specified in ***smartdefense ai cifs file-sharing*** on page 553.

You can reset the CIFS worm patterns to their defaults. See ***reset smartdefense ai cifs file-sharing patterns*** on page 54.

SYNTAX

When used with `add`:

add smartdefense ai cifs file-sharing patterns name *name* active *active* regexp *regexp*

When used with `set`:

set smartdefense ai cifs file-sharing patterns *number* [name *name*] [active *active*] [regexp *regexp*]

When used with `delete`:

delete smartdefense ai cifs file-sharing patterns *number*

When used with `show`:

show smartdefense ai cifs file-sharing patterns [*number*] [name | active | regexp]

When used with `clear`:

clear smartdefense ai cifs file-sharing patterns

FIELDS

`number`	Integer. The worm pattern's row in the CIFS Worm Patterns table.
`name`	String. The worm's name.
`active`	String. Indicates whether SmartDefense should check files for this worm pattern. This can have the following values: • `true` - Check files for this worm pattern. • `false` - Do not check files for this worm pattern. The default value is `true`.
`regexp`	String. The worm pattern's regular expression.

EXAMPLE 1

The following command adds a worm pattern and activates it:

```
add smartdefense ai cifs file-sharing patterns name Worm active true
regexp \.worm$
```

EXAMPLE 2

The following command deactivates worm pattern 1 in the CIFS Worm Patterns table:

```
set smartdefense ai cifs file-sharing patterns 1 active false
```

EXAMPLE 3

The following command deletes worm pattern 1 in the CIFS Worm Patterns table:

```
delete smartdefense ai cifs file-sharing patterns 1
```

EXAMPLE 4

The following command displays all worm patterns:

```
show smartdefense ai cifs file-sharing patterns
```

EXAMPLE 5

The following command clears the CIFS Worm Patterns table:

```
clear smartdefense ai cifs file-sharing patterns
```

smartdefense ai ftp

PURPOSE

The `smartdefense ai ftp` variable is used for working with FTP settings in the following ways:

- Configuring FTP settings
- Displaying and exporting FTP settings, including FTP Bounce settings and FTP command settings

  For information on configuring specific FTP Bounce settings, see ***smartdefense ai ftp bounce*** on page 561. For information on configuring specific FTP Command settings, see ***smartdefense ai ftp commands*** on page 563.

FTP settings allow you to configure various protections related to the FTP protocol.

SYNTAX

When used with `set`:

set smartdefense ai ftp [enforce-commands *enforce-commands*] [known-ports *known-ports*] [port-overflow *port-overflow*]

When used with `show`:

show smartdefense ai ftp [enforce-commands | known-ports | port-overflow]

FIELDS

`enforce-commands` — String. Indicates whether to block illegal FTP commands in the FTP commands list. For information on configuring and viewing the FTP commands list, see ***smartdefense ai ftp commands*** on page 563.

This field can have the following values:

- `enabled` - Block illegal FTP commands.
- `disabled` - Do not block illegal FTP commands.

The default value is `enabled`.

`known-ports`

String. Indicates whether to block the FTP server from connecting to well-known ports. This provides a second layer of protection against FTP bounce attacks, by preventing such attacks from reaching well-known ports.

Note: Known ports are published ports associated with services (for example, SMTP is port 25).

This field can have the following values:

- `enabled` - Block the FTP server from connecting to well-known ports.
- `disabled` - Do not block the FTP server from connecting to well-known ports.

The default value is `disabled`.

`port-overflow`

String. Indicates whether block PORT commands that contain a number greater than 255.

FTP clients send PORT commands when connecting to the FTP sever. A PORT command consists of a series of numbers between 0 and 255, separated by commas. Blocking PORT commands that do not comply to the FTP standard helps prevent potential attacks against the FTP server.

This field can have the following values:

- `enabled` - Block PORT commands that contain a number greater than 255.
- `disabled` - Do not block PORT commands that contain a number greater than 255.

The default value is `disabled`.

EXAMPLE 1

The following command enables blocking the FTP server from connecting to well-known ports:

```
set smartdefense ai ftp known-ports enabled
```

EXAMPLE 2

The following command displays all FTP settings:

```
show smartdefense ai ftp
```

smartdefense ai ftp bounce

PURPOSE

The `smartdefense ai ftp bounce` variable is used for working with FTP Bounce settings in the following ways:

- Configuring FTP Bounce settings
- Displaying and exporting FTP Bounce settings

When connecting to an FTP server, the client sends a PORT command specifying the IP address and port to which the FTP server should connect and send data. An FTP Bounce attack is when an attacker sends a PORT command specifying the IP address of a third party instead of the attacker's own IP address. The FTP server then sends data to the victim machine.

SYNTAX

When used with `set`:

set smartdefense ai ftp bounce [enforce *enforce*] [log *log*]

When used with `show`:

show smartdefense ai ftp bounce [enforce | log]

FIELDS

`enforce`	String. Indicates whether to enable FTP Bounce attack blocking. This can have the following values: • `enabled` - FTP Bounce attack blocking is enabled. • `disabled` - FTP Bounce attack blocking is disabled. The default value is `enabled`.

`log`	String. Indicates whether to log FTP Bounce attacks. This can have the following values: • `enabled` - Log FTP Bounce attacks. • `disabled` - Do not log FTP Bounce attacks. The default value is `enabled`.

EXAMPLE 1

The following command enables blocking and logging FTP Bounce attacks:

```
set smartdefense ai ftp bounce enforce enabled log enabled
```

EXAMPLE 2

The following command displays all FTP Bounce settings:

```
show smartdefense ai ftp bounce
```

smartdefense ai ftp commands

PURPOSE

The `smartdefense ai ftp commands` variable is used for working with FTP command settings in the following ways:

- Adding FTP commands
- Modifying FTP commands
- Deleting FTP commands
- Displaying and exporting FTP commands
- Clearing the FTP Commands table

Some seldom-used FTP commands may compromise FTP server security and integrity. You can specify which FTP commands should be considered illegal.

If SmartDefense detects an illegal FTP command, it takes action according to `enforce-commands` settings specified in ***smartdefense ai ftp*** on page 558.

SYNTAX

When used with `add`:

add smartdefense ai ftp commands command *command* [allowed *allowed*]

When used with `set`:

set smartdefense ai ftp commands *number* [command *command*] [allowed *allowed*]

When used with `delete`:

delete smartdefense ai ftp commands *number*

When used with `show`:

show smartdefense ai ftp commands [*number*] [command | allowed]

When used with `clear`:

clear smartdefense ai ftp commands

FIELDS

`number`	Integer. The FTP command's row in the FTP Commands table.
`command`	String. The FTP command.
`allowed`	String. Indicates whether the FTP command is legal. This can have the following values: • `true` - The FTP command is legal. SmartDefense will allow this command. • `false` - The FTP command is illegal. SmartDefense will handle this command in accordance with `enforce-commands` settings specified in ***smartdefense ai ftp*** on page 558. The default value is `true`.

EXAMPLE 1

The following command adds an FTP command and marks it as illegal:

```
add smartdefense ai ftp commands command ARBOR allowed true
```

EXAMPLE 2

The following command marks FTP command 1 in the FTP Commands table as legal:

```
set smartdefense ai ftp commands 1 allowed false
```

EXAMPLE 3

The following command deletes FTP command 1 in the FTP Commands table:

```
delete smartdefense ai ftp commands 1
```

EXAMPLE 4

The following command displays all FTP commands:

```
show smartdefense ai ftp commands
```

EXAMPLE 5

The following command clears the FTP Commands table:

```
clear smartdefense ai ftp commands
```

smartdefense ai games xbox-live

PURPOSE

The `smartdefense ai games xbox-live` variable is used for working with XBox LIVE settings in the following ways:

- Configuring XBox LIVE settings
- Displaying and exporting XBox LIVE settings

XBox 360 requires gateways hosting XBox LIVE games to use the "Open NAT" method rather than the normal "Strict NAT" method. Therefore, if you want to host online games on an XBox 360 console, you must first configure your Embedded NGX appliance to use the "Open NAT" method.

SYNTAX

When used with `set`:

set smartdefense ai games xbox-live open-nat *open-nat*

When used with `show`:

show smartdefense ai games xbox-live [open-nat]

FIELDS

`open-nat`	String. Indicates whether the Embedded NGX appliance should use the "Open NAT" method. This field can have the following values: • `enabled` - Use the "Open NAT" method. You will be able to host XBox LIVE games and join existing ones. • `disabled` - Do not use the "Open NAT" method. You will not be able to host XBox LIVE games, but you will still be able to join existing ones. The default value is `disabled`.

EXAMPLE 1

The following command enables host XBox LIVE games and join existing ones:

```
set smartdefense ai games xbox-live open-nat enabled
```

EXAMPLE 2

The following command displays all XBox LIVE settings:

```
show smartdefense ai games xbox-live
```

smartdefense ai http header-rejection

PURPOSE

The `smartdefense ai http header-rejection` variable is used for working with HTTP header settings in the following ways:

- Configuring HTTP header settings
- Displaying and exporting HTTP header settings, including header patterns

  For information on configuring, displaying, and exporting specific header pattern settings, see ***smartdefense ai http header-rejection patterns*** on page 570.

Some exploits are carried in standard HTTP headers with custom values (for example, in the Host header), or in custom HTTP headers. You can protect against such exploits by rejecting HTTP requests that contain specific headers and header values.

SYNTAX

When used with `set`:

set smartdefense ai http header-rejection [enforce *enforce*] [log *log*]

When used with `show`:

show smartdefense ai http header-rejection [enforce | log]

FIELDS

`enforce`	String. Indicates whether to enable HTTP header-based exploit blocking. This can have the following values: • `enabled` - HTTP header-based exploit blocking is enabled. • `disabled` - HTTP header-based exploit blocking is disabled. The default value is `disabled`.

`log`	String. Indicates whether to log HTTP header-based exploits. This can have the following values: • `disabled` - Do not log attacks. • `log` - Log attacks. The default value is `disabled`.

EXAMPLE 1

The following command enables HTTP header-based exploit blocking and logging:

```
set smartdefense ai http header-rejection enforce enabled log log
```

EXAMPLE 2

The following command displays all HTTP header-based exploit settings, including header patterns:

```
show smartdefense ai http header-rejection
```

smartdefense ai http header-rejection patterns

PURPOSE

The `smartdefense ai http header-rejection patterns` variable is used for working with HTTP header patterns in the following ways:

- Adding HTTP header patterns
- Modifying HTTP header patterns
- Deleting HTTP header patterns
- Displaying and exporting HTTP header patterns
- Clearing the HTTP Header Patterns table

HTTP header patterns are matched against HTTP headers that the client receives from the Web server. If a match is detected, SmartDefense takes action according to the settings specified in ***smartdefense ai http header-rejection*** on page 568.

You can reset the HTTP header patterns to their defaults. See ***reset smartdefense ai http header-rejection patterns*** on page 55.

SYNTAX

When used with `add`:

add smartdefense ai http header-rejection patterns name *name* active *active* header-name *header-name* header-value *header-value*

When used with `set`:

set smartdefense ai http header-rejection patterns *number* [name *name*] [active *active*] [header-name *header-name*] [header-value *header-value*]

When used with `delete`:

delete smartdefense ai http header-rejection patterns *number*

When used with `show`:

show smartdefense ai http header-rejection patterns [*number*] [name | active | header-name | header-value]

When used with `clear`:

clear smartdefense ai http header-rejection patterns

FIELDS

`number`	Integer. The header pattern's row in the HTTP Header Patterns table.
`name`	String. The HTTP header-based exploit's name.
`active`	String. Indicates whether SmartDefense should check HTTP headers for this pattern. This can have the following values: • `true` - Check headers for this pattern. • `false` - Do not check headers for this pattern.
`header-name`	String. The HTTP header pattern's name.
`header-value`	String. The HTTP header pattern's value.

EXAMPLE 1

The following command adds an HTTP header pattern and activates it:

```
add smartdefense ai http header-rejection patterns name Atwola
active true header-name Host header-value \.atwola\.com
```

EXAMPLE 2

The following command deactivates header pattern 1 in the HTTP Header Patterns table:

```
set smartdefense ai http header-rejection patterns 1 active false
```

EXAMPLE 3

The following command deletes header pattern 1 in the HTTP Header Patterns table:

```
delete smartdefense ai http header-rejection patterns 1
```

EXAMPLE 4

The following command displays all header patterns:

```
show smartdefense ai http header-rejection patterns
```

EXAMPLE 5

The following command clears the HTTP Header Patterns table:

```
clear smartdefense ai http header-rejection patterns
```

smartdefense ai http worm-catcher

PURPOSE

The `smartdefense ai http worm-catcher` variable is used for working with HTTP-based worm settings in the following ways:

- Configuring HTTP-based worm settings
- Displaying and exporting HTTP-based worm settings, including worm patterns.

  For information on configuring, displaying, and exporting specific worm pattern settings, see ***smartdefense ai http worm-catcher patterns*** on page 575.

A worm is a self-replicating malware (malicious software) that propagates by actively sending itself to new machines. Some worms propagate by using security vulnerabilities in the HTTP protocol.

SYNTAX

When used with `set`:

set smartdefense ai http worm-catcher [enforce *enforce*] [log *log*]

When used with `show`:

show smartdefense ai http worm-catcher [enforce | log]

FIELDS

`enforce`	String. Indicates whether to enable HTTP-based worm blocking. This can have the following values: • `enabled` - HTTP-based worm blocking is enabled. • `disabled` - HTTP-based worm blocking is disabled. The default value is `disabled`.

`log`	String. Indicates whether to log HTTP-based worm attacks. This can have the following values: • `disabled` - Do not log attacks. • `log` - Log attacks The default value is `disabled`.

EXAMPLE 1

The following command enables HTTP-based worm blocking and logging:

```
set smartdefense ai http worm-catcher enforce enabled log log
```

EXAMPLE 2

The following command displays all HTTP-based worm settings, including worm patterns:

```
show smartdefense ai http worm-catcher
```

smartdefense ai http worm-catcher patterns

PURPOSE

The `smartdefense ai http worm-catcher patterns` variable is used for working with HTTP-based worm patterns in the following ways:

- Adding worm patterns
- Modifying worm patterns
- Deleting worm patterns
- Displaying and exporting worm patterns
- Clearing the HTTP Worm Patterns table

Worm patterns are matched against HTTP requests that the server receives from the client. If a match is detected, SmartDefense takes action according to the settings specified in ***smartdefense ai http worm-catcher*** on page 573.

You can reset the HTTP worm patterns to their defaults. See ***reset smartdefense ai http worm-catcher patterns*** on page 56.

SYNTAX

When used with `add`:

add smartdefense ai http worm-catcher patterns name *name* active *active* regexp *regexp*

When used with `set`:

set smartdefense ai http worm-catcher patterns *number* [name *name*] [active *active*] [regexp *regexp*]

When used with `delete`:

delete smartdefense ai http worm-catcher patterns *number*

When used with `show`:

show smartdefense ai http worm-catcher patterns [*number*] [name | active | regexp]

When used with `clear`:

clear smartdefense ai http worm-catcher patterns

FIELDS

`number`	Integer. The worm pattern's row in the HTTP Worm Patterns table.
`name`	String. The worm's name.
`active`	String. Indicates whether SmartDefense should check files for this worm pattern. This can have the following values: • `true` - Check files for this worm pattern. • `false` - Do not check files for this worm pattern. The default value is `true`.
`regexp`	String. The worm pattern's regular expression.

EXAMPLE 1

The following command adds a worm pattern and activates it:

```
add smartdefense ai http worm-catcher patterns name Nimda active
true regexp (cmd\.exe)|(root\.exe)
```

EXAMPLE 2

The following command deactivates worm pattern 1 in the HTTP Worm Patterns table:

```
set smartdefense ai http worm-catcher patterns 1 active false
```

EXAMPLE 3

The following command deletes worm pattern 1 in the HTTP Worm Patterns table:

```
delete smartdefense ai http worm-catcher patterns 1
```

EXAMPLE 4

The following command displays all worm patterns:

```
show smartdefense ai http worm-catcher patterns
```

EXAMPLE 5

The following command clears the CFS Worm Patterns table:

```
clear smartdefense ai http worm-catcher patterns
```

smartdefense ai im icq

PURPOSE

The `smartdefense ai im icq` variable is used for working with ICQ instant messenger settings in the following ways:

- Configuring ICQ SmartDefense settings
- Displaying and exporting ICQ SmartDefense settings

SmartDefense can block ICQ connections, by identifying the ICQ application's fingerprints and HTTP headers.

Note: SmartDefense can detect ICQ traffic regardless of the TCP port being used to initiate the session.

SYNTAX

When used with `set`:

set smartdefense ai im icq [enforce *enforce*] [log *log*] [block-proprietary *block-proprietary*] [block-http *block-http*]

When used with `show`:

show smartdefense ai im icq [enforce | log | block-proprietary | block-http]

FIELDS

`enforce`	String. Indicates whether to enable ICQ connection blocking. This can have the following values: • `enabled` - Connection blocking is enabled. • `disabled` - Connection blocking is disabled. The default value is `disabled`.

`log`	String. Indicates whether to log ICQ connections. This can have the following values: • `enabled` - Log connections. • `disabled` - Do not log connections. The default value is `disabled`.
`block-proprietary`	String. Indicates whether to enable blocking proprietary protocols on all ports. This can have the following values: • `enabled` - Block the proprietary protocol on all ports. This in effect prevents all communication using this instant messenger application. • `disabled` - Do not block the proprietary protocol on all ports. The default value is `enabled`.
`block-http`	String. Indicates whether to block using ICQ over HTTP. This can have the following values: • `enabled` - Block using the application over HTTP. • `disabled` - Do not block using the application over HTTP. The default value is `enabled`.

EXAMPLE 1

The following command enables blocking and logging ICQ connections:

```
set smartdefense ai im icq enforce enabled log enabled
```

EXAMPLE 2

The following command displays all ICQ SmartDefense settings:

```
show smartdefense ai im icq
```

smartdefense ai im msn

PURPOSE

The `smartdefense ai im msn` variable is used for working with MSN instant messenger settings in the following ways:

- Configuring MSN SmartDefense settings
- Displaying and exporting MSN SmartDefense settings

SmartDefense can block MSN connections, by identifying the MSN application's fingerprints and HTTP headers.

SYNTAX

When used with `set`:

set smartdefense ai im msn [enforce *enforce*] [log *log*] [block-proprietary *block-proprietary*] [block-http *block-http*]

When used with `show`:

show smartdefense ai im msn [enforce | log | block-proprietary | block-http]

FIELDS

`enforce`

String. Indicates whether to enable MSN connection blocking. This can have the following values:

- `enabled` - Connection blocking is enabled.
- `disabled` - Connection blocking is disabled.

The default value is `disabled`.

`log`

String. Indicates whether to log MSN connections. This can have the following values:

- `enabled` - Log connections.
- `disabled` - Do not log connections.

The default value is `disabled`.

`block-proprietary`	String. Indicates whether to enable blocking proprietary protocols on TCP port 1863. This can have the following values: • `enabled` - Block the proprietary protocol. This in effect prevents all communication using this instant messenger application. • `disabled` - Do not block the proprietary protocol. The default value is `enabled`.
`block-http`	String. Indicates whether to block using MSN over HTTP. This can have the following values: • `enabled` - Block using the application over HTTP. • `disabled` - Do not block using the application over HTTP. The default value is `enabled`.

EXAMPLE 1

The following command enables blocking and logging MSN connections:

```
set smartdefense ai im msn enforce enabled log enabled
```

EXAMPLE 2

The following command displays all MSN SmartDefense settings:

```
show smartdefense ai im msn
```

smartdefense ai im skype

PURPOSE

The `smartdefense ai im skype` variable is used for working with Skype instant messenger settings in the following ways:

- Configuring Skype SmartDefense settings
- Displaying and exporting Skype SmartDefense settings

SmartDefense can block Skype connections, by identifying the Skype application's fingerprints and HTTP headers.

Note: SmartDefense can detect Skype traffic regardless of the TCP port being used to initiate the session.

SYNTAX

When used with `set`:

set smartdefense ai im skype[enforce *enforce*] [log *log*] [block-proprietary *block-proprietary*] [block-http *block-http*]

When used with `show`:

show smartdefense ai im skype [enforce | log | block-proprietary | block-http]

FIELDS

See ***smartdefense ai im icq*** on page 578.

EXAMPLE 1

The following command enables blocking and logging Skype connections:

```
set smartdefense ai im skype enforce enabled log enabled
```

EXAMPLE 2

The following command displays all Skype SmartDefense settings:

```
show smartdefense ai im skype
```

smartdefense ai im yahoo

PURPOSE

The `smartdefense ai im yahoo` variable is used for working with Yahoo instant messenger settings in the following ways:

- Configuring Yahoo SmartDefense settings
- Displaying and exporting Yahoo SmartDefense settings

SmartDefense can block Yahoo connections, by identifying the Yahoo application's fingerprints and HTTP headers.

Note: SmartDefense can detect Yahoo traffic regardless of the TCP port being used to initiate the session.

SYNTAX

When used with `set`:

set smartdefense ai im yahoo [enforce *enforce*] [log *log*] [block-proprietary *block-proprietary*] [block-http *block-http*]

When used with `show`:

show smartdefense ai im yahoo [enforce | log | block-proprietary | block-http]

FIELDS

See ***smartdefense ai im icq*** on page 578.

EXAMPLE 1

The following command enables blocking and logging Yahoo connections:

```
set smartdefense ai im yahoo enforce enabled log enabled
```

EXAMPLE 2

The following command displays all Yahoo SmartDefense settings:

```
show smartdefense ai im yahoo
```

smartdefense ai p2p bittorrent

PURPOSE

The `smartdefense ai p2p bittorrent` variable is used for working with BitTorrent peer-to-peer settings in the following ways:

- Configuring BitTorrent SmartDefense settings
- Displaying and exporting BitTorrent SmartDefense settings

SmartDefense can block BitTorrent traffic, by identifying the proprietary protocols and preventing the initial connection to the BitTorrent networks. This prevents not only downloads, but also search operations.

Note: SmartDefense can detect BitTorrent traffic regardless of the TCP port being used to initiate the session.

SYNTAX

When used with `set`:

set smartdefense ai p2p bittorrent [enforce *enforce*] [log *log*] [block-proprietary *block-proprietary*] [block-http *block-http*]

When used with `show`:

show smartdefense ai p2p bittorrent [enforce | log | block-proprietary | block-http]

FIELDS

`enforce`

String. Indicates whether to enable BitTorrent connection blocking. This can have the following values:

- `enabled` - BitTorrent connection blocking is enabled.
- `disabled` - BitTorrent connection blocking is disabled.

The default value is `disabled`.

`log`	String. Indicates whether to log BitTorrent connections. This can have the following values: • `enabled` - Log BitTorrent connections. • `disabled` - Do not log BitTorrent connections. The default value is `disabled`.
`block-proprietary`	String. Indicates whether to enable blocking proprietary protocols on all ports. This can have the following values: • `enabled` - Proprietary protocol blocking is enabled. This in effect prevents all communication using this instant messenger application. • `disabled` - Proprietary protocol blocking is disabled. The default value is `enabled`.
`block-http`	String. Indicates whether to block using ICQ over HTTP. This can have the following values: • `enabled` - Block using the application over HTTP. • `disabled` - Do not block using the application over HTTP. The default value is `enabled`.

EXAMPLE 1

The following command enables blocking and logging BitTorrent connections:

```
set smartdefense ai p2p bittorrent enforce enabled log enabled
```

EXAMPLE 2

The following command displays all BitTorrent SmartDefense settings:

```
show smartdefense ai p2p bittorrent
```

smartdefense ai p2p emule

PURPOSE

The `smartdefense ai p2p emule` variable is used for working with eMule peer-to-peer settings in the following ways:

- Configuring eMule SmartDefense settings
- Displaying and exporting eMule SmartDefense settings

SmartDefense can block eMule traffic, by identifying the proprietary protocols and preventing the initial connection to the eMule networks. This prevents not only downloads, but also search operations.

Note: SmartDefense can detect eMule traffic regardless of the TCP port being used to initiate the session.

SYNTAX

When used with `set`:

set smartdefense ai p2p emule [enforce *enforce*] [log *log*] [block-proprietary *block-proprietary*]

When used with `show`:

show smartdefense ai p2p emule [enforce | log | block-proprietary]

FIELDS

See ***smartdefense ai p2p bittorrent*** on page 584.

EXAMPLE 1

The following command enables blocking and logging eMule connections:

```
set smartdefense ai p2p emule enforce enabled log enabled
```

EXAMPLE 2

The following command displays all eMule SmartDefense settings:

```
show smartdefense ai p2p emule
```

smartdefense ai p2p gnutella

PURPOSE

The `smartdefense ai p2p gnutella` variable is used for working with Gnutella peer-to-peer settings in the following ways:

- Configuring Gnutella SmartDefense settings
- Displaying and exporting Gnutella SmartDefense settings

SmartDefense can block Gnutella traffic, by identifying the proprietary protocols and preventing the initial connection to the Gnutella networks. This prevents not only downloads, but also search operations.

Note: SmartDefense can detect Gnutella traffic regardless of the TCP port being used to initiate the session.

SYNTAX

When used with `set`:

set smartdefense ai p2p gnutella [enforce *enforce*] [log *log*] [block-proprietary *block-proprietary*] [block-http *block-http*]

When used with `show`:

show smartdefense ai p2p gnutella [enforce | log | block-proprietary | block-http]

FIELDS

See ***smartdefense ai p2p bittorrent*** on page 584.

EXAMPLE 1

The following command enables blocking and logging Gnutella connections:

```
set smartdefense ai p2p gnutella enforce enabled log enabled
```

EXAMPLE 2

The following command displays all Gnutella SmartDefense settings:

```
show smartdefense ai p2p gnutella
```

smartdefense ai p2p kazaa

PURPOSE

The `smartdefense ai p2p kazaa` variable is used for working with KaZaA peer-to-peer settings in the following ways:

- Configuring KaZaA SmartDefense settings
- Displaying and exporting KaZaA SmartDefense settings

SmartDefense can block KaZaA traffic, by identifying the proprietary protocols and preventing the initial connection to the KaZaA networks. This prevents not only downloads, but also search operations.

Note: SmartDefense can detect KaZaA traffic regardless of the TCP port being used to initiate the session.

SYNTAX

When used with `set`:

set smartdefense ai p2p kazaa [enforce *enforce*] [log *log*] [block-proprietary *block-proprietary*] [block-http *block-http*]

When used with `show`:

show smartdefense ai p2p kazaa [enforce | log | block-proprietary | block-http]

FIELDS

See ***smartdefense ai p2p bittorrent*** on page 584.

EXAMPLE 1

The following command enables blocking and logging KaZaA connections:

```
set smartdefense ai p2p kazaa enforce enabled log enabled
```

EXAMPLE 2

The following command displays all KaZaA SmartDefense settings:

```
show smartdefense ai p2p kazaa
```

smartdefense ai p2p winny

PURPOSE

The `smartdefense ai p2p winny` variable is used for working with Winny peer-to-peer settings in the following ways:

- Configuring Winny SmartDefense settings
- Displaying and exporting Winny SmartDefense settings

SmartDefense can block Winny traffic, by identifying the proprietary protocols and preventing the initial connection to the Winny networks. This prevents not only downloads, but also search operations.

Note: SmartDefense can detect Winny traffic regardless of the TCP port being used to initiate the session.

SYNTAX

When used with `set`:

set smartdefense ai p2p winny [enforce *enforce*] [log *log*] [block-proprietary *block-proprietary*]

When used with `show`:

show smartdefense ai p2p winny [enforce | log | block-proprietary]

FIELDS

See ***smartdefense ai p2p bittorrent*** on page 584.

EXAMPLE 1

The following command enables blocking and logging Winny connections:

```
set smartdefense ai p2p winny enforce enabled log enabled
```

EXAMPLE 2

The following command displays all Winny SmartDefense settings:

```
show smartdefense ai p2p winny
```

smartdefense ai routing igmp

PURPOSE

The `smartdefense ai routing igmp` variable is used for working with IGMP SmartDefense settings in the following ways:

- Configuring IGMP SmartDefense settings
- Displaying and exporting IGMP SmartDefense settings

IGMP is used by hosts and routers to dynamically register and discover multicast group membership. Attacks on the IGMP protocol usually target a vulnerability in the multicast routing software/hardware used, by sending specially crafted IGMP packets.

SYNTAX

When used with `set`:

set smartdefense ai routing igmp [enforce *enforce*] [log *log*] [enforce-mcast *enforce-mcast*]

When used with `show`:

show smartdefense ai routing igmp [enforce | log | enforce-mcast]

FIELDS

`enforce`

String. Indicates whether to enable IGMP attack blocking. This can have the following values:

- `enabled` - IGMP attack blocking is enabled.
- `disabled` - IGMP attack blocking is disabled.

The default value is `enabled`.

`log`

String. Indicates whether to log IGMP attacks. This can have the following values:

- `enabled` - Log IGMP attacks.
- `disabled` - Do not log IGMP attacks.

The default value is `enabled`.

`enforce-mcast`	String. Indicates whether to enable blocking IGMP packets that are sent to non-multicast addresses. According to the IGMP specification, IGMP packets must be sent to multicast addresses. Sending IGMP packets to a unicast or broadcast address might constitute and attack; therefore the Embedded NGX appliance blocks such packets. This field can have the following values: • `enabled` - Non-multicast IGMP packet blocking is enabled. All IGMP packets that are sent to non-multicast addresses will be blocked. • `disabled` - Non-multicast IGMP packet blocking is disabled. The default value is `enabled`.

Example 1

The following command enables blocking and logging IGMP attacks:

```
set smartdefense ai routing igmp enforce enabled log enabled
```

EXAMPLE 2

The following command displays IGMP multicast settings:

```
show smartdefense ai routing igmp enforce-mcast
```

smartdefense ai scada modbus

PURPOSE

The `smartdefense ai scada modbus` variable is used for working with Modbus settings in the following ways:

- Configuring Modbus settings
- Displaying and exporting Modbus settings, including Modbus command settings.

  For information on configuring, displaying, and exporting specific Modbus command settings, see ***smartdefense ai scada modbus allowed-functions*** on page 595.

SCADA equipment uses the Modbus/TCP protocol over TCP port 502 for communication. You can configure SmartDefense to scan Modbus/TCP connections, enforce compliance to the Modbus/TCP standard, and limit Modbus/TCP requests to a specified set of functions, devices, and registers.

This command is only relevant for UTM-1 Edge appliances.

SYNTAX

When used with `set`:

set smartdefense ai scada modbus [enforce *enforce*] [log *log*] [verify-protocol *verify-protocol*] [enforce-allowed *enforce-allowed*]

When used with `show`:

show smartdefense ai scada modbus [enforce | log | verify-protocol | enforce-allowed]

FIELDS

`enforce`	String. Indicates whether to enforce enforce global SCADA protection, by blocking SCADA connection attempts that do not match the configured protocol compliance policy and allowed command policy. This can have the following values: • `enabled` - Enforce global SCADA protection. • `disabled` - Do not enforce global SCADA protection. The default value is `disabled`.

`log`

String. Indicates whether to log blocked SCADA connection attempts. This can have the following values:

- `enabled` - Log blocked connections.
- `disabled` - Do not log blocked connections.
- `alert`
- `mail`
- `trap`
- `useralert1`
- `useralert2`
- `useralert3`

The default value is `disabled`.

`verify-protocol`

String. Indicates whether to verify compliance to the Modbus/TCP standard, by selecting one of the following:

- `enabled` - Verify compliance.
- `disabled` - Do not verify compliance.

The default value is `disabled`.

`enforce-allowed`

String. Indicates whether to allow use of certain Modbus commands that are specified using ***smartdefense ai scada modbus allowed-functions*** on page 595. This can have the following values:

- `enabled` - Allow use of specified Modbus commands.
- `disabled` - Do not allow use of specified Modbus commands.

The default value is `disabled`.

EXAMPLE 1

The following command enables global SCADA protection and logging:

```
set smartdefense ai scada modbus enforce enabled log enabled
```

EXAMPLE 2

The following command displays all SCADA settings, including allowed Modbus commands:

```
show smartdefense ai scada modbus
```

smartdefense ai scada modbus allowed-functions

PURPOSE

The `smartdefense ai scada modbus allowed-functions` variable is used for working with allowed Modbus commands in the following ways:

- Adding allowed Modbus commands
- Modifying allowed Modbus commands
- Deleting allowed Modbus commands
- Displaying and exporting allowed Modbus commands
- Clearing the Allowed Modbus Commands table

If you enabled global SCADA protection with the exception of specified Modbus commands, then you must configure the list of allowed Modbus commands.

This command is only relevant for UTM-1 Edge appliances.

SYNTAX

When used with `add`:

add smartdefense ai scada modbus allowed-functions [functions *functions*] [addresses *addresses*] [unit-id *unit-id*] [src *src*] [dest *dest*]

When used with `set`:

set smartdefense ai scada modbus allowed-functions [functions *functions*] [addresses *addresses*] [unit-id *unit-id*] [src *src*] [dest *dest*]

When used with `delete`:

delete smartdefense ai scada modbus allowed-functions *number*

When used with `show`:

show ssmartdefense ai scada modbus allowed-functions [*number*] [functions | addresses | unit-id | src | dest]

When used with `clear`:

clear smartdefense ai scada modbus allowed-functions

FIELDS

`number`
Integer. The command's row in the Allowed Modbus Commands table.

`functions`
String or Integer. The function range that the allowed command must include. This can have the following values:

- An integer between 1 and 255.
- `any` - The command can include any function.

The default value is `any`.

`addresses`
String or Integer. The Modbus memory address range for the command. This can have the following values:

- An integer between 0 and 65535
- `any` - The command can have any memory address range.

The default value is `any`.

This setting is only available through the command line.

`unit-id`
String or Integer. The ID number of the Modbus/TCP unit that the command can access. This can have the following values:

- An integer between 0 and 255
- `any` - The command can access any unit.

The default value is `any`.

`src`	IP Address or String. The source of the connections for which you want to allow this command. This can have the following values: • An IP address • An IP address range - To specify a range, use the following format: `<Start IP Address>-<End IP Address>` • The name of a VPN site • The name of a network object The default value is `any`.
`dst`	IP Address or String. The destination of the connections for which you want to allow this command. This can have the following values: • An IP address • An IP address range - To specify a range, use the following format: `<Start IP Address>-<End IP Address>` • The name of a VPN site • The name of a network object The default value is `any`.

EXAMPLE 1

The following command adds an allowed Modbus command:

```
add smartdefense ai scada modbus allowed-functions functions 1
```

EXAMPLE 2

The following command limits the command 1 in the Allowed Modbus Commands table to a single Modbus/TCP unit:

```
set smartdefense ai scada modbus allowed-functions 1 unti-id 0
```

EXAMPLE 3

The following command deletes commad 1 in the Allowed Modbus Commands table:

```
delete smartdefense ai scada modbus allowed-functions 1
```

EXAMPLE 4

The following command displays all worm patterns:

```
show smartdefense ai scada modbus allowed-functions
```

EXAMPLE 5

The following command clears the Allowed Modbus Commands table:

```
clear smartdefense ai scada modbus allowed-functions
```

smartdefense ai voip h323

PURPOSE

The `smartdefense ai voip h323` variable is used for working with H323 SmartDefense settings in the following ways:

- Configuring H323 SmartDefense settings
- Displaying and exporting H323 SmartDefense settings

H.323 telephony is used by various devices and applications, such as Microsoft Netmeeting. SmartDefense allows you to choose whether to disable or enable the H.323 Application Level Gateway (ALG), which allows firewall and NAT traversal of H.323 calls.

SYNTAX

When used with `set`:

set smartdefense ai voip h323 alg *alg*

When used with `show`:

show smartdefense ai voip h323 [alg]

FIELDS

`alg`	String. Indicates whether to enable peer-to-peer H.323 support. This can have the following values: • `enabled` - Enable peer-to-peer H.323 support. • `disabled` - Disable peer-to-peer H.323 support. The default value is `disabled`.

EXAMPLE 1

The following command enables peer-to-peer H.323 support:

```
set smartdefense ai voip h323 alg enabled
```

EXAMPLE 2

The following command displays H323 settings:

```
show smartdefense ai voip h323
```

smartdefense ai voip sip

PURPOSE

The `smartdefense ai voip sip` variable is used for working with SIP SmartDefense settings in the following ways:

- Configuring SIP SmartDefense settings
- Displaying and exporting SIP SmartDefense settings

The SmartDefense SIP Application Level Gateway (ALG) processes the SIP protocol, allows firewall and NAT traversal, and enables Traffic Shaper to operate on SIP connections.

By default, the SIP ALG checks SIP sessions for RFC compliance. If desired, you can allow non-RFC-compliant SIP connections, so that VoIP devices that initiate non-standard SIP calls can communicate through the firewall. You can also disable the SIP ALG altogether, if it is not needed by your SIP clients, or if it interferes with their operation.

SYNTAX

When used with `set`:

set smartdefense ai voip sip [alg *alg*] [enforce-rfc *enforce-rfc*]

When used with `show`:

show smartdefense ai voip sip [alg | enforce-rfc]

FIELDS

`alg`	String. Indicates whether to enable SIP support. This can have the following values: • `enabled` - Enable SIP support. • `disabled` - Disable SIP support. The default value is `enabled`.

`enforce-rfc`	String. Indicates whether to block non-RFC-compliant SIP packets. This can have the following values: • `enabled` - Block the packets. • `disabled` - No action. The default value is `enabled`.

EXAMPLE 1

The following command enables SIP support:

```
set smartdefense ai voip sip alg enabled
```

EXAMPLE 2

The following command displays SIP settings:

```
show smartdefense ai voip sip
```

smartdefense network-security dos ddos

PURPOSE

The `smartdefense network-security dos land` variable is used for working with DDoS settings in the following ways:

- Configuring DDoS settings
- Displaying and exporting DDoS settings

In a distributed denial-of-service attack (DDoS attack), the attacker directs multiple hosts in a coordinated attack on a victim computer or network. The attacking hosts send large amounts of spurious data to the victim, so that the victim is no longer able to respond to legitimate service requests.

SYNTAX

When used with `set`:

set smartdefense network-security dos ddos [enforce *enforce*] [log *log*]

When used with `show`:

show smartdefense network-security dos ddos [enforce | log]

FIELDS

`enforce`	String. Indicates whether to enable DDoS attack blocking. This can have the following values: • `enabled` - DDoS attack blocking is enabled. • `disabled` - DDoS attack blocking is disabled. The default value is `enabled`.
`log`	String. Indicates whether to log DDoS attacks. This can have the following values: • `enabled` - Log DDoS attacks. • `disabled` - Do not log DDoS attacks. The default value is `enabled`.

EXAMPLE 1

The following command enables blocking and logging DDoS attacks:

```
set smartdefense network-security dos ddos enforce enabled log enabled
```

EXAMPLE 2

The following command displays all DDoS settings:

```
show smartdefense network-security dos ddos
```

smartdefense network-security dos flooding

PURPOSE

The `smartdefense network-security dos flooding` variable is used for working with Non-TCP Flooding settings in the following ways:

- Configuring Non-TCP Flooding settings
- Displaying and exporting Non-TCP Flooding settings

Advanced firewalls maintain state information about connections in a State table. In Non-TCP Flooding attacks, the attacker sends high volumes of non-TCP traffic. Since such traffic is connectionless, the related state information cannot be cleared or reset, and the firewall State table is quickly filled up. This prevents the firewall from accepting new connections and results in a Denial of Service (DoS).

You can protect against Non-TCP Flooding attacks by limiting the percentage of state table capacity used for non-TCP connections.

SYNTAX

When used with `set`:

set smartdefense network-security dos flooding [enforce *enforce*] [log *log*] [percent *percent*]

When used with `show`:

show smartdefense network-security dos flooding [enforce | log | percent]

FIELDS

`enforce`	String. Indicates whether to enable blocking additional non-TCP connections, when the percentage of state table capacity used for non-TCP connections reaches the `percent` threshold. This can have the following values: • `enabled` - Blocking additional non-TCP connection is enabled. • `disabled` - Blocking additional non-TCP connection is disabled. The default value is `disabled`.

`log`	String. Indicates whether to log non-TCP connections that exceed the `percent` threshold. This can have the following values: • `enabled` - Log the connections. • `disabled` - Do not log the connections. The default value is `disabled`.
`percent`	Integer. The maximum percentage of state table capacity allowed for non-TCP connections. The default value is 10.

Example 1

The following command enables blocking and logging non-TCP connections that exceed the 50% of the state table capacity:

```
set smartdefense network-security dos flooding enforce enabled log
enabled percent 50
```

EXAMPLE 2

The following command displays all Non-TCP Flooding settings:

```
show smartdefense network-security dos flooding
```

smartdefense network-security dos land

PURPOSE

The `smartdefense network-security dos land` variable is used for working with LAND settings in the following ways:

- Configuring LAND settings
- Displaying and exporting LAND settings

In a LAND attack, the attacker sends a SYN packet, in which the source address and port are the same as the destination (the victim computer). The victim computer then tries to reply to itself and either reboots or crashes.

SYNTAX

When used with `set`:

set smartdefense network-security dos land [enforce *enforce*] [log *log*]

When used with `show`:

show smartdefense network-security dos land [enforce | log]

FIELDS

`enforce`	String. Indicates whether to enable LAND attack blocking. This can have the following values: • `enabled` - LAND attack blocking is enabled. • `disabled` - LAND attack blocking is disabled. The default value is `enabled`.
`log`	String. Indicates whether to log LAND attacks. This can have the following values: • `enabled` - Log LAND attacks. • `disabled` - Do not log LAND attacks. The default value is `enabled`.

EXAMPLE 1

The following command enables blocking and logging LAND attacks:

```
set smartdefense network-security dos land enforce enabled log enabled
```

EXAMPLE 2

The following command displays all LAND settings:

```
show smartdefense network-security dos land
```

smartdefense network-security dos ping-of-death

PURPOSE

The `smartdefense network-security dos ping-of-death` variable is used for working with Ping of Death settings in the following ways:

- Configuring Ping of Death settings
- Displaying and exporting Ping of Death settings

In a Ping of Death attack, the attacker sends a fragmented PING request that exceeds the maximum IP packet size (64KB). Some operating systems are unable to handle such requests and crash.

SYNTAX

When used with `set`:

set smartdefense network-security dos ping-of-death [enforce *enforce*] [log *log*]

When used with `show`:

show smartdefense network-security dos ping-of-death [enforce | log]

FIELDS

`enforce`	String. Indicates whether to enable Ping of Death attack blocking. This can have the following values: • `enabled` - Ping of Death attack blocking is enabled. • `disabled` - Ping of Death attack blocking is disabled. The default value is `enabled`.
`log`	String. Indicates whether to log Ping of Death attacks. This can have the following values: • `enabled` - Log Ping of Death attacks. • `disabled` - Do not log Ping of Death attacks. The default value is `enabled`.

EXAMPLE 1

The following command enables blocking and logging Ping of Death attacks:

```
set smartdefense network-security dos ping-of-death enforce enabled
log enabled
```

EXAMPLE 2

The following command displays all Ping of Death settings:

```
show smartdefense network-security dos ping-of-death
```

smartdefense network-security dos teardrop

PURPOSE

The `smartdefense network-security dos teardrop` variable is used for working with Teardrop settings in the following ways:

- Configuring Teardrop settings
- Displaying and exporting Teardrop settings

In a Teardrop attack, the attacker sends two IP fragments, the latter entirely contained within the former. This causes some computers to allocate too much memory and crash.

SYNTAX

When used with `set`:

set smartdefense network-security dos teardrop [enforce *enforce*] [log *log*]

When used with `show`:

show smartdefense network-security dos teardrop [enforce | log]

FIELDS

`enforce`	String. Indicates whether to enable Teardrop attack blocking. This can have the following values: • `enabled` - Teardrop attack blocking is enabled. • `disabled` - Teardrop attack blocking is disabled. The default value is `enabled`.
`log`	String. Indicates whether to log Teardrop attacks. This can have the following values: • `enabled` - Log Teardrop attacks. • `disabled` - Do not log Teardrop attacks. The default value is `enabled`.

EXAMPLE 1

The following command enables blocking and logging Teardrop attacks:

```
set smartdefense network-security dos teardrop enforce enabled log
enabled
```

EXAMPLE 2

The following command displays all Teardrop settings:

```
show smartdefense network-security dos teardrop
```

smartdefense network-security ip-icmp checksum

PURPOSE

The `smartdefense network-security ip-icmp checksum` variable is used for working with Checksum Verification settings in the following ways:

- Configuring Checksum Verification settings
- Displaying and exporting Checksum Verification settings

SmartDefense identifies any IP, TCP, or UDP packets with incorrect checksums. You can configure how these packets should be handled.

SYNTAX

When used with `set`:

set smartdefense network-security ip-icmp checksum [enforce *enforce*] [log *log*]

When used with `show`:

show smartdefense network-security ip-icmp checksum [enforce | log]

FIELDS

`enforce`	String. Indicates whether to enable blocking packets with incorrect checksums. This can have the following values: • `enabled` - Blocking is enabled. • `disabled` - Blocking is disabled. The default value is `enabled`.
`log`	String. Indicates whether to log packets with incorrect checksums. This can have the following values: • `enabled` - Log the packets. • `disabled` - Do not log the packets. The default value is `enabled`.

EXAMPLE 1

The following command enables blocking and logging packets with incorrect checksums:

```
set smartdefense network-security ip-icmp checksum enforce enabled log
enabled
```

EXAMPLE 2

The following command displays all Checksum Verification settings:

```
show smartdefense network-security ip-icmp checksum
```

smartdefense network-security ip-icmp cisco-ios

PURPOSE

The `smartdefense network-security ip-icmp cisco-ios` variable is used for working with Cisco IOS DOS settings in the following ways:

- Configuring Cisco IOS DOS settings
- Displaying and exporting Cisco IOS DOS settings

Cisco routers are configured to process and accept Internet Protocol version 4 (IPv4) packets by default. When a Cisco IOS device is sent a specially crafted sequence of IPv4 packets (with protocol type 53 - SWIPE, 55 - IP Mobility, 77 - Sun ND, or 103 - Protocol Independent Multicast - PIM), the router will stop processing inbound traffic on that interface.

Note: You cannot enable CISCO IOS DOS PIM protection when the PIM-SM multicast routing protocol is enabled. For information on disabling the PIM-SM protocol, *see pim-sm* on page *485*.

SYNTAX

When used with `set`:

set smartdefense network-security ip-icmp cisco-ios [enforce *enforce*] [log *log*] [num-hops *num-hops*] [proto-53 *proto-53*] [proto-55 *proto-55*] [proto-77 *proto-77*] [proto-103 *proto-103*]

When used with `show`:

show smartdefense network-security ip-icmp cisco-ios [enforce | log | num-hops | proto-53 | proto-55 | proto-77 | proto-103]

FIELDS

`enforce`

String. Indicates whether to enable Cisco IOS DOS attack blocking. This can have the following values:

- `enabled` - Cisco IOS DOS attack blocking is enabled.
- `disabled` - Cisco IOS DOS attack blocking is disabled.

The default value is `enabled`.

`log`

String. Indicates whether to log Cisco IOS DOS attacks. This can have the following values:

- `enabled` - Log Cisco IOS DOS attacks.
- `disabled` - Do not log Cisco IOS DOS attacks.

The default value is `enabled`.

`num-hops`

Integer. The number of hops from the enforcement module that Cisco routers should be protected.

The default value is 10.

`proto-53`

String. Indicates whether to enable dropping IPv4 packets of the SWIPE - Protocol 53 type. This can have the following values:

- `enabled` - Packet dropping is enabled for this protocol type.
- `disabled` - Packet dropping is disabled for this protocol type.

The default value is `enabled`.

`proto-55`

String. Indicates whether to enable dropping IPv4 packets of the IP Mobility - Protocol 55 type. This can have the following values:

- `enabled` - Packet dropping is enabled for this protocol type.

- `disabled` - Packet dropping is disabled for this protocol type.

The default value is `enabled`.

`proto-77`

String. Indicates whether to enable dropping IPv4 packets of the SUN-ND - Protocol 77 type. This can have the following values:

- `enabled` - Packet dropping is enabled for this protocol type.
- `disabled` - Packet dropping is disabled for this protocol type.

The default value is `enabled`.

`proto-103`

String. Indicates whether to enable dropping IPv4 packets of the PIM - Protocol 103 type. This can have the following values:

- `enabled` - Packet dropping is enabled for this protocol type.
- `disabled` - Packet dropping is disabled for this protocol type.

The default value is `enabled`.

EXAMPLE 1

The following command enables blocking and logging Cisco IOS DOS attacks, as well as dropping PIM - Protocol 103 packets:

```
set smartdefense network-security ip-icmp cisco-ios enforce enabled
log enabled proto-103 enabled
```

EXAMPLE 2

The following command displays all Cisco IOS DOS settings:

```
show smartdefense network-security ip-icmp cisco-ios
```

smartdefense network-security ip-icmp fragments

PURPOSE

The `smartdefense network-security ip-icmp fragments` variable is used for working with IP Fragments settings in the following ways:

- Configuring IP Fragments settings
- Displaying and exporting IP Fragments settings

When an IP packet is too big to be transported by a network link, it is split into several smaller IP packets and transmitted in fragments. To conceal a known attack or exploit, an attacker might imitate this common behavior and break the data section of a single packet into several fragmented packets. Without reassembling the fragments, it is not always possible to detect such an attack. Therefore, the Embedded NGX appliance always reassembles all the fragments of a given IP packet, before inspecting it to make sure there are no attacks or exploits in the packet.

SYNTAX

When used with `set`:

set smartdefense network-security ip-icmp fragments [forbid *forbid*] [max-incomplete *max-incomplete*] [timeout *timeout*] [log *log*]

When used with `show`:

show smartdefense network-security ip-icmp fragments [forbid | max-incomplete | timeout | log]

FIELDS

`forbid`	String. Indicates whether to enable dropping all fragmented packets. This can have the following values: • `enabled` - Fragmented packet dropping is enabled. • `disabled` - Fragmented packet dropping is disabled. The default value is `disabled`. Under normal circumstances, it is recommended to leave this field set to `disabled`. Setting this field to `enabled` may disrupt Internet connectivity, because it does not allow any fragmented packets.
`max-incomplete`	Integer. The maximum number of fragmented packets allowed. Packets exceeding this threshold will be dropped. The default value is 300.
`timeout`	Integer. The number of seconds to wait before discarding incomplete packets. When the Embedded NGX appliance receives packet fragments, it waits for additional fragments to arrive, so that it can reassemble the packet. If no packets arrive within the specified number of seconds, it discards the packet. The default value is 10.
`log`	String. Indicates whether to log IP Fragments attacks. This can have the following values: • `enabled` - Log IP Fragments attacks. • `disabled` - Do not log IP Fragments attacks. The default value is `disabled`.

EXAMPLE 1

The following command enables dropping IP and logging IP fragments:

```
set smartdefense network-security ip-icmp fragments forbid enabled log enabled
```

EXAMPLE 2

The following command displays all IP Fragments settings:

```
show smartdefense network-security ip-icmp fragments
```

smartdefense network-security ip-icmp max-ping-size

PURPOSE

The `smartdefense network-security ip-icmp max-ping-size` variable is used for working with Max Ping Size settings in the following ways:

- Configuring Max Ping Size settings
- Displaying and exporting Max Ping Size settings

PING (ICMP echo request) is a program that uses ICMP protocol to check whether a remote machine is up. A request is sent by the client, and the server responds with a reply echoing the client's data.

An attacker can echo the client with a large amount of data, causing a buffer overflow. You can protect against such attacks by limiting the allowed size for ICMP echo requests.

SYNTAX

When used with `set`:

set smartdefense network-security ip-icmp max-ping-size [enforce *enforce*] [log *log*] [size *size*]

When used with `show`:

show smartdefense network-security ip-icmp max-ping-size [enforce | log | size]

FIELDS

`enforce`	String. Indicates whether to enable blocking ICMP echo responses that exceed the `size` threshold. This can have the following values: • `enabled` - Blocking is enabled. • `disabled` - Blocking is disabled. The default value is `enabled`.

`log`	String. Indicates whether to log ICMP echo responses that exceed the `size` threshold. This can have the following values: • `enabled` - Log the responses. • `disabled` - Do not log the responses. The default value is `enabled`.
`size`	Integer. The maximum data size for ICMP echo response. The default value is 1500.

EXAMPLE 1

The following command enables blocking and logging ICMP echo responses that exceed the size 1400:

```
set smartdefense network-security ip-icmp max-ping-size enforce
enabled log enabled size 1400
```

EXAMPLE 2

The following command displays all Max Ping Size settings:

```
show smartdefense network-security ip-icmp max-ping-size
```

smartdefense network-security ip-icmp net-quota

PURPOSE

The `smartdefense network-security ip-icmp net-quota` variable is used for working with Network Quota settings in the following ways:

- Configuring Network Quota settings
- Displaying and exporting Network Quota settings

An attacker may try to overload a server in your network by establishing a very large number of connections per second. To protect against Denial Of Service (DoS) attacks, Network Quota enforces a limit upon the number of connections per second that are allowed from the same source IP address.

You can configure how connection that exceed that limit should be handled.

SYNTAX

When used with `set`:

set smartdefense network-security ip-icmp net-quota [enforce *enforce*] [log *log*] [max *max*]

When used with `show`:

show smartdefense network-security ip-icmp net-quota [enforce | log | max]

FIELDS

`enforce`	String. Indicates whether to enable blocking all new connections from a specific source, when the number of network connections from the same source reaches the `max` threshold. This can have the following values: • `enabled` - Blocking new connections from the same source is enabled. Existing connections will not be blocked. • `disabled` - Blocking new connections from the same source is disabled. The default value is `enabled`.

`log`	String. Indicates whether to log connections from a specific source that exceed the `max` threshold. This can have the following values: • `enabled` - Log the connections. • `disabled` - Do not log the connections. The default value is `enabled`.
`max`	Integer. The maximum number of network connections allowed per second from the same source IP address. The default value is 100. Set a lower threshold for stronger protection against DoS attacks. Note: Setting this value too low can lead to false alarms.

EXAMPLE 1

The following command enables blocking and logging connections from a specific source that exceeds 150 connections/second:

```
set smartdefense network-security ip-icmp net-quota enforce enabled
log enabled max 150
```

EXAMPLE 2

The following command displays all Network Quota settings:

```
show smartdefense network-security ip-icmp net-quota
```

smartdefense network-security ip-icmp null-payload

PURPOSE

The `smartdefense network-security ip-icmp null-payload` variable is used for working with Null Payload settings in the following ways:

- Configuring Null Payload settings
- Displaying and exporting Null Payload settings

Some worms, such as Sasser, use ICMP echo request packets with null payload to detect potentially vulnerable hosts.

SYNTAX

When used with `set`:

set smartdefense network-security ip-icmp null-payload [enforce *enforce*] [log *log*]

When used with `show`:

show smartdefense network-security ip-icmp null-payload [enforce | log]

FIELDS

`enforce`	String. Indicates whether to enable blocking null payload ping packets. This can have the following values: • `enabled` - Blocking is enabled. • `disabled` - Blocking is disabled. The default value is `enabled`.
`log`	String. Indicates whether to log null payload ping packets. This can have the following values: • `enabled` - Log the packets. • `disabled` - Do not log the packets. The default value is `enabled`.

EXAMPLE 1

The following command enables blocking and logging null payload packets:

```
set smartdefense network-security ip-icmp null-payload enforce enabled
log enabled
```

EXAMPLE 2

The following command displays all Null Payload settings:

```
show smartdefense network-security ip-icmp null-payload
```

smartdefense network-security ip-icmp packet-sanity

PURPOSE

The `smartdefense network-security ip-icmp packet-sanity` variable is used for working with Packet Sanity settings in the following ways:

- Configuring Packet Sanity settings
- Displaying and exporting Packet Sanity settings

Packet Sanity performs several Layer 3 and Layer 4 sanity checks. These include verifying packet size, UDP and TCP header lengths, dropping IP options, and verifying the TCP flags.

SYNTAX

When used with `set`:

set smartdefense network-security ip-icmp packet-sanity [enforce *enforce*] [log *log*] [disable-relaxed-udp-len-verification *disable-relaxed-udp-len-verification*]

When used with `show`:

show smartdefense network-security ip-icmp packet-sanity [enforce | log | disable-relaxed-udp-len-verification]

FIELDS

`enforce`	String. Indicates whether to enable blocking packets that fail a sanity test. This can have the following values: • `enabled` - Blocking is enabled. • `disabled` - Blocking is disabled. The default value is `enabled`.
`log`	String. Indicates whether to log packets that fail a sanity test. This can have the following values: • `enabled` - Log the packets. • `disabled` - Do not log the packets. The default value is `enabled`.

`disable-relaxed-udp-len-verification`

String. Indicates whether the Embedded NGX appliance should relax the UDP length verification sanity check or not.

The UDP length verification sanity check measures the UDP header length and compares it to the UDP header length specified in the UDP header. If the two values differ, the packet may be corrupted.

However, since different applications may measure UDP header length differently, the Embedded NGX appliance relaxes the UDP length verification sanity check by default, performing the check but not dropping offending packets. This is called relaxed UDP length verification.

This field can have the following values:

- `true` - Disable relaxed UDP length verification. The Embedded NGX appliance will drop packets that fail the UDP length verification check.
- `false` - Do not disable relaxed UDP length verification. The Embedded NGX appliance will not drop packets that fail the UDP length verification check.

The default value is `false`.

EXAMPLE 1

The following command enables blocking and logging packets that fail a sanity test:

```
set smartdefense network-security ip-icmp packet-sanity enforce
enabled log enabled
```

EXAMPLE 2

The following command displays all Packet Sanity settings:

```
show smartdefense network-security ip-icmp packet-sanity
```

smartdefense network-security ip-icmp welchia

PURPOSE

The `smartdefense network-security ip-icmp welchia` variable is used for working with Welchia worm settings in the following ways:

- Configuring Welchia worm settings
- Displaying and exporting Welchia worm settings

The Welchia worm uses the MS DCOM vulnerability or a WebDAV vulnerability. After infecting a computer, the worm begins searching for other live computers to infect. It does so by sending a specific ping packet to a target and waiting for the reply that signals that the target is alive. This flood of pings may disrupt network connectivity.

SYNTAX

When used with `set`:

set smartdefense network-security ip-icmp welchia [enforce *enforce*] [log *log*]

When used with `show`:

show smartdefense network-security ip-icmp welchia [enforce | log]

FIELDS

`enforce`

String. Indicates whether to enable blocking Welchia worm attacks. This can have the following values:

- `enabled` - Blocking Welchia worm attacks is enabled.
- `disabled` - Blocking Welchia worm attacks is disabled.

The default value is `enabled`.

`log`

String. Indicates whether to log Welchia worm attacks. This can have the following values:

- `enabled` - Log the attack.
- `disabled` - Do not log the attack.

The default value is `enabled`.

EXAMPLE 1

The following command enables blocking and logging Welchia worm attacks:

```
set smartdefense network-security ip-icmp welchia enforce enabled log
enabled
```

EXAMPLE 2

The following command displays all Welchia worm settings:

```
show smartdefense network-security ip-icmp welchia
```

smartdefense network-security port-scan host-port-scan

PURPOSE

The `smartdefense network-security port-scan host-port-scan` variable is used for working with Host Port Scan settings in the following ways:

- Configuring Host Port Scan settings
- Displaying and exporting Host Port Scan settings

An attacker can perform a port scan to determine whether ports are open and vulnerable to an attack. This is most commonly done by attempting to access a port and waiting for a response. The response indicates whether or not the port is open. In a Host Port Scan, the attacker scans a specific host's ports to determine which of the ports are open.

SYNTAX

When used with `set`:

set smartdefense network-security port-scan host-port-scan [num *num*] [period *period*] [external-only *external-only*] [log *log*]

When used with `show`:

show smartdefense network-security port-scan host-port-scan [num | period | external-only | log]

FIELDS

num

Integer. The minimum number of ports that must be accessed within the `period` period, in order for SmartDefense to detect the activity as a port scan.

SmartDefense detects ports scans by measuring the number of ports accessed over a period of time. The number of ports accessed must exceed the `num` value, within the number of seconds specified by the `period` value, in order for SmartDefense to consider the activity a scan.

For example, if this field is set to 30, and 40 ports are accessed within a specified period of time, SmartDefense will detect the activity as a port scan.

The default value is 30.

period

Integer. The maximum number of seconds that can elapse, during which the `num` threshold is exceeded, in order for SmartDefense to detect the activity as a port scan.

SmartDefense detects ports scans by measuring the number of ports accessed over a period of time. The number of ports accessed must exceed the `num` value, within the number of seconds specified by the `period` value, in order for SmartDefense to consider the activity a scan.

For example, if this field is set to 20, and the `num` threshold is exceeded for 15 seconds, SmartDefense will detect the activity as a port scan. If the threshold is exceeded for 30 seconds, SmartDefense will not detect the activity as a port scan.

The default value is 20 seconds.

`external-only`	String. Indicates whether to detect only scans originating from the Internet. This can have the following values: • `true` - Detect only scans from the Internet. • `false` - Do not detect only scans from the Internet. The default value is `false.`
`log`	String. Indicates whether to issue logs for scans. This can have the following values: • `enabled` - Log the scan. • `disabled` - Do not log the scan. The default value is `disabled`.

EXAMPLE 1

The following command configures SmartDefense to detect the accessing of 30 or more ports within a period of up to 20 seconds as a Host Port Scan:

```
set smartdefense network-security port-scan host-port-scan num 30
period 20
```

EXAMPLE 2

The following command displays all Host Port Scan settings:

```
show smartdefense network-security port-scan host-port-scan
```

smartdefense network-security port-scan ip-sweep-scan

PURPOSE

The `smartdefense network-security port-scan ip-sweep-scan` variable is used for working with Sweep Scan settings in the following ways:

- Configuring Sweep Scan settings
- Displaying and exporting Sweep Scan settings

An attacker can perform a port scan to determine whether ports are open and vulnerable to an attack. This is most commonly done by attempting to access a port and waiting for a response. The response indicates whether or not the port is open. In a Sweep Scan, the attacker scans a specific host's ports to determine which of the ports are open.

SYNTAX

When used with `set`:

set smartdefense network-security port-scan ip-sweep-scan [num *num*] [period *period*] [external-only *external-only*] [log *log*]

When used with `show`:

show smartdefense network-security port-scan ip-sweep-scan [num | period | external-only | log]

FIELDS

num

Integer. The minimum number of ports that must be accessed within the `period` period, in order for SmartDefense to detect the activity as a port scan.

SmartDefense detects ports scans by measuring the number of ports accessed over a period of time. The number of ports accessed must exceed the `num` value, within the number of seconds specified by the `period` value, in order for SmartDefense to consider the activity a scan.

For example, if this field is set to 30, and 40 ports are accessed within a specified period of time, SmartDefense will detect the activity as a port scan.

The default value is 50.

period

Integer. The maximum number of seconds that can elapse, during which the `num` threshold is exceeded, in order for SmartDefense to detect the activity as a port scan.

SmartDefense detects ports scans by measuring the number of ports accessed over a period of time. The number of ports accessed must exceed the `num` value, within the number of seconds specified by the `period` value, in order for SmartDefense to consider the activity a scan.

For example, if this field is set to 20, and the `num` threshold is exceeded for 15 seconds, SmartDefense will detect the activity as a port scan. If the threshold is exceeded for 30 seconds, SmartDefense will not detect the activity as a port scan.

The default value is 20 seconds.

`external-only`	String. Indicates whether to detect only scans originating from the Internet. This can have the following values: • `true` - Detect only scans from the Internet. • `false` - Do not detect only scans from the Internet. The default value is `false.`
`log`	String. Indicates whether to issue logs for scans. This can have the following values: • `enabled` - Log the scan. • `disabled` - Do not log the scan. The default value is `disabled`.

EXAMPLE 1

The following command configures SmartDefense to detect the accessing of 30 or more ports within a period of up to 20 seconds as a Sweep Scan:

```
set smartdefense network-security port-scan ip-sweep-scan num 30
period 20
```

EXAMPLE 2

The following command displays all Sweep Scan settings:

```
show smartdefense network-security port-scan ip-sweep-scan
```

smartdefense network-security tcp flags

PURPOSE

The `smartdefense network-security tcp flags` variable is used for working with TCP Flag settings in the following ways:

- Configuring TCP Flag settings
- Displaying and exporting TCP Flag settings

The URG flag is used to indicate that there is urgent data in the TCP stream, and that the data should be delivered with high priority. Since handling of the URG flag is inconsistent between different operating systems, an attacker can use the URG flag to conceal certain attacks.

You can configure how the URG flag should be handled.

SYNTAX

When used with `set`:

set smartdefense network-security tcp flags urg-flag *urg-flag*

When used with `show`:

show smartdefense network-security tcp flags [urg-flag]

FIELDS

`urg-flag`	String. Indicates whether to clear or allow the URG flag. This can have the following values: • `clear` - Clear the URG flag on all incoming packets. • `allow` - Allow the URG flag. The default value is `clear`.

EXAMPLE 1

The following command allows the URG flag on all incoming packets:

```
set smartdefense network-security tcp flags urg-flag allow
```

EXAMPLE 2

The following command displays all TCP Flag settings:

```
show smartdefense network-security tcp flags
```

smartdefense network-security tcp seq-verifier

PURPOSE

The `smartdefense network-security tcp seq-verifier` variable is used for working with Sequence Verifier settings in the following ways:

- Configuring Sequence Verifier settings
- Displaying and exporting Sequence Verifier settings

The Embedded NGX appliance examines each TCP packet's sequence number and checks whether it matches a TCP connection state. You can configure how the appliance handles packets that match a TCP connection in terms of the TCP session but have incorrect sequence numbers.

SYNTAX

When used with `set`:

set smartdefense network-security tcp seq-verifier [enforce *enforce*] [log *log*]

When used with `show`:

show smartdefense network-security tcp seq-verifier [enforce | log]

FIELDS

`enforce`	String. Indicates whether to enable blocking TCP packets with incorrect sequence numbers. This can have the following values: • `enabled` - Blocking is enabled. • `disabled` - Blocking is disabled. The default value is `disabled`.
`log`	String. Indicates whether to log TCP packets with incorrect sequence numbers. This can have the following values: • `enabled` - Log the packet. • `disabled` - Do not log the packet. The default value is `enabled`.

EXAMPLE 1

The following command enables blocking and logging TCP packets with incorrect sequence numbers:

```
set smartdefense network-security tcp seq-verifier enforce enabled log enabled
```

EXAMPLE 2

The following command displays all Strict TCP settings:

```
show smartdefense network-security tcp seq-verifier
```

smartdefense network-security tcp small-pmtu

PURPOSE

The `smartdefense network-security tcp small-pmtu` variable is used for working with Small PMTU settings in the following ways:

- Configuring Small PMTU settings
- Displaying and exporting Small PMTU settings

Small PMTU (Packet MTU) is a bandwidth attack in which the client fools the server into sending large amounts of data using small packets. Each packet has a large overhead that creates a "bottleneck" on the server.

You can protect against this attack by specifying a minimum packet size for data sent over the Internet.

SYNTAX

When used with `set`:

set smartdefense network-security tcp small-pmtu [enforce *enforce*] [log *log*] [size *size*]

When used with `show`:

show smartdefense network-security tcp small-pmtu [enforce | log | size]

FIELDS

`enforce`

String. Indicates whether to enable blocking packets that are smaller than the `size` threshold. This can have the following values:

- `enabled` - Blocking is enabled.
- `disabled` - Blocking is disabled.

The default value is `disabled`.

`log`	String. Indicates whether to log packets that are smaller than the `size` threshold. This can have the following values: • `enabled` - Log the packet. • `disabled` - Do not log the packet. The default value is `enabled`.
`size`	Integer. The minimum value allowed for the MTU field in IP packets sent by a client. An overly small value will not prevent an attack, while an overly large value might degrade performance and cause legitimate requests to be dropped. The default value is 300.

EXAMPLE 1

The following command enables blocking and logging packets with an MTU value that is smaller than 250:

```
set smartdefense network-security tcp small-pmtu enforce enabled log
enabled size 250
```

EXAMPLE 2

The following command displays all Small PMTU settings:

```
show smartdefense network-security tcp small-pmtu
```

smartdefense network-security tcp strict-tcp

PURPOSE

The `smartdefense network-security tcp strict-tcp` variable is used for working with Strict TCP settings in the following ways:

- Configuring Strict TCP settings
- Displaying and exporting Strict TCP settings

Out-of-state TCP packets are SYN-ACK or data packets that arrive out of order, before the TCP SYN packet.

Note: In normal conditions, out-of-state TCP packets can occur after the Embedded NGX restarts, since connections which were established prior to the reboot are unknown. This is normal and does not indicate an attack.

You can configure how out-of-state TCP packets should be handled.

SYNTAX

When used with `set`:

set smartdefense network-security tcp strict-tcp [enforce *enforce*] [log *log*]

When used with `show`:

show smartdefense network-security tcp strict-tcp [enforce | log]

FIELDS

`enforce`	String. Indicates whether to enable blocking out-of-state TCP packets. This can have the following values: • `enabled` - Blocking is enabled. • `disabled` - Blocking is disabled. The default value is `disabled`.

`log`	String. Indicates whether to log out-of-state TCP packets. This can have the following values: • `enabled` - Log the packet. • `disabled` - Do not log the packet. The default value is `enabled`.

EXAMPLE 1

The following command enables blocking and logging out-of-state TCP packets:

```
set smartdefense network-security tcp strict-tcp enforce enabled log
enabled
```

EXAMPLE 2

The following command displays all Strict TCP settings:

```
show smartdefense network-security tcp strict-tcp
```

smartdefense network-security tcp syndefender

PURPOSE

The `smartdefense network-security tcp syndefender` variable is used for working with SynDefender settings in the following ways:

- Configuring SynDefender settings
- Displaying and exporting SynDefender settings

In a SYN attack, the attacker sends many SYN packets without finishing the three-way handshake. This causes the attacked host to be unable to accept new connections. You can protect against this attack by specifying a maximum amount of time for completing handshakes.

SYNTAX

When used with `set`:

set smartdefense network-security tcp syndefender [enforce *enforce*] [log *log*] [log-mode *log-mode*] [timeout *timeout*] [ext_only *ext_only*]

When used with `show`:

show smartdefense network-security tcp syndefender [enforce | log | log-mode | timeout | ext_only]

FIELDS

`enforce`

String. Indicates whether to enable blocking SYN attacks. This can have the following values:

- `enabled` - Blocking is enabled.
- `disabled` - Blocking is disabled.

A SYN attack is when more than 5 incomplete TCP handshakes are detected within 10 seconds. A handshake is considered incomplete when it exceeds the `timeout` threshold.

The default value is `enabled`.

`log`	String. Indicates whether to issue logs for the events specified by the `log_mode` parameter. This can have the following values: • `enabled` - Log the event. • `disabled` - Do not log the event. The default value is `enabled`.
`log_mode`	String. The logging mode. This can have the following values: • `none` - Do not issue logs. • `attack` - Issue logs for each SYN attack. • `individual` - Issue logs for each incomplete handshake. The default value is `attack`. This field is only relevant if the `log` field is set to `enabled`.
`timeout`	Integer. The maximum amount of time in seconds after which a TCP handshake is considered incomplete. The default value is 10 seconds.
`ext_only`	String. Indicates whether to enable SynDefender for external (WAN) interfaces only. This can have the following values: • `enabled` - Enable SynDefender for external interfaces only. • `disabled` - Enable SynDefender for all the firewall interfaces. The default value is `disabled`.

EXAMPLE 1

The following command enables blocking SYN attacks without logging them:

```
set smartdefense network-security tcp syndefender enforce enabled log
disabled timeout 10
```

EXAMPLE 2

The following command displays all SynDefender settings:

```
show smartdefense network-security tcp syndefender
```

smp

PURPOSE

The `smp` variable is used for doing the following:

- Connecting to a Service Center
- Disconnecting from a Service Center
- Displaying and exporting Service Center connection settings
- Configuring the Software Updates service when the appliance is locally managed

Note: Check with your reseller regarding availability of subscription services, or surf to www.sofaware.com/servicecenters to locate your nearest Service Center.

SYNTAX

When used with `set`:

set smp [server *server*] [gatewayid *gatewayid*] [registrationkey *registrationkey*] [connect *connect*]

When used with `show`:

show smp [server | gatewayid | registrationkey | connect]

FIELDS

`server`	IP Address. The desired Service Center's IP address, as given to you by your system administrator.
`gatewayid`	String. Your gateway ID, as given to you by your service provider.
`registrationkey`	String. Your registration key, as given to you by your service provider.

`connect`	String. Indicates whether your Embedded NGX appliance should connect to the Service Center. This can have the following values: • `enabled` - Connect to the Service Center • `disabled` - Disconnect from the Service Center If you disconnect from the Service Center, the services to which you are subscribed are no longer available on your Embedded NGX appliance.
`softwareupdates`	String. The Software Updates service mode. This can have the following values: • `automatic` - The appliance automatically checks for software updates and installs them without user intervention. • `manual` - Software updates must be checked for manually. • `none` - The Sofaware Updates service is disabled.

EXAMPLE 1

The following command disconnects you from your Service Center:

```
set smp connect disabled
```

EXAMPLE 2

The following displays the gateway ID you are using to connect to the Service Center:

```
show smp gatewayid
```

snmp

PURPOSE

The `snmp` variable is used for working with SNMP in the following ways:

- Enabling and configuring SNMP access to the Embedded NGX Portal
- Displaying and exporting SNMP settings, including SNMP traps

  For information on displaying and exporting specific SNMP trap settings, see ***snmp traps*** on page 654.

Embedded NGX appliance users can monitor the Embedded NGX appliance, using tools that support SNMP (Simple Network Management Protocol). You can enable users can do so via the Internet, by configuring remote SNMP access.

The Embedded NGX appliance supports the following SNMP MIBs:

- SNMPv2-MIB
- RFC1213-MIB
- IF-MIB
- IP-MIB

All SNMP access is read-only.

SYNTAX

When used with `set`:

set snmp [mode *mode*] [iprange *iprange*] [community *community*] [location *location*] [contact *contact*] [port *port*]

When used with `show`:

show snmp [mode | iprange | community | location | contact | port]

FIELDS

mode

String. Indicates from where SNMP access to the Embedded NGX Portal should be granted. This can have the following values:

- `internal` - The internal network only. This disables remote SNMP capability.
- `range` - A particular range of IP addresses. If you choose this mode, you must include the `iprange` field.
- `any` - Any IP address.
- `vpn` - The internal network and your VPN.
- `disabled` - SNMP access is disabled.

The default value is `disabled`.

iprange

IP Address or String. The desired IP address range. This can have the following values:

- An IP address
- An IP address range. To specify a range, use the following format: `<Start IP Address>-<End IP Address>`
- `undefined` - No IP address range is defined.

The default value is `undefined`.

community

String. The name of the SNMP community string.

The SNMP agents use the SNMP community string as a password, when connecting to the Embedded NGX appliance.

The default value is `public`.

location

String. A description of the appliance's location.

This information will be visible to SNMP agents, and is useful for administrative purposes.

`contact`	String. The name of the contact person. This information will be visible to SNMP agents, and is useful for administrative purposes.
`port`	Integer. The port to use for SNMP. The default value is 161.

EXAMPLE 1

The following command enables Embedded NGX users to access the Embedded NGX Portal using SNMP from any IP address:

```
set snmp mode any
```

EXAMPLE 2

The following command displays the IP address or IP address range from which SNMP access is granted:

```
show snmp iprange
```

snmp traps

PURPOSE

The `snmp traps` variable is used for working with SNMP traps in the following ways:

- Enabling and configuring SNMP traps
- Displaying and exporting SNMP traps settings

An SNMP trap is a notification sent from one application to another. The Embedded NGX appliance supports sending traps upon the following events:

- Startup / Shutdown
- SNMP Authentication Failure
- Link Up / Link Down

These settings are only available through the command line.

SYNTAX

When used with `set`:

set snmp traps [mode *mode*] [community *community*] [linkupdown *linkupdown*] [authfail *authfail*] [port *port*] [host *host*] [format *format*]

When used with `show`:

show snmp [mode | community | linkupdown | authfail | port | host | format]

FIELDS

`mode`	String. Indicates whether to enable sending SNMP traps. This can have the following values: • `enable` - Enable sending SNMP traps. SNMP traps will automatically be sent upon startup/shutdown events. • `disable` - Disable sending SNMP traps. The default value is `disable`.

`community`
String. The SNMP community string of the trap receiver.

The default value is `public`.

`linkupdown`
String. Indicates whether to send an SNMP trap on each link up/down event. This can have the following values:

- `enable` - Send an SNMP trap on each link up/down event.
- `disable` - Do not send an SNMP trap on each link up/down event.

The default value is `enable`.

`authfail`
String. Indicates whether to send an SNMP trap on each SNMP authentication failure event. This can have the following values:

- `enable` - Send an SNMP trap on each SNMP authentication failure event.
- `disable` - Do not send an SNMP trap on each SNMP authentication failure event.

The default value is `enable`.

`port`
Integer. The UDP port of the trap receiver.

The default value is 162.

`host`
String. The IP address or DNS name of the SNMP trap receiver agent.

`format`
String. The type of SNMP traps to use. This can have the following values:

- `v1` - SNMPv1 traps
- `v2` - SNMPv2 traps
- `inform` - SNMP INFORM traps

The default value is `v1`.

EXAMPLE 1

The following command enables sending SNMPv1 SNMP traps upon startup/shutdown and SNMP authentication failure events:

```
set snmp traps mode enable authfail enable format v1
```

EXAMPLE 2

The following command displays SNMP trap settings:

```
show snmp traps
```

ssh

PURPOSE

The `ssh` variable is used for working with SSH in the following ways:

- Enabling and configuring SSH access to the Embedded NGX Portal
- Displaying and exporting SSH settings

Embedded NGX appliance users can control the appliance via the command line, using the SSH (Secure Shell) management protocol. You can enable users can do so via the Internet, by configuring remote SSH access. You can also integrate the Embedded NGX appliance with SSH-based management systems.

Note: The Embedded NGX appliance supports SSHv2 clients only.

SYNTAX

When used with `set`:

set ssh [mode *mode*] [iprange *iprange*]

When used with `show`:

show ssh [mode | iprange]

FIELDS

mode

String. Indicates from where SSH access to the Embedded NGX Portal should be granted. This can have the following values:

- `internal` - The internal network only. This disables remote SSH capability.
- `range` - A particular range of IP addresses. If you choose this mode, you must include the `iprange` field.
- `any` - Any IP address.
- `vpn` - The internal network and your VPN.

The default value is `internal`.

Warning: If remote SSH is enabled, your Embedded NGX appliance settings can be changed remotely, so it is especially important to make sure all Embedded NGX appliance users' passwords are difficult to guess.

iprange

IP Address or String. The desired IP address range. This can have the following values:

- An IP address
- An IP address range. To specify a range, use the following format: `<Start IP Address>-<End IP Address>`
- `undefined` - No IP address range is defined.

The default value is `undefined`.

EXAMPLE 1

The following command enables Embedded NGX users to access the Embedded NGX Portal using SSH from any IP address:

```
set ssh mode any
```

EXAMPLE 2

The following command displays the IP address or IP address range from which SSH access is granted:

```
show ssh iprange
```

statistics

PURPOSE

The `statistics` variable is used for working with Traffic Monitor settings in the following ways:

- Configuring Traffic Monitor settings
- Displaying and exporting Traffic Monitor settings

The Traffic Monitor displays traffic rates in kilobits/second. If desired, you can change the interval at which the Embedded NGX appliance should collect traffic data.

SYNTAX

When used with `set`:

set statistics interval *interval*

When used with `show`:

show statistics [interval]

FIELDS

`interval`	Integer. The interval (in seconds) at which the Embedded NGX appliance should collect traffic data. The default value is 18000.

EXAMPLE 1

The following command configures the Embedded NGX appliance to collect traffic data every 2 minutes:

```
set statistics interval 7200
```

EXAMPLE 2

The following command displays the Traffic Monitor settings:

```
show statistics
```

svc-objects

PURPOSE

The `svc-objects` variable is used for working with network service objects in the following ways:

- Adding network objects
- Modifying network object settings
- Deleting network objects
- Displaying and exporting network object settings
- Clearing the Network Objects table

You can add custom services as network service objects. This enables you to configure firewall rules, VStream Antivirus rules, custom NAT rules, and static routes for the services represented by the network service objects.

Defining network service objects can make your policies easier to understand and maintain. When a network service object is modified, the change automatically takes effect in all rules and settings that reference the network service object.

SYNTAX

When used with `add`:

add svc-objects name *name* protocol *protocol* ports *ports*

When used with `set`:

set svc-objects *number* [name *name*] [protocol *protocol*] [ports *ports*]

When used with `delete`:

delete svc-objects *number*

When used with `show`:

show svc-objects *number* [name | protocol | ports]

When used with `clear`:

clear svc-objects

FIELDS

number

Integer. The network service object's row in the Network Service Objects table.

name

String. The network service object's name.

protocol

String or Integer. The network service's IP protocol.

This can have the following values:

- `any` - Any protocol
- `tcp`
- `udp`
- `gre`
- `esp`
- `igmp`
- `ospf`
- `icmp`
- The desired network service's IP protocol number

ports

String. The network service object's ports or port range.

This can have the following values:

- A port number
- A port range - To specify a range, use the following format:
  `<Start Port Number>-<End Port Number>`

Note: You can only define a port range for TCP and UDP protocols.

EXAMPLE 1

The following command adds a network service object called "MyNSO":

```
add svc-objects name MailService protocol tcp ports 110
```

EXAMPLE 2

The following command changes the name of network service object 1 in the Network Service Objects table:

```
set svc-objects 1 name MyService
```

EXAMPLE 3

The following command deletes network service object 1 in the Network Service Objects table:

```
delete svc-objects 1
```

EXAMPLE 4

The following command displays the protocol for network service object 1 in the Network Service Objects table:

```
show svc-objects 1 protocol
```

EXAMPLE 5

The following command deletes all network service objects in the Network Service Objects table:

```
clear svc-objects
```

syslog

PURPOSE

The `syslog` variable is used for working with Embedded NGX appliance Syslog settings in the following ways:

- Configuring Syslog settings
- Displaying and exporting Syslog settings

You can configure the Embedded NGX appliance to send event logs to a Syslog server residing in your internal network or on the Internet. The logs detail the date and the time each event occurred. If the event is a communication attempt that was rejected by the firewall, the event details include the source and destination IP address, the destination port, and the protocol used for the communication attempt (for example, TCP or UDP).

This same information is also available in the Event Log page. However, while the Event Log can display hundreds of logs, a Syslog server can store an unlimited number of logs. Furthermore, Syslog servers can provide useful tools for managing your logs.

Note: Kiwi Syslog Daemon is freeware and can be downloaded from http://www.kiwisyslog.com. For technical support, contact Kiwi Enterprises.

SYNTAX

When used with `set`:

set syslog [**address** *address*] [**port** *port*]

When used with `show`:

show syslog [**address** | **port**]

FIELDS

`address`	IP Address or String. The IP address of the computer that will run the Syslog service (one of your network computers). This can have the following values: • An IP address • `undefined` - No Syslog server is defined. The default value is `undefined`.
`port`	Integer. The port number of the Syslog server. The default value is 514.

EXAMPLE 1

The following command configures the Embedded NGX appliance to send logs to computer 192.168.10.11:

```
set syslog address 192.168.10.11
```

EXAMPLE 2

The following command displays the Syslog server IP address:

```
show syslog address
```

terminal-server

PURPOSE

The `terminal-server` variable is used for working with the Embedded NGX appliance's built-in terminal server in the following ways:

- Configuring the terminal server's mode
- Setting the TCP port to use for terminal server connections
- Displaying and exporting the above terminal server settings
- Displaying and exporting all terminal server settings, including active mode settings.

  For information on configuring, displaying, and exporting specific active mode settings, see ***terminal-server active-mode*** on page 668.

The Embedded NGX appliance includes a built-in terminal server (also called a device server), which allows you to Internet-enable legacy RS-232 serial devices by simply connecting them to the appliance's Serial port; there is no need for hardware modification or additional equipment. By adding IP connectivity to your serial devices, the terminal server enables remote monitoring, diagnostics, and management of the devices.

The terminal server can be used in the following modes:

- Passive Mode. The terminal server accepts connections from an external Telnet client, and relays traffic to and from the appliance's Serial port. This mode allows Telnet clients to remotely access devices attached to the appliance's Serial port.
- Active Mode. The terminal server connects to an external Telnet server, and relays traffic to and from the appliance's Serial port. This mode affords devices attached to the appliance's Serial port permanent access an external Telnet server.

Note: Before configuring the terminal server, you must configure the Serial port for terminal server use. For information, see ***dialup*** on page *310*.

This command is only relevant for models with a built-in terminal server.

SYNTAX

When used with `set`:

set terminal-server [**mode** *mode*] [**port** *port*]

When used with `show`:

set terminal-server [mode | port]

FIELDS

`mode`	String. The terminal server's operation mode. This can have the following values: • `active` • `passive` The default value is `passive`. If this field is set to `active`, you must configure active mode settings. See ***terminal-server active-mode*** on page 668.
`speed`	Integer. The TCP port that the terminal server should use for incoming and outgoing connections between the Serial port and the Internet. The default value is 9200.

EXAMPLE 1

The following command configures the terminal server in active mode:

```
set terminal-server mode active
```

EXAMPLE 2

The following command displays the port used for terminal server connections:

```
show terminal-server port
```

terminal-server active-mode

PURPOSE

The `terminal-server active-mode` variable is used for working with the built-in terminal server's active mode settings in the following ways:

- Specifying servers to which the terminal server should connect
- Displaying and exporting these settings

When in active mode, the terminal server connects to an external Telnet server, and relays traffic to and from the appliance's Serial port.

This command is only relevant for models with a built-in terminal server.

SYNTAX

When used with `set`:

set terminal-server active-mode [host1 *host1*] [host2 *host2*]

When used with `show`:

set terminal-server [host1 | host2]

FIELDS

`host1`	IP Address or String. The IP address or DNS name of the primary Telnet server to which the terminal server should connect.
`host2`	IP Address or String. The IP address or DNS name of the secondary Telnet server to which the terminal server should connect.

EXAMPLE 1

The following command configures the primary Telnet server's IP address:

```
set terminal-server active-mode host1 1.2.3.4
```

EXAMPLE 2

The following command displays the configured Telnet servers' IP addresses or DNS names:

```
show terminal-server active-mode
```

usb modems

PURPOSE

The `usb modems` variable is used for working with USB-based modem settings in the following ways:

- Setting up a USB dialup modem
- Displaying and exporting all USB modem settings, including USB-based cellular modem settings.

  For information on configuring, displaying, and exporting specific USB-based cellular modem settings, see ***usb modems cellular*** on page 674.

You can use a USB-based modem as a primary or secondary Internet connection method. This is useful in locations where broadband Internet access is unavailable. When used as a backup Internet connection, the Embedded NGX appliance automatically dials the modem if the primary Internet connection fails. The modem can be automatically disconnected when not in use.

You can connect up to two USB-based modems to the appliance's USB port.

Note: Before setting up a USB dialup modem, you must connect it to your Embedded NGX appliance's USB port. You can use either a dialup (PSTN/ISDN) or cellular (GPRS/EVDO/3G) modem.

Note: After you have finished setting up the modem, you must configure a Dialup Internet connection.
If you want to use the dialup connection as a backup connection, you must configure a LAN or broadband connection as the primary Internet connection, and configure the Dialup connection as the secondary Internet connection. Refer to the User Guide and to ***net wan2*** on page *430*.

These settings are only relevant for models with USB ports.

For information on setting up an RS232 dialup modem, see ***dialup*** on page 310.

SYNTAX

When used with `set`:

set usb modems *number* [type *type*] [speed *speed*] [dialmode *dialmode*] [incoming-ppp *incoming-ppp*] [custominit *custominit*]

When used with `show`:

set usb modems *number* [type | speed | dialmode | incoming-ppp | custominit]

FIELDS

`number` — Integer. The USB modem's row in the USB Modems table.

Currently one USB modem is supported; therefore , the row number is always 1.

`type` — String. The modem type. This can have the following values:

- `Custom` - A custom modem.
  If the modem type is `Custom`, you must include the `custominitstring` field.
- `Teltonika ModemUSB GPRS`
- `Teltonika ModemUSB/H1.8`
- `Teltonika G10 UM1000`
- `Radicom MB-U`
- `Nokia E60`
- `Huawei E220`
- `Huawei E169`
- `AnyData CDMA EVDO`
- `Novatel Ovation U720`
- `Samsung I607 Blackjack`

Reminder: The values are case-sensitive. To enter a string containing spaces, enclose the string in quotation marks.

`speed` — Integer. The modem's port speed (in bits per second). This can have the following values:

- `9600`
- `19200`
- `38400`
- `57600`
- `115200`

- `230400`

The default value is 57600.

`dialmode`

String. The dial mode the modem uses. This can have the following values:

- tone
- pulse

The default value is `tone`.

`incoming-ppp`

String. Indicates whether the modem should answer incoming PPP calls. This allows accessing the appliance out of band for maintenance purposes, in case the primary Internet connection fails.

This can have the following values:

- `enabled` - The modem will answer incoming PPP calls.
- `disabled` - The modem will not answer incoming PPP calls.

The default value is `disabled`.

The client is assigned an IP address from the OfficeMode network; therefore, the OfficeMode network must be enabled. For information on enabling the OfficeMode network, see ***net officemode*** on page 395.

`custominit`

String. The installation string for the custom modem type.

This information is provided automatically if a standard modem type is used.

EXAMPLE 1

The following command sets up a custom USB modem with a port speed of 57600 bps. The dial mode is tone.

```
set usb modems type custom speed 57600 dialmode tone
```

EXAMPLE 2

The following command displays all USB modem settings:

```
show usb modems
```

usb modems cellular

PURPOSE

The `usb modems cellular` variable is used for working with USB-based cellular modem settings in the following ways:

- Configuring the modem's Personal Identity Number (PIN) and Access Point Name (APN) codes
- Displaying and exporting the modem's PIN and APN codes

These settings are only relevant for models with USB ports.

SYNTAX

When used with `set`:

set usb modems *number* **cellular pin** *pin* **apn** *apn*

When used with `show`:

show usb modems *number* **cellular** [**pin** | **apn**]

FIELDS

`number`	Integer. The USB modem's row in the USB Modems table. Currently one USB modem is supported; therefore , the row number is always 1.
`pin`	String. The Personal Identification Number (PIN) code that you received with your cellular SIM card, if required by your modem. The PIN code is normally 4 digits long. Warning: Entering an incorrect PIN code may cause your SIM card to be blocked.

apn	String. Your Access Point Name (APN) as given by your cellular provider. If your cellular provider has not provided you with an APN, leave this field empty.

EXAMPLE 1

The following command sets the PIN and APN codes for USB modem 1:

```
set usb modems 1 cellular pin 7638 apn “myapn”
```

EXAMPLE 2

The following command displays all USB modem PIN and APN codes:

```
show usb modems 1 cellular
```

usb usbmodem-info

PURPOSE

The `usb usbmodem-info` variable is used for working with USB-based modem settings in the following ways:

- Enabling/disabling the display of 3G cellular modem information in the Embedded NGX Portal
- Displaying and exporting the above setting

By default, the Embedded NGX Portal displays information about attached 3G cellular modems in the Status Monitor and when viewing network statistics. If your modem produces unexpected or unwanted behavior when the feature is enabled, you can disable this feature.

These settings are only relevant for models with USB ports, and they are only available through the command line.

SYNTAX

When used with `set`:

set usb usbmodem-info mode *mode*

When used with `show`:

show usb usbmodem-info [mode]

FIELDS

`mode`	String. Indicates whether to enable the display of 3G cellular modem information in the Embedded NGX Portal. This can have the following values: • `disable` • `enable` The default value is `enable`.

EXAMPLE 1

The following command disables the display of 3G cellular modem information in the Embedded NGX Portal:

```
set usb usbmodem-info mode disable
```

EXAMPLE 2

The following command displays 3G cellular modem information mode:

```
show usb usbmodem-info
```

usb printers

PURPOSE

The `usb printers` variable is used for working with network printers in the following ways:

- Modifying printer port numbers
- Displaying and exporting printer port numbers

Some Embedded NGX models include a built-in print server, enabling you to connect up to four USB-based printers to the appliance and share them across the network. The appliance automatically detects printers as they are plugged in, and they immediately become available for printing.

Usually, no special configuration is required on the Embedded NGX appliance. However, you may sometimes need to change the port number after completing printer setup. For example, you may want to replace a malfunctioning network printer, with another existing network printer, without reconfiguring the client computers. To do this, you must change the replacement printer's port number to the malfunctioning printer's port number, using the `usb printers` variable.

These settings are only relevant for models with USB ports.

SYNTAX

When used with `set`:

set usb printers *number* port *port*

When used with `show`:

show usb printers [*number* [port]]

FIELDS

number	The printer's row in the USB Printers table.
port	Integer. The network printer's TCP port number. Note: Printer port numbers may not overlap, and must be high ports.

EXAMPLE 1

The following command assigns TCP port 9100 to printer 1:

```
set usb printers 1 port 9100
```

EXAMPLE 2

The following command displays all printers and their port numbers:

```
show usb printers
```

users

PURPOSE

The `users` variable is used for working with local users in the following ways:

- Adding Embedded NGX appliance users
- Modifying Embedded NGX appliance users details
- Deleting Embedded NGX appliance users
- Displaying and exporting Embedded NGX appliance users details
- Clearing the Users table

Note: You cannot change the following details for the admin user (user 1):

- Administrator level
- Web Filtering override

Furthermore, you cannot delete this user.

SYNTAX

When used with `add`:

add users name *name* password *password* [adminaccess *adminaccess*] [vpnaccess *vpnaccess*] [filteroverride *filteroverride*] [hotspotaccess *hotspotaccess*] [rdpaccess *rdpaccess*] [users-manager *users-manager*] [networkaccess *networkaccess*] [expire *expire*]

When used with `set`:

set users *number* [name *name*] [password *password*] [adminaccess *adminaccess*] [vpnaccess *vpnaccess*] [filteroverride *filteroverride*] [hotspotaccess *hotspotaccess*] [rdpaccess *rdpaccess*] [users-manager *users-manager*] [networkaccess *networkaccess*] [expire *expire*]

When used with `delete`:

delete users *number*

When used with `show`:

show users [*number*] [adminaccess | vpnaccess | filteroverride | hotspotaccess | users-manager | networkaccess | expire]

When used with `clear`:

clear users

FIELDS

`number`	Integer. The user's row in the Users table.
`name`	String. The user's username.
`password`	String. The user's password. This must be five to 25 characters (letters or numbers).
`adminaccess`	String. The user's level of access to the Embedded NGX Portal. This can have the following values: • `none` - The user cannot access the Embedded NGX Portal. • `readonly` - The user can log on to the Embedded NGX Portal, but cannot modify system settings. • `users-manager` - The user can log on to the Embedded NGX Portal and add, edit, or delete "No Access"-level users. However, the user cannot modify other system settings. • `readwrite` - The user can log on to the Embedded NGX Portal and modify system settings. The default level is `none`.

`vpnaccess`

String. Indicates whether to allow the user to connect to this Embedded NGX appliance using their VPN client. This can have the following values:

- `true` - The user can remotely access your network via VPN.
- `false` - The user cannot remotely access your network via VPN.

This field is only relevant if the Embedded NGX Remote Access VPN Server or internal VPN Server is enabled. See ***vpn externalserver*** on page 727 and ***vpn internalserver*** on page 734.

`filteroverride`

String. Indicates whether to allow the user to override the Web Filtering service and Web rules. This can have the following values:

- `true` - The user can override the Web Filtering service and Web rules.
- `false` - The user cannot override the Web Filtering and Web rules.

For information on enabling the Web Filtering service, see webfilter mode. For information on defining Web rules, see ***webfilter rule*** on page 790.

`hotspotaccess`

String. Indicates whether to allow the user to log on to the My HotSpot page. This can have the following values:

- `true` - The user can log on to the My HotSpot page.
- `false` - The user cannot log on to the My HotSpot page.

This field is only relevant if Secure HotSpot is configured. See ***hotspot*** on page 343.

`rdpaccess`

String. Indicates whether to allow the user to remotely access computers' desktops, using the Remote Desktop feature. This can have the following values:

- `true` - The user can log on to the my.firewall portal, view the Active Computers page, and remotely access computers' desktops.
  Note: The user can perform these actions, even if their level of administrative access (`adminaccess`) is `none`.
- `false` - The user cannot remotely access computers' desktops.

This option is only relevant if Remote Desktop is enabled. See ***remote-desktop*** on page 534.

`users-manager`

String. Indicates whether to allow the user to log in to the Embedded NGX Portal and add, edit, or delete "No Access"-level users, but not modify other system settings. This can have the following values:

- `true` - The user can log in to the Embedded NGX Portal and add, edit, or delete "No Access"-level users.
- `false` - The user cannot log in to the Embedded NGX Portal and add, edit, or delete "No Access"-level users.

`networkaccess`

String. Indicates whether to allow the user to connect to this Embedded NGX appliance via a wireless client or by connecting to the appliance's ports, when the Embedded NGX EAP authenticator is used.

This can have the following values:

- `true` - The user can connect to this Embedded NGX appliance, when the Embedded NGX EAP authenticator is used.
- `false` - The user cannot connect to this Embedded NGX appliance, when the Embedded NGX EAP authenticator is used.

For information on setting up the Embedded NGX EAP authenticator, refer to the User Guide.

`expire`

String. The expiration date and time for the user's account. When the user account expires, it is locked, and the user can no longer log on to the Embedded NGX appliance.

This field can have the following values:

- `never` - The account never expires.
- A specific date and time in the format:
  `MMM DD YYYY hh:mm:ss<meridian>`
  where:
  MMM = month
  DD = day
  YYYY = year
  hh = hours
  mm = minutes
  `ss` = seconds
  `<meridian>` = AM or PM
  For example, "Dec 01 2005 06:16:00PM"

The default value is `never`.

EXAMPLE 1

The following command adds the user JohnSmith, assigns him the password JohnS1, and sets an expiration time.

```
add users name JohnSmith password JohnS1 expire "Dec 01 2005 06:16:00PM"
```

EXAMPLE 2

The following command specifies that user 2 in the Users table may override the Web Filtering service and Web rules:

```
set users 2 filteroverride true
```

EXAMPLE 3

The following command deletes user 2:

```
delete users 2
```

EXAMPLE 4

The following command displays the details for all users:

```
show users
```

EXAMPLE 5

The following command clears the Users table:

```
clear users
```

vlan

PURPOSE

The `vlan` variable is used for working with virtual networks (VLANs) in the following ways:

- Adding a VLAN
- Configuring a VLAN network's settings, including:
  - Hide Network Address Translation (NAT)
  - The VLAN network's default gateway
  - The VLAN network’s internal network range
  - DHCP (Dynamic Host Configuration Protocol) settings
  - High Availability settings
  - Secure HotSpot access
  - The VLAN network's bridge assignment and settings
- Deleting VLAN networks
- Displaying and exporting the above VLAN network settings
- Displaying and exporting all VLAN network settings, including VLAN OSPF, RIP, and wireless connection settings.

  For information on configuring, displaying, and exporting specific VLAN OSPF settings, see ***vlan ospf*** on page 699 and ***vlan ospf authentication*** on page 702. For information on configuring, displaying, and exporting specific VLAN RIP settings, see ***vlan rip*** on page 704 and ***vlan rip authentication*** on page 706. For information on configuring, displaying, and exporting specific wireless connection settings, see ***vlan wireless*** on page 708.
- Clearing the VLAN Networks table

Your Embedded NGX appliance allows you to partition your network into several virtual LAN networks (VLANs). A VLAN is a logical network behind the Embedded NGX appliance. Computers in the same VLAN behave as if they were on the same physical network: traffic flows freely between them, without passing through a firewall. In contrast, traffic between a VLAN and other networks passes through the firewall and is subject to the security policy. By default, traffic from a VLAN to any other internal network (including

other VLANs) is blocked. In this way, defining VLANs can increase security and reduce network congestion.

You can easily customize this behavior by creating firewall user rules. For information on defining rules, see ***fw rules*** on page 322. For information on the default security policy for VLANs, refer to the User Guide.

The Embedded NGX appliance supports the following VLAN types:

- Tag-based

  In tag-based VLAN you use one of the gateway's ports as a 802.1Q VLAN trunk, connecting the appliance to a VLAN-aware switch. Each VLAN behind the trunk is assigned an identifying number called a "VLAN ID", also referred to as a "VLAN tag". All outgoing traffic from a tag-based VLAN contains the VLAN's tag in the packet headers. Incoming traffic to the VLAN must contain the VLAN's tag as well, or the packets are dropped. Tagging ensures that traffic is directed to the correct VLAN.

  For information on setting up one of the appliance's ports as a VLAN trunk, see port.

- Port-based

  Port-based VLAN allows assigning the appliance's LAN ports to VLANs, effectively transforming the appliance's four-port switch into up to four firewall-isolated security zones. You can assign multiple ports to the same VLAN, or each port to a separate VLAN.

  For information on assigning ports to VLAN networks, see port.

- Virtual access point (VAP)

  In wireless Embedded NGX models, you can partition the primary WLAN into wireless VLANs called virtual access points (VAPs). You can use VAPs to grant different permissions to groups of wireless users, by configuring each VAP with the desired security policy and network settings, and then assigning each group of wireless users to the relevant VAP.

  To use VAPs, you must enable the primary WLAN network, and you must configure wireless connection settings for the VAP. For information on enabling the primary WLAN, see ***net wlan*** on page 442. For information on configuring a VAP's wireless connection settings, see ***vlan wireless*** on page 708.

- Wireless Distribution System (WDS) links

  In wireless Embedded NGX models, you can extend the primary WLAN's coverage area, by creating a Wireless Distribution System (WDS). A WDS is a system of access points that communicate with each other wirelessly via WDS links, without any need for a wired backbone. WDS is usually used together with bridge mode to connect the networks behind the access points.

  To use a WDS, you must enable the primary WLAN network, and you must configure wireless connection settings for each WDS link in the WDS. For information on enabling the primary WLAN, see ***net wlan*** on page 442. For information on configuring a WDS link's wireless connection settings, see ***vlan wireless*** on page 708.

In Embedded NGX models with unlimited nodes, you can define up to 32 VLAN networks (port-based, tag-based, VAP, and WDS links combined), while in other models, you can define up to ten VLAN networks. In wireless models, up to three of the VLAN networks can be VAPs, and up to seven of the VLAN networks can be WDS links.

For more information about VLANs, refer to the User Guide.

SYNTAX

When used with `add`:

add vlan name *name* type *type* [mode *mode*] [hidenat *hidenat*] [address *address*] [netmask *netmask*] [dhcpserver *dhcpserver*] [dhcprange *dhcprange*] [dhcprelayip1 *dhcprelayip1*] [dhcprelayip2 *dhcprelayip2*] [virtualip *virtualip*] [hotspot *hotspot*] [tag *tag*] [wds-peer-mac *wds-peer-mac*] [bridge-to *bridge-to*] [bridge-range *bridge-range*] [bridge-stp-priority *bridge-stp-priority*] [bridge-stp-cost *bridge-stp-cost*] [bridge-antispoofing *bridge-antispoofing*]

When used with `set`:

set vlan *number* [name *name*] [type *type*] [mode *mode*] [hidenat *hidenat*] [address *address*] [netmask *netmask*] [dhcpserver *dhcpserver*] [dhcprange *dhcprange*] [dhcprelayip1 *dhcprelayip1*] [dhcprelayip2 *dhcprelayip2*] [virtualip *virtualip*] [hotspot *hotspot*] [tag *tag*] [wds-peer-mac *wds-peer-mac*] [bridge-to *bridge-to*] [bridge-range *bridge-range*] [bridge-stp-priority *bridge-stp-priority*] [bridge-stp-cost *bridge-stp-cost*] [bridge-antispoofing *bridge-antispoofing*]

When used with `delete`:

delete vlan *number*

When used with `show`:

show vlan *number* [name | type | mode | hidenat | address | netmask | dhcpserver | dhcprange | dhcprelayip1 | dhcprelayip2 | virtualip | hotspot | tag | wds-peer-mac | bridge-to | bridge-range | bridge-stp-priority | bridge-stp-cost | bridge-antispoofing]

When used with `clear`:

clear vlan

FIELDS

`number` — Integer. The VLAN network's row in the VLAN table.

`name` — String. The VLAN network's name.

`type` — String. The VLAN network's type. This can have the following values:

- `portbased` - A port-based VLAN.
- `tagbased` - A tag-based VLAN.
- `vap` - A virtual access point (VAP)
- `wds` - A wireless distribution system (WDS) link

`mode` — String. The VLAN network mode. This can have the following values:

- `enabled` - The VLAN network is enabled.
- `disabled` - The VLAN network is disabled.
- `bridged` - The VLAN network is assigned to a bridge.

The default value is `disabled`.

`hidenat`

String. Indicates whether to use Hide NAT.

Hide NAT enables you to share a single public Internet IP address among several computers, by “hiding” the private IP addresses of the internal VLAN computers behind the VLAN network's single Internet IP address.

This field can have the following values:

- `enabled` - Hide NAT is enabled.
- `disabled` - Hide NAT is disabled.

The default value is `enabled`.

Note: If Hide NAT is disabled, you must obtain a range of Internet IP addresses from your ISP. Hide NAT is enabled by default.

Note: Static NAT and Hide NAT can be used together.

`address`

IP Address. The IP address of the VLAN network's default gateway.

The default value is 192.168.200.1.

Note: The VLAN network must not overlap the LAN network.

`netmask`

IP Address. The VLAN network’s internal network range.

`dhcpserver`

String. Indicates whether the Embedded NGX DHCP server is enabled. This can have the following values:

- `enabled` - The Embedded NGX DHCP server is enabled.
- `disabled` - The Embedded NGX DHCP server is disabled.
- `relay` - DHCP relay is enabled.

The default value is `enabled`.

By default, the Embedded NGX appliance operates as a DHCP server. This allows the Embedded NGX appliance to automatically configure all the devices on the VLAN network with their network configuration details.

If you already have a DHCP server in the VLAN's internal network, and you want to use it instead of the Embedded NGX DHCP server, you must disable the Embedded NGX DHCP server, since you cannot have two DHCP servers or relays on the same network segment.

If you want to use a DHCP server on the Internet or via a VPN, instead of the Embedded NGX DHCP server, you can configure DHCP relay. When in DHCP relay mode, the Embedded NGX appliance relays information from the desired DHCP server to the devices on the VLAN network.

`dhcprange`

String. Indicates how the DHCP server should obtain the DHCP address range.

The DHCP address range is the range of IP addresses that the DHCP server can assign to network devices. IP addresses outside of the DHCP address range are reserved for statically addressed computers.

This field can have the following values:

- `automatic` - The Embedded NGX DHCP server automatically sets the DHCP address range.
- A DHCP address range - Relevant only if the Embedded NGX DHCP server is enabled. To specify a range, use the following format: `<Start IP Address>-<End IP Address>`

The default value is `automatic`.

`dhcprelayip1`

IP Address. The IP address of the primary DHCP relay server. This can have the following values:

- An IP address
- `undefined` - No primary DHCP relay server is defined.

The default value is `undefined`.

This field is only relevant if DHCP relay is enabled.

`dhcprelayip2`

IP Address. The IP address of the secondary DHCP relay server. This can have the following values:

- An IP address
- `undefined` - No secondary DHCP relay server is defined.

The default value is `undefined`.

This field is only relevant if DHCP relay is enabled.

`virtualip`

IP Address. The default gateway IP address. This can have the following values:

- An IP address - This can be any unused IP address in the VLAN network, and must be the same for both gateways.
- `undefined` - High Availability is not configured for this network.

The default value is `undefined`.

This field is only relevant if you want to configure High Availability for the VLAN. For more information on High Availability, see ***ha*** on page 335.

`hotspot`

String. Indicates whether to enable Secure HotSpot for the VLAN network. This can have the following values:

- `enabled` - Secure HotSpot is enabled for the VLAN.
- `disabled` - Secure HotSpot is disabled for the VLAN.

The default value is `disabled`.

`tag`

Integer. The VLAN network's VLAN tag.

By default, the appliance assigns a number that is one more than the tag of the last tag-based VLAN defined. For example, if you assigned the tag 9 to the last tag-based VLAN you defined, then by default the new VLAN network's tag will be 10.

This field is only relevant for tag-based VLANs. The default value for all other VLAN types is 0.

`wds-peer-mac`

MAC Address or String. The WLAN MAC address of the access point to which you want to create a WDS link.

This field can have the following values:

- A MAC address
- `undefined` - The MAC address is undefined.

Note: This is the MAC address of the WLAN interface, not the WAN MAC address. To see your access point's WLAN MAC address, in the Embedded NGX Portal, click Reports in the main menu, and then click Wireless.

This field is only relevant for WDS links. The default value for all other VLAN types is `undefined`.

`bridge-to`

String. The bridge to which the VLAN is assigned. This can have the following values:

- `none` - The VLAN is not assigned to a bridge.
- The name of a bridge

The default value is `none`.

`bridge-range`

String. The range of IP addresses that should be allowed on the VLAN network. This can have the following values:

- `undefined` - The no range is defined.
- The name of a bridge

The default value is `undefined`.

Note: When assigning IP addresses to machines in a bridged network segment, the Embedded NGX DHCP server allocates only addresses within the allowed IP address range.

To enable clients to move between bridged networks without changing IP addresses, configure identical IP address ranges for the desired networks, thus allowing the IP addresses to be used on either of the bridged networks.

Note: Configuring overlapping or identical allowed IP address ranges will decrease the effectiveness of anti-spoofing between the bridged networks.

`bridge-stp-priority`	Integer. The port priority of the VLAN network. This field is only relevant if STP is enabled for the bridge. The port's priority is combined with the port's logical number to create the port's ID. The port with the lowest ID is elected as the root port, which forwards frames out of the bridge. The other ports in the bridge calculate the least-cost path to the root port, in order to eliminate loops in the topology and provide fault tolerance. To increase the chance of this port being elected as the root port, select a lower priority. Note: If you select the same priority for all ports, the root port will be elected based on the port's logical number. This must be an integer between 0 and 240, in increments of 16. The default value is 128.
`bridge-stp-cost`	Integer. The port cost of the VLAN network. This field is only relevant if STP is enabled for the bridge. STP uses the available port with the lowest cost to forward frames to the root port. All other ports are blocked. It is recommended to set a lower value for faster links. The default value is 100.

`bridge-antispoofing` String. Indicates whether anti-spoofing is enabled on the bridged VLAN network. This can have the following values:

- `enabled` - Anti-spoofing is enabled for the VLAN. Only IP addresses within the allowed IP range (specified in the `bridge-range` field) can be source IP addresses for packets on this network
- `disabled` - Anti-spoofing is disabled for the VLAN.

The default value is `enabled`.

EXAMPLE 1

The following command adds a tag-based VLAN network called "office". Hide NAT is disabled for this VLAN:

```
add vlan name office type tagbased hidenat disabled
```

EXAMPLE 2

The following command adds a WDS link called "WDS1" and sets the peer MAC address:

```
add vlan name WDS1 type wds wds-peer-mac aa:bb:cc:dd:ee:ff
```

EXAMPLE 3

The following command sets the tag of the first VLAN network in the VLAN Networks table to 10, and disables the DHCP server:

```
set vlan 1 dhcpserver disabled tag 10
```

EXAMPLE 4

The following command assigns the first VLAN network to the "Bridge1" bridge.

```
set vlan 1 mode bridged bridge-to Bridge1
```

EXAMPLE 5

The following command deletes the first VLAN network in the VLAN Networks table:

```
delete vlan 1
```

EXAMPLE 6

The following command displays the DHCP range of the first VLAN in the VLAN Networks table:

```
show vlan 1 dhcprange
```

EXAMPLE 7

The following command clears the VLAN Networks table:

```
clear vlan
```

vlan ospf

PURPOSE

The `vlan ospf` variable is used for working with OSPF (Open Shortest Path First) settings for VLAN networks in the following ways:

- Configuring OSPF settings for the VLAN
- Displaying and exporting OSPF settings for the VLAN, including authentication settings

  For information on configuring, displaying, and exporting specific authentication settings, see ***vlan ospf authentication*** on page 702.

These settings are only relevant if OSPF is enabled. For information, see ***ospf*** on page 470.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set vlan *number* ospf [cost *cost*] [passive-interface *passive-interface*] [hello-interval *hello-interval*] [dead-interval *dead-interval*] [retransmit-interval *retransmit-interval*] [transmit-delay *transmit-delay*]

When used with `show`:

show vlan *number* ospf [cost | passive-interface | hello-interval | dead-interval | retransmit-interval | transmit-delay]

FIELDS

`number`	Integer. The VLAN network's row in the VLAN table.
`cost`	Integer. The cost of sending a packet on the VLAN interface. OSPF routers send a packet to the route that matches the packet's destination and has the lowest cost. The default value is 0.

`passive-interface`	String. Indicates whether to define the VLAN as a passive interface. A passive interface is included in the AS topology, but it does not generate or accept OSPF traffic. This can have the following values: • `enabled` - Define the VLAN as a passive interface. • `disabled` - Do not define the VLAN as a passive interface. The default value is `disabled`.
`hello-interval`	Integer. The interval of time (in seconds) between transmissions of hello packets on this interface. The default value is 10 seconds.
`dead-interval`	Integer. The interval of time (in seconds) after which the OSPF neighbor will be considered "dead", if it does not send hello packets. The default value is 40 seconds.
`retransmit-interval`	Integer. The interval of time (in seconds) after which the gateway will send an LSA to a neighbor, if the neighbor does not respond to the previous transmission. The default value is 5 seconds.
`transmit-delay`	Integer. The amount of time (in seconds) required to transmit an LSA packet. This value is added to the LSA packet's age before transmission. When specifying this value, take into account the interface's transmission and propagation delays. Slower Internet connections will require a higher value. The default value is 1 second.

EXAMPLE 1

The following command sets the OSPF cost for VLAN network 1:

```
set vlan 1 ospf cost 10
```

EXAMPLE 2

The following command displays the OSPF settings for VLAN network 1:

```
show vlan 1 ospf
```

vlan ospf authentication

PURPOSE

The `vlan ospf authentication` variable is used for working with OSPF authentication settings for VLAN networks in the following ways:

- Configuring OSPF authentication settings for the VLAN
- Displaying and exporting OSPF authentication settings for the VLAN

These settings are only relevant if OSPF is enabled. For information, see ***ospf*** on page 470.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set vlan *number* ospf authentication [simple-text-password *simple-text-password*] [md5-key *md5-key*] [md5-password *md5-password*] [mode *mode*]

When used with `show`:

show vlan *number* ospf authentication [simple-text-password | md5-key | md5-password | mode]

FIELDS

`number`	Integer. The VLAN network's row in the VLAN table.
`simple-text-password`	String. The password to use for clear-text authentication. Passwords need not be the identical throughout an OSPF area, but they must be the same for OSPF neighbors.
`md5-key`	Integer. The key ID to use for MD5 authentication.
`md5-password`	String. The password to use for MD5 authentication. Passwords need not be the identical throughout an OSPF area, but they must be the same for OSPF neighbors.

`mode`	String. The authentication scheme to use for OSPF connections. This can have the following values: • `none` - Do not use authentication. • `md5` - Use the MD5 authentication scheme. • `simple-text` - Use the clear-text authentication scheme. The default value is `none`.

EXAMPLE 1

The following command enables MD5 authentication for OSPF connections for VLAN network 1:

```
set vlan 1 ospf authentication md5-key 1 md5-password thepassword mode
md5
```

EXAMPLE 2

The following command displays the OSPF authentication settings for VLAN network 1:

```
show vlan 1 ospf authentication
```

vlan rip

PURPOSE

The `vlan rip` variable is used for working with RIP settings for VLAN networks in the following ways:

- Configuring the RIP settings for the VLAN
- Displaying and exporting RIP settings for the VLAN, including authentication settings

  For information on configuring, displaying, and exporting specific authentication settings, see ***vlan rip authentication*** on page 706.

These settings are only relevant if RIP is enabled. For information, see ***rip*** on page 541.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set vlan *number* rip passive-interface *passive-interface*

When used with `show`:

show vlan *number* rip [passive-interface]

FIELDS

`number`	Integer. The VLAN network's row in the VLAN table.
`passive-interface`	String. Indicates whether to define the VLAN as a passive interface. A passive interface does not generate or accept RIP traffic. This can have the following values: • `enabled` - Define this interface as a passive interface. • `disabled` - Do not define this interface as a passive interface. The default value is `disabled`.

EXAMPLE 1

The following command configures VLAN network 1 as a passive interface for RIP traffic:

```
set vlan 1 rip passive-interface enabled
```

EXAMPLE 2

The following command displays RIP settings for VLAN network 1:

```
show vlan 1 rip
```

vlan rip authentication

PURPOSE

The `vlan rip authentication` variable is used for working with RIP authentication settings for VLAN networks in the following ways:

- Configuring RIP authentication settings for the VLAN
- Displaying and exporting RIP authentication settings for the VLAN

These settings are only relevant if RIP is enabled. For information, see ***rip*** on page 541.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set vlan *number* rip authentication [simple-text-password *simple-text-password*] [md5-key *md5-key*] [md5-password *md5-password*] [mode *mode*]

When used with `show`:

show vlan *number* rip authentication [simple-text-password | md5-key | md5-password | mode]

FIELDS

`number`	Integer. The VLAN network's row in the VLAN table.
`simple-text-password`	String. The password to use for clear-text authentication.
`md5-key`	Integer. The key ID to use for MD5 authentication.
`md5-password`	String. The password to use for MD5 authentication.

`mode`	String. The authentication scheme to use for RIP connections. This can have the following values: • `none` - Do not use authentication. • `md5` - Use the MD5 authentication scheme. • `simple-text` - Use the clear-text authentication scheme. The default value is `none`.

EXAMPLE 1

The following command enables MD5 authentication for RIP connections for VLAN network 1:

```
set vlan 1 rip authentication md5-key 1 md5-password thepassword mode
md5
```

EXAMPLE 2

The following command displays the RIP authentication settings for VLAN network 1:

```
show vlan 1 rip authentication
```

vlan wireless

PURPOSE

The `vlan wireless` variable is used for working with a VAP or WDS link's wireless connection settings in the following ways:

- Configuring the VAP or WDS link's wireless connection settings, including:
  - The network's SSID
  - The security protocol
  - Advanced security settings
- Displaying and exporting the above wireless connection settings
- Displaying and exporting all of the VAP or WDS link's wireless connection settings, including security settings.

  For information on configuring, displaying, and exporting specific WEP settings, see ***vlan wireless wep*** on page 711. For information on configuring, displaying, and exporting specific WPA settings (VAPs only), see ***vlan wireless wpa*** on page 714. For information on configuring, displaying, and exporting specific WPA-Personal settings (VAPs only), see ***vlan wireless wpapsk*** on page 716.

The Embedded NGX appliance enables you to partition the primary WLAN by using virtual access points (VAPs), and to extend the primary WLAN by using wireless distribution system (WDS) links.

For more information, see ***vlan*** on page 686.

Note: In order for the VAP or WDS link's wireless connection settings to take effect, you must do the following:

- Configure the VAP or WDS link's network settings. For information, see ***vlan*** on page 686.
- Enable the primary WLAN. For information, see ***net wlan*** on page 442.
- Configure global wireless connection settings, including the operation mode, security settings, and wireless transmitter settings. For information, see ***wireless*** on page 800.

If you disable the primary WLAN, all VAP and WDS links are automatically disabled.

Note: The access points in a WDS use the same radio channel for the WDS link and for communicating with wireless stations. Therefore, using WDS may have a negative impact on wireless throughput. In this case, it is recommended to use a traditional wired backbone to connect the access points, instead of WDS links.

These settings are only relevant for models supporting a wireless interface.

SYNTAX

When used with `set`:

set vlan *number* wireless [netname *netname*] [hidenetname *hidenetname*] [macfilter *macfilter*] [datarate *datarate*] [fragthreshold *fragthreshold*] [rtsthreshold *rtsthreshold*] [station-to-station *station-to-station*] [beacon-interval *beacon-interval*] [dtim-period *dtim-period*] [xr *xr*] [wmm *wmm*] [security *security*] [wds *wds*]

When used with `show`:

show vlan *number* wireless [netname | hidenetname | macfilter | datarate | fragthreshold | rtsthreshold | station-to-station | beacon-interval | dtim-period | xr | wmm | security | **wds**]

FIELDS

`number`	Integer. The VLAN network's row in the VLAN table.

For additional fields, see ***net wlan wireless*** on page 446.

Note: Both sides of the WDS link must use the same radio channel and security settings.

Note: WDS links support using the WEP security mode or no security. However, the access point can use any supported security protocol to communicate with wireless stations, including the WPA/WPA2 protocols.

EXAMPLE 1

The following command configures wireless settings for VLAN 1, (which is a VAP or WDS link). The SSID is MyGuests, the SSID is hidden, and the security protocol used is WEP.

```
set vlan 1 wireless netname MyGuests hidenetname yes security wep
```

EXAMPLE 2

The following command displays the wireless settings of VLAN 2:

```
show vlan 2 wireless
```

vlan wireless wep

PURPOSE

The `net wlan wireless wep` variable is used for working with a VAP or WDS link's WEP settings in the following ways:

- Configuring WEP keys
- Displaying and exporting WEP keys

These settings are only relevant when the VAP or WDS link is configured to use the WEP security protocol. For information on configuring wireless settings for VAPs and WDS links, see ***vlan wireless*** on page 708.

These settings are only relevant for models supporting a wireless interface.

SYNTAX

When used with `set`:

set vlan *number* wireless wep [defkey *defkey*] [key1 *key1*] [key2 *key2*] [key3 *key3*] [key4 *key4*]

When used with `show`:

show vlan *number* wireless wep [defkey | key1 | key2 | key3 | key4]

FIELDS

number

Integer. The VLAN network's row in the VLAN table.

defkey

Integer. The number of the WEP key to use for transmission. The value must be between 1 and 4.

The default value is 1.

The selected key must be entered in the same key slot (1-4) on the station devices, but the key need not be selected as the transmit key on the stations.

Note: You can use all four keys to receive data.

key1 - key4

String. A WEP key.

The key is composed of hexadecimal characters 0-9 and A-F, and is not case-sensitive.

The key length can be any of the following:

- 64 Bits. The key length is 10 characters.
- 128 Bits. The key length is 26 characters.
- 152 Bits. The key length is 32 characters.

Note: Some wireless card vendors call these lengths 40/104/128, respectively.

For the highest security, choose a long passphrase that is hard to guess.

Note: WEP is generally considered to be insecure, regardless of the selected key length.

EXAMPLE 1

The following command configures WEP settings for VLAN 1, (which is a VAP or WDS link). It defines two WEP keys and specifies that the second WEP key should be used for transmission.

```
set vlan 1 wireless wep defkey 2 key1 4FC0046169 key2 D8462C0BA9
```

EXAMPLE 2

The following command displays the WEP settings for VLAN 2, (which is a VAP or WDS link):

```
show vlan 2 wireless wep
```

vlan wireless wpa

PURPOSE

The `net wlan wireless wpa` variable is used for working with a VAP's WPA settings in the following ways:

- Configuring the WPA settings, including:
  - Restricting access to wireless clients that support WPA2
  - Key management settings
  - Data encryption settings
  - The authentication server to use for authenticating wireless clients
- Displaying and exporting WPA settings

These settings are only relevant when the VAP is configured to use the WPA-Enterprise or WPA-Personal security protocol. For information on VAPs and their configuration, see ***vlan wireless*** on page 708.

These settings are only relevant for models supporting a wireless interface.

SYNTAX

When used with `set`:

set vlan *number* wireless wpa [wpa2only *wpa2only*] [group-key-update-interval *group-key-update-interval*] [master-key-update-interval *master-key-update-interval*] [cipher-suites *cipher-suites*]

When used with `show`:

show vlan *number* wireless wpa [wpa2only | group-key-update-interval | master-key-update-interval | cipher-suites]

FIELDS

number	Integer. The VLAN network's row in the VLAN table.

For more fields, see ***net wlan wireless wpa*** on page 459.

EXAMPLE 1

The following command configures the VLAN 1, (which is a VAP), to allow only wireless station using WPA2 to connect:

```
set vlan 1 wireless wpa wpa2only yes
```

EXAMPLE 2

The following command displays all WPA settings for VLAN 2, (which is a VAP):

```
show vlan 2 wireless wpa
```

vlan wireless wpapsk

PURPOSE

The `vlan wireless wpapsk` variable is used for working with a VAP's WPA-Personal settings in the following ways:

- Configuring the WPA-Personal passphrase
- Displaying and exporting the WPA-Personal passphrase

These settings are only relevant when the VAP is configured to use the WPA-Personal security protocol. For information on VAPs and their configuration, see ***vlan wireless*** on page 708.

These settings are only relevant for models supporting a wireless interface.

SYNTAX

When used with `set`:

set vlan *number* wireless wpapsk passphrase *passphrase*

When used with `show`:

show vlan *number* wireless wpapsk [passphrase]

FIELDS

`number`	Integer. The VLAN network's row in the VLAN table.
`passphrase`	String. The passphrase for accessing the network. This must be between 8 and 63 characters. It can contain spaces and special characters, and is case-sensitive. For the highest security, choose a long passphrase that is hard to guess.

EXAMPLE 1

The following command configures the WPA-Personal passphrase for VLAN 1, (which is a VAP):

```
set vlan 1 wireless wpapsk passphrase D@34462Crf3-4%-ehj
```

EXAMPLE 2

The following command displays the WPA-Personal passphrase for VLAN 2, (which is a VAP):

```
show wlan 2 wireless wpapsk
```

vpn advanced

PURPOSE

The `vpn advanced` variable is used for doing the following:

- Setting the source IP address for all outgoing VPN connections
- Displaying and exporting the above VPN setting, as well as VPN Manual Login settings.

  For information on configuring, displaying, and exporting VPN Manual Login settings, see ***vpn advanced manual-login*** on page 721.

When the gateway initiates an outgoing VPN connection, it automatically selects an IP address to use as the source IP address for the connection. The `vpn advanced` variable enables you to select a fixed IP address to use for all such connections.

This setting is only available through the command line.

SYNTAX

When used with `set`:

set vpn advanced gateway-bind-network *gateway-bind-network* replay-counter-window *replay-counter-window* delay-interval *delay-interval*

When used with `show`:

show vpn advanced [gateway-bind-network]

FIELDS

`gateway-bind-network`

String. The internal network or bridge, whose default gateway IP address should be used as the source IP address for all outgoing VPN connections initiated by this gateway.

This can have the following values:

- `lan` - The LAN network.
- `dmz` - The DMZ network.
- `wlan` - The primary WLAN network.
- The name of a VLAN network
- The name of a bridge
- `automatic` - The source IP address is selected automatically.

The default value is `automatic`.

`replay-counter-window`

Integer. The replay window size in packets.

The default value is 64 packets.

`delay-interval`

Integer. The maximum amount of time (in seconds), that attempts to open a VPN tunnel should be blocked.

The number of VPN tunnels that a firewall can handle is limited; therefore, when multiple, simultaneous attempts are made to open VPN tunnels, the remote firewall may reject some of them. Setting a delay interval prevents this situation.

When a delay interval is set, the firewall will randomly generate a number between 0 and the specified delay interval. This is called the blocking interval, (also measured in seconds). The firewall will block all new attempt to establish the VPN tunnel, for the duration of the blocking interval. A new blocking interval is generated for each new VPN tunnel trying to established.

For example, if the delay interval is set to 60 seconds, the firewall will randomly generate a blocking interval between 0-60 seconds in length, such as 42 seconds. The firewall will block all attempts to establish the VPN tunnel or to reopen it for 42 seconds. Upon each new attempt to bring up a VPN tunnel, the firewall will generate a new blocking interval between 0-60 seconds.

The default value is 0, meaning that no delay interval is defined, and no blocking interval will be generated.

EXAMPLE 1

The following command sets the LAN's default gateway IP address as the source IP address for all outgoing VPN connections:

```
set vpn advanced gateway-bind-network lan
```

EXAMPLE 2

The following command displays the advanced VPN connection settings:

```
show vpn advanced
```

vpn advanced manual-login

PURPOSE

The `vpn advanced manual-login` variable is used for working with VPN Manual Login settings in the following ways:

- Configuring VPN Manual Login settings
- Displaying and exporting VPN Manual Login settings

By default, when you manually log in to a Remote Access VPN Server, only your computer is logged in. This means that when you generate traffic to the VPN site, thereby establishing a VPN tunnel, only your computer can use the tunnel. In order to share the tunnel with other computers in your network, you must log in to the VPN site from those computers, using the same user name and password. If desired, you can change this behavior and specify that upon manual login all computers in your network should be logged in simultaneously and allowed to use the VPN tunnel.

Note: This variable is only relevant for Remote Access VPN Servers configured for Manual Login.

This setting is only available through the command line.

SYNTAX

When used with `set`:

set vpn advanced manual-login domain *domain*

When used with `show`:

show vpn advanced manual-login [domain]

FIELDS

`domain`	String. The computer(s) for which Manual Login is performed. This can have the following values: • `single-client` - Only the computer that establishes the connection is logged in and can use the VPN tunnel. • `full-network` - Once the connection is established, all computers in your network are logged in and can use the VPN tunnel, unless a specific firewall rule prevents VPN access. The default value is `single-client`.

EXAMPLE 1

The following command specifies that the entire network should be logged in, when Manual Login is performed:

```
set vpn advanced manual-login domain full-network
```

EXAMPLE 2

The following command displays the VPN Manual Login settings:

```
show vpn advanced manual-login
```

vpn enterprise-site

PURPOSE

The `vpn enterprise-site` variable is used for doing the following:

- Enabling/disabling the Enterprise VPN site
- Displaying and exporting the Enterprise VPN site settings

If your Embedded NGX appliance is a member of a VPN community, then the first time your Embedded NGX appliance connects to the SofaWare Management Portal (SMP) or Check Point SmartCenter, the Enterprise VPN site is automatically downloaded to your appliance. You can disable this site if needed.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set vpn enterprise-site disabled *disabled*

When used with `show`:

show vpn enterprise-site [disabled]

FIELDS

`disabled`	String. Indicates whether the Enterprise VPN site is disabled. This can have the following values: • `true` - The Enterprise site is disabled. • `false` - The Enterprise site is enabled. The default value is `true`. Note: You can only connect to this site if it is enabled.

EXAMPLE 1

The following command disables the Enterprise VPN site:

```
set vpn enterprise-site disabled true
```

EXAMPLE 2

The following command displays the Enterprise VPN site settings:

```
show vpn enterprise-site
```

vpn epc

PURPOSE

The `vpn epc` variable is used for doing the following:

- Configuring the Embedded NGX Endpoint Connect VPN Server
- Displaying and exporting Embedded NGX Endpoint Connect VPN Server settings

The Endpoint Connect VPN Server must be enabled *in addition* to one or more of the SecuRemote VPN Servers, to allow users to connect from relevant locations using an Endpoint Connect VPN Client. For example, if both the SecuRemote Remote Access VPN Server and the Endpoint Connect VPN Server are enabled, but the SecuRemote Internal VPN Server is *not* enabled, then users will be able to use the Endpoint Connect VPN Client to connect from the Internet but not from your internal networks. For information on enabling the SecuRemote Remote Access VPN Server, see ***vpn externalserver*** on page 727. For information on enabling the SecuRemote Internal VPN Server, see ***vpn internalserver*** on page 734.

Endpoint Connect users are automatically assigned to the OfficeMode network, enabling you to configure special security rules for them. For information on configuring the OfficeMode network, see ***net officemode*** on page 395.

Note: After you have set up the Endpoint Connect VPN Server, you must configure Endpoint Connect VPN Clients on the internal network computers that should be allowed to access your network. For information, refer to the User Guide.

You must also grant VPN access permissions to the users who should be allowed to access your network via VPN. For information, see ***users*** on page 680.

SYNTAX

When used with `set`:

set vpn epc [**mode** *mode*] [**port** *port*]

When used with `show`:

show vpn epc [**mode**] [**port**]

FIELDS

`mode`	String. The Endpoint Connect VPN Server mode. This can have the following values: • `enabled` - The Endpoint Connect VPN Server is enabled. • `disabled` - The Endpoint Connect VPN Server is disabled. The default value is `disabled`. Note: Disabling the Endpoint Connect VPN Server will cause all existing Endpoint Connect VPN tunnels to disconnect.
`port`	Integer. The port on which the Endpoint Connect VPN Server should accept incoming Endpoint Connect connection requests. The default value is TCP port 443.

EXAMPLE 1

The following command enables the Endpoint Connect VPN Server:

```
set vpn epc mode enabled
```

EXAMPLE 2

The following command displays the Endpoint Connect VPN Server settings:

```
show vpn epc
```

vpn externalserver

PURPOSE

The `vpn externalserver` variable is used for doing the following:

- Configuring the Embedded NGX SecuRemote Remote Access VPN Server
- Displaying and exporting Embedded NGX SecuRemote Remote Access VPN Server settings

You can set up your Embedded NGX appliance as a SecuRemote Remote Access VPN Server. This is useful when you want to make your network remotely available to authorized users connecting from the Internet.

Remote access users can connect to the Remote Access VPN Server via Check Point SecureClient/SecuRemote or a via Embedded NGX appliance in Remote Access VPN mode.

Note: The Check Point SecuRemote Remote Access VPN Client can be downloaded for free via the Embedded NGX Portal. For instructions, refer to the User Guide.

Note: After you have set up the VPN Server, you must grant VPN access permissions to the users who should be allowed to access your network via VPN. For information, see ***users*** on page *680*.

Note: SecureClient/SecuRemote supports split tunneling, which means that VPN Clients can connect directly to the Internet, while traffic to and from VPN sites passes through the VPN Server. If you want all Internet traffic to and from a VPN Client to pass through the VPN Server, configure the L2TP VPN Server instead of the SecuRemote VPN Server. For information, see ***vpn l2tp-server*** on page *736*.

SYNTAX

When used with `set`:

set vpn externalserver [**mode** *mode*] [**bypassnat** *bypassnat*] [**bypassfw** *bypassfw*]

When used with `show`:

show vpn externalserver [**mode** | **bypassnat** | **bypassfw**]

FIELDS

`mode`

String. The SecuRemote Remote Access VPN Server mode. This can have the following values:

- `enabled` - The SecuRemote Remote Access VPN Server is enabled.
- `disabled` - The SecuRemote Remote Access VPN Server is disabled.

The default value is `disabled`.

Note: Disabling the SecuRemote Remote Access VPN Server will cause all existing VPN tunnels from the Internet to disconnect.

`bypassnat`

String. Indicates whether to allow authenticated users connecting from the Internet to bypass NAT when connecting to your internal network. This can have the following values:

- `enabled` - Authenticated users connecting from the Internet can bypass NAT.
- `disabled` - Authenticated users connecting from the Internet cannot bypass NAT.

The default value is `disabled`.

`bypassfw`

String. Indicates whether to allow authenticated users to bypass the default firewall policy and access your internal network without restriction. This can have the following values:

- `enabled` - Authenticated users connecting from the Internet can bypass the default firewall policy. User-defined rules will still apply to the authenticated users.
- `disabled` - Authenticated users connecting from the Internet cannot bypass the default firewall policy.

The default value is `disabled`.

Example 1

The following command enables the SecuRemote Remote Access VPN Server and specifies that authenticated users should be allowed to bypass NAT, but not the default firewall policy:

```
set vpn externalserver mode enabled bypassnat enabled bypassfw disabled
```

EXAMPLE 2

The following command displays the SecuRemote Remote Access VPN Server Bypass NAT settings:

```
show vpn externalserver bypassnat
```

vpn internal-encryption-domain

PURPOSE

The `vpn internal-encryption-domain` variable is used for doing the following:

- Setting the VPN internal encryption domain mode
- Displaying and exporting all VPN internal encryption domain settings, including the encryption domain.

  For information on configuring, displaying and exporting the VPN internal encryption domain, see ***vpn internal-encryption-domain ranges*** on page 732.

The *VPN internal encryption domain* is a list of internal IP addresses on the gateway that are permitted to access Site-to-Site VPNs. If a host outside of the VPN internal encryption domain attempts to access a Site-to-Site VPN, the connection will pass unencrypted (provided that such connections are allowed by the security policy), and it will not go through VPN processing. Likewise, encrypted connections from a Site-to-Site VPN to hosts that are not in the internal VPN encryption domain will be denied.

You can specify whether the VPN internal encryption domain should include all internal networks or only specific networks.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set vpn internal-encryption-domain mode *mode*

When used with `show`:

show vpn internal-encryption-domain [mode]

FIELDS

`mode`	String. The VPN internal encryption domain mode. This can have the following values: • `manual` - Only specific internal networks are members of the encryption domain. In this case, you must set the internal encryption domain manually. See ***vpn internal-encryption-domain ranges*** on page 732. • `automatic` - All the internal networks are members of the encryption domain and can access Site-to-Site VPN sites. The default value is `automatic`.

EXAMPLE 1

The following command configures the VPN internal encryption domain to include all internal networks:

```
set vpn internal-encryption-domain mode automatic
```

EXAMPLE 2

The following command displays all VPN encryption domain settings:

```
show vpn internal-encryption-domain
```

vpn internal-encryption-domain ranges

PURPOSE

The `vpn internal-encryption-domain ranges` variable is used for doing the following:

- Adding IP address ranges to the VPN internal encryption domain
- Modifying IP address ranges in the VPN internal encryption domain
- Deleting IP address ranges from the VPN internal encryption domain
- Displaying and exporting the VPN internal encryption domain
- Clearing the VPN Internal Encryption Domain table

When the VPN internal encryption domain mode is set to manual, you must manually set the VPN internal encryption domain to a specific list of IP address ranges. For information on setting the VPN internal encryption domain mode, see ***vpn internal-encryption-domain*** on page 730.

These settings are only available through the command line.

SYNTAX

When used with `add`:

add vpn internal-encryption-domain ranges iprange *iprange*

When used with `set`:

set vpn internal-encryption-domain ranges *number* iprange *iprange*

When used with `delete`:

delete vpn internal-encryption-domain ranges *number*

When used with `show`:

show vpn internal-encryption-domain ranges [*number*] [iprange]

When used with `clear`:

clear vpn internal-encryption-domain ranges

FIELDS

number	Integer. The IP address range's row in the VPN Internal Encryption Domain table.
iprange	IP Address. An IP address range that belongs to the internal encryption domain.

EXAMPLE 1

The following command adds the IP address range “1.2.3.4-1.2.3.255" to the VPN internal encryption domain:

```
add vpn internal-encryption-domain ranges iprange 1.2.3.4-1.2.3.255
```

EXAMPLE 2

The following command modifies the first IP address range in the VPN Internal Encryption Domain table:

```
set vpn internal-encryption-domain ranges 1 iprange 1.2.3.4-4.3.2.255
```

EXAMPLE 3

The following command deletes the first IP address range in the VPN Internal Encryption Domain table:

```
delete vpn internal-encryption-domain ranges 1
```

EXAMPLE 4

The following command displays all VPN encryption domain members:

```
show vpn internal-encryption-domain ranges
```

EXAMPLE 4

The following command clears the VPN Internal Encryption Domain table:

```
clear vpn internal-encryption-domain ranges
```

vpn internalserver

PURPOSE

The `vpn internalserver` variable is used for doing the following:

- Configuring the Embedded NGX SecuRemote Internal VPN Server
- Displaying and exporting Embedded NGX SecuRemote Internal VPN Server settings

You can make your network available to authorized users connecting from your internal networks, by enabling your Embedded NGX appliance's SecuRemote Internal VPN Server. Users can connect to the internal VPN Server via Check Point SecureClient/SecuRemote or a via Embedded NGX appliance in Remote Access VPN mode.

Enabling the VPN Server for users connecting from your internal networks adds a layer of security to such connections. For example, while you could create a firewall rule allowing a specific user on the DMZ to access the LAN, enabling VPN access for the user means that such connections can be encrypted and authenticated. For more information on the SecuRemote Internal VPN Server, refer to the User Guide.

Note: The Check Point SecureClient/SecuRemote Remote Access VPN Client can be downloaded for free via the Embedded NGX Portal. For instructions, refer to the User Guide.

Note: After you have set up the VPN Server, you must grant VPN access permissions to the users who should be allowed to access your network via VPN. For information, see ***users*** on page *680*.

SYNTAX

When used with `set`:

set vpn internalserver [**mode** *mode*] [**bypassfw** *bypassfw*]

When used with `show`:

show vpn internalserver [**mode** | **bypassfw**]

FIELDS

`mode`

String. The SecuRemote Internal VPN Server mode. This can have the following values:

- `enabled` - The Embedded NGX internal VPN Server is enabled.
- `disabled` - The Embedded NGX internal VPN Server is disabled.

The default value is `disabled`.

Note: Disabling the internal VPN Server will cause all existing VPN tunnels from your internal networks to disconnect.

`bypassfw`

String. Indicates whether to allow authenticated users to bypass the default firewall policy and access your internal network without restriction. This can have the following values:

- `enabled` - Authenticated users connecting from the Internet can bypass the default firewall policy. User-defined rules will still apply to the authenticated users.
- `disabled` - Authenticated users connecting from the Internet cannot bypass the default firewall policy.

The default value is `disabled`.

EXAMPLE 1

The following command enables the SecuRemote Internal VPN Server and specifies that authenticated users should be allowed to bypass NAT, but not the default firewall policy:

```
set vpn internalserver mode enabled bypassfw disabled
```

EXAMPLE 2

The following command displays the SecuRemote Internal VPN Server Bypass Firewall settings:

```
show vpn internalserver bypassfw
```

vpn l2tp-server

PURPOSE

The `vpn l2tp-server` variable is used for doing the following:

- Configuring the Embedded NGX L2TP VPN Server
- Displaying and exporting Embedded NGX L2TP VPN Server settings

You can set up your Embedded NGX appliance as an L2TP (Layer 2 Tunneling Protocol) VPN Server. This is useful when you want to make your network available to authorized users who connect from the Internet or from your internal networks using an L2TP client such as the Microsoft L2TP IPSec VPN Client.

L2TP users are automatically assigned to the OfficeMode network, enabling you to configure special security rules for them. For information on configuring the OfficeMode network, see ***net officemode*** on page 395.

Note: After you have set up the L2TP VPN Server, you must configure L2TP VPN Clients on the internal network computers that should be allowed to access your network via L2TP connections. For information, refer to the User Guide.

You must also grant VPN access permissions to the users who should be allowed to access your network via VPN. For information, see ***users*** on page 680.

Note: The L2TP VPN Client does not support split tunneling, meaning that all Internet traffic to and from a VPN Client passes through the VPN Server and is routed to the Internet. If you want to allow clients to connect directly to the Internet, while traffic to and from VPN sites passes through the VPN Server, configure the SecuRemote VPN Servers instead of the L2TP VPN Server. For information, see ***vpn externalserver*** on page *727* and ***vpn internalserver*** on page *734*.

SYNTAX

When used with `set`:

set vpn l2tp-server [**mode** *mode*] [**bypassfw** *bypassfw*] [**shared-secret** *shared-secret*]

When used with `show`:

show vpn l2tp-server [**mode** | **bypassfw** | **shared-secret**]

FIELDS

`mode`

String. The L2TP VPN Server mode. This can have the following values:

- `enabled` - The L2TP VPN Server is enabled.
- `disabled` - The L2TP VPN Server is disabled.

The default value is `disabled`.

Note: Disabling the L2TP VPN Server will cause all existing VPN tunnels from the Internet to disconnect.

`bypassfw`

String. Indicates whether to allow authenticated users to bypass the default firewall policy and access your internal network without restriction. This can have the following values:

- `enabled` - Authenticated users connecting from the Internet can bypass the default firewall policy. User-defined rules will still apply to the authenticated users.
- `disabled` - Authenticated users connecting from the Internet cannot bypass the default firewall policy.

The default value is `disabled`.

`shared-secret`

String. The preshared secret to use for secure communications between the L2TP clients and the VPN Server.

The secret can contain spaces and special characters. It is used to secure L2TP connections for all users.

Note: In addition to entering this secret, each L2TP user will have to authenticate with a username and password. For information on defining users with VPN access permissions, see ***users*** on page 680.

EXAMPLE 1

The following command enables the L2TP VPN Server and specifies that authenticated users should be allowed to bypass the default firewall policy:

```
set vpn l2tp-server mode enabled bypassfw enabled secret mysecret
```

EXAMPLE 2

The following command displays the L2TP VPN Server settings:

```
show vpn l2tp-server
```

vpn pkcs12

PURPOSE

The `vpn pkcs12` variable is used for doing the following:

- Configuring the Embedded NGX appliance's certificate password
- Displaying and exporting this password in encrypted format

This variable is used internally by the restore process, in order to set the Embedded NGX appliance's certificate password before installing the certificate. For information on restoring the Embedded NGX appliance, see ***restore usb*** on page 62.

This setting is only available through the command line.

SYNTAX

When used with `set`:

set vpn pkcs12 password *password*

When used with `show`:

show vpn pkcs12 [password]

FIELDS

`password`	String. The certificate password. This can have the following values: • A password • `""` - The certificate is not password-protected.

EXAMPLE 1

The following command configures the certificate password:

```
set vpn pkcs12 password mysecretpassword
```

EXAMPLE 2

The following command displays the certificate password in encrypted format:

```
show vpn pkcs12
```

vpn sites

PURPOSE

The `vpn sites` variable is used for working with VPN sites in the following ways:

- Adding VPN sites
- Modifying VPN site settings
- Deleting VPN sites
- Displaying and exporting VPN site settings, including OSPF, RIP, and keep-alive settings

  For information on configuring, displaying, and exporting specific VPN site OSPF settings, see ***vpn sites ospf*** on page 755 and ***vpn sites ospf authentication*** on page 758.For information on configuring, displaying, and exporting specific VPN site RIP settings, see ***vpn sites rip*** on page 760 and ***vpn sites rip authentication*** on page 762. For information on configuring, displaying, and exporting specific VPN site keep-alive settings, see ***vpn sites keepalive-settings*** on page 753.
- Clearing the VPN Sites table

For detailed information on VPN sites, refer to the User Guide.

SYNTAX

When used with `add`:

add vpn sites name *name* type *type* gateway *gateway* [gateway2 *gateway2*] [disabled *disabled*] [loginmode *loginmode*] [configmode *configmode*] [authmethod *authmethod*] [bypassnat *bypassnat*] [bypassfw *bypassfw*] [user *user*] [password *password*] [topopass *topopass*] [servicename *servicename*] [net1 *net1*] [netmask1 *netmask1*] [net2 *net2*] [netmask2 *netmask2*] [net3 *net3*] [netmask3 *netmask3*] [usepfs *usepfs*] [phase1ikealgs *phase1ikealgs*] [phase1exptime *phase1exptime*] [phase1dhgroup *phase1dhgroup*] [phase2ikealgs *phase2ikealgs*] [phase2exptime *phase2exptime*] [phase2dhgroup *phase2dhgroup*] [dnsname *dnsname*] [vti-mtu *vti-mtu*] [vtilocalip *vtilocalip*] [vtiremoteip *vtiremoteip*]

When used with `set`:

set vpn sites [*number*] [name *name*] [type *type*] [gateway *gateway*] [gateway2 *gateway2*] [disabled *disabled*] [loginmode *loginmode*] [configmode *configmode*] [authmethod *authmethod*] [bypassnat *bypassnat*] [bypassfw *bypassfw*] [user *user*] [password *password*] [topopass *topopass*] [servicename *servicename*] [net1 *net1*] [netmask1 *netmask1*] [net2 *net2*] [netmask2 *netmask2*] [net3 *net3*] [netmask3 *netmask3*] [usepfs *usepfs*] [phase1ikealgs *phase1ikealgs*] [phase1exptime *phase1exptime*] [phase1dhgroup *phase1dhgroup*] [phase2ikealgs *phase2ikealgs*] [phase2exptime *phase2exptime*] [phase2dhgroup *phase2dhgroup*] [dnsname *dnsname*] [vti-mtu *vti-mtu*] [vtilocalip *vtilocalip*] [vtiremoteip *vtiremoteip*]

When used with `delete`:

delete vpn sites *number*

When used with `show`:

show vpn sites [*number*] [name | type | gateway | gateway2 | disabled | loginmode | configmode | authmethod | bypassnat | bypassfw | user | password | topopass | servicename | net1 | netmask1 | net2 | netmask2 | net3 | netmask3 | usepfs | phase1ikealgs | phase1exptime | phase1dhgroup | phase2ikealgs | phase2exptime | phase2dhgroup | dnsname | vti-mtu | vtilocalip | vtiremoteip]

When used with `clear`:

clear vpn sites

FIELDS

`number`
Integer. The VPN site's row in the VPN Sites table.

`name`
String. The VPN site's name.

You may choose any name.

`type`
String. The type of VPN site to establish. This can have the following values:

- `remoteaccess` - Establishes remote access from your Remote Access VPN Client to a Remote Access VPN Server
- `sitetosite` - Creates a permanent bi-directional connection to another Site-to-Site VPN Gateway.

`gateway`
IP Address. The IP address of the VPN Gateway to which you want to connect, as given to you by the network administrator.

`gateway2`
IP Address or String. The IP address of the VPN site to use if the primary VPN site fails. This field can have the following values:

- An IP address
- `undefined` - No backup VPN site is defined.

The default value is `undefined`.

`disabled`
String. Indicates whether the VPN site is enabled or disabled. This can have the following values:

- `true` - The VPN site is disabled.
- `false` - The VPN site is enabled.

The default value is `false`.

You can only connect to VPN sites that are enabled.

`loginmode`

String. The mode for logging on to the Remote Access VPN site. This can have the following values:

- `manual` - Configures the VPN site for Manual Login.
  Manual Login connects only the computer you are currently logged onto to the VPN site, and only when the appropriate user name and password have been entered.
- `automatic` - Enables the Embedded NGX appliance to log on to the VPN site automatically. You must then include the `user` and `password` fields.
  Automatic Login provides all the computers on your internal network with constant access to the VPN site.

The default value is `manual`.

This field is only relevant for Remote Access VPN sites.

For further information on Automatic and Manual Login, refer to the User Guide.

`configmode`

String. The mode for obtaining the VPN network configuration.

This can have the following values:

- `manual` - Allows you to provide the network configuration manually.
- `automatic` - Obtains the network configuration by downloading it from the VPN site.
  This option will automatically configure your VPN settings, by downloading the network topology definition from the Remote Access VPN Server.
  Note: Downloading the network configuration is only possible if you are connecting to a Check Point VPN-1 or Embedded NGX Site-to-Site VPN Gateway.
- `routealltraffic` - Routes all network traffic through the VPN site.
  For example, if your VPN consists of a central office and a number of remote offices, and the remote offices are only allowed to access Internet resources through the central office, you can choose to route all traffic from the remote offices through the central office.
  Note: You can only configure one VPN site to route all traffic.

- `routebased` - Allows this VPN site to participate in a route-based VPN. Route-based VPNs allow routing connections over VPN tunnels, so that remote VPN sites can participate in dynamic or static routing schemes. This improves network and VPN management efficiency for large networks.
  For constantly changing networks, it is recommended to use a route-based VPN combined with OSPF dynamic routing. This enables you to make frequent changes to the network topology, such as adding an internal network, without having to reconfigure static routes. For information on enabling OSPF, see ***ospf*** on page 470. For information on configuring the VPN site's OSPF settings, see ***vpn sites ospf*** on page 755 and ***vpn sites ospf md5*** on page 758.
  This option is only available for Site-to-Site VPN gateways.

The default value is `manual`.

`authmethod`

String. The VPN authentication mode. This can have the following values:

- `sharedsecret` - Use a shared secret to use for secure communications with the VPN site. This shared secret is a string used to identify the VPN sites to each other. The secret can contain spaces and special characters.
  Shared secret is only supported for Site-to-Site VPN sites.
- `certificate` - Use a certificate for VPN authentication.
  If you select this option, a certificate must have been installed. (Refer to the User Guide for more information about certificates and instructions on how to install a certificate.)
- `secureid` - Use an RSA SecurID token for VPN authentication.
  When authenticating to the VPN site, you must enter a four-digit PIN code and the SecurID passcode shown in your SecurID token's display. The RSA SecurID token generates a new passcode every minute.
  SecurID is only supported in Remote Access manual login mode.

The default value is `sharedsecret.`

`bypassnat`

String. Indicates whether to allow the VPN site to bypass NAT when connecting to your internal network. This can have the following values:

- `enabled` - The VPN site can bypass NAT.
- `disabled` - The VPN site cannot bypass NAT.

The default value is `disabled.`

This field is only relevant for Site-to-Site VPNs.

`bypassfw`

String. Indicates whether to allow the VPN site to bypass the default firewall policy and access your internal network without restriction. This can have the following values:

- `enabled` - The VPN site can bypass the default firewall policy. User-defined rules will still apply to the VPN site.
- `disabled` - The VPN site cannot bypass the default firewall policy.

The default value is `disabled.`

This field is only relevant for Site-to-Site VPNs.

`user`

String. A user name. The value of this field depends on the type of VPN site:

- For Remote Access VPN sites configured for Automatic Login, this is the user name to be used for logging on to the VPN site.
- For Site-to-Site VPNs configured to automatically download the network configuration, this is the topology user.

`password`

String. The password to use for logging on to the VPN site.

This field is only relevant for Remote Access VPNs.

`topopass`

String. The topology user's password.

This field is only relevant for Site-to-Site VPNs configured to automatically download the network configuration.

`net1` through `net3`	IP Address. A destination network address at the VPN site to which you want to connect. This field can have the following values: • A net work address • `undefined` - No network address is defined. The default value is `undefined.` There can be up to three destination network addresses. These fields are only relevant for VPN sites with manually specified network configurations.
`netmask1` through `netmask3`	IP Address. The subnet mask for the destination network address. This field can have the following values: • A subnet mask • `undefined` - No subnet mask is defined. The default value is `undefined.` These fields are only relevant for VPN sites with manually specified network configurations.
`usepfs`	String. Indicates whether to enable Perfect Forward Secrecy (PFS) for the VPN site. This can have the following values: • `true` - Use PFS. • `false` - Do not use PFS. The default value is `false`. This field is only relevant for Site-to-Site VPNs.

`phase1ikealgs`

String. The encryption and integrity algorithm to use for IKE negotiations. This can have the following values:

- `automatic` - The Embedded NGX appliance automatically selects the best security methods supported by the site.
- `des/md5`
- `des/sha1`
- `3des/md5`
- `3des/sha1`
- `aes128/md5`
- `aes128/sha1`
- `aes256/md5`
- `aes256/sha1`

The default value is `automatic`.

`phase1exptime`

Integer. The interval in minutes between IKE Phase-1 key negotiations. This is the *IKE Phase-1 SA lifetime*.

A shorter interval ensures higher security, but impacts heavily on performance. Therefore, it is recommended to keep the SA lifetime around its default value.

The default value is 1440 minutes (one day).

`phase1dhgroup`

String. The Diffie-Hellman group to use for IKE Phase-1:

- `automatic` - The Embedded NGX appliance automatically selects a group.
- `group1`
- `group2`
- `group5`

A group with more bits ensures a stronger key but lowers performance.

The default value is `automatic`.

`phase2ikealgs`

String. The encryption and integrity algorithm to use for VPN traffic. This can have the following values:

- `automatic` - The Embedded NGX appliance automatically selects the best security methods supported by the site.
- `des/md5`
- `des/sha1`
- `3des/md5`
- `3des/sha1`
- `aes128/md5`
- `aes128/sha1`
- `aes256/md5`
- `aes256/sha1`

The default value is `automatic`.

`phase2exptime`

Integer. The interval in seconds between IPSec SA key negotiations. This is the *IKE Phase-2 SA lifetime*.

A shorter interval ensures higher security.

The default value is 3600 seconds (one hour).

`phase2dhgroup`

String. The Diffie-Hellman group to use for IKE Phase-2:

- `automatic` - The Embedded NGX appliance automatically selects a group.
- `group1`
- `group2`
- `group5`

A group with more bits ensures a stronger key but lowers performance.

The default value is `automatic`.

`dnsname`	String. The gateway's DNS name. The Embedded NGX appliance resolves the DNS name to the IP address.
`vti-mtu`	Integer or String. The maximum transmission unit size that can be sent via the virtual tunnel interface (VTI). This can have the following values: • An integer • `automatic` - The maximum transmission unit size is automatically detected for each VTI. The default value is 1500.
`vtilocalip`	IP Address or String. The local virtual tunnel interface (VTI) IP address. This can have the following values: • An IP address • `undefined` - The VTI IP address is not defined. The default value is `undefined.`
`vtiremoteip`	IP Address or String. The VPN peer's VTI IP address. This can have the following values: • An IP address • `undefined` - The VTI IP address is not defined. The default value is `undefined.`

EXAMPLE 1

The following command adds a Remote Access VPN site called "office". The site is enabled.

```
add vpn sites name office type remoteaccess gateway 1.2.3.4 disabled
false
```

EXAMPLE 2

The following command sets the login mode of VPN site 1 in the VPN Sites table to Automatic. This mode requires you to specify the user name and password for logging on to the VPN site.

```
set vpn sites 1 loginmode automatic user JohnS password
```

EXAMPLE 3

The following command deletes VPN site 1:

```
delete vpn sites 1
```

EXAMPLE 4

The following command displays the VPN network configuration mode for VPN site 1:

```
show vpn sites 1 configmode
```

EXAMPLE 5

The following command clears the VPN Sites table:

```
clear vpn sites
```

vpn sites keepalive-settings

PURPOSE

The `vpn sites keepalive-settings` variable is used for working with keep-alive settings for VPN sites in the following ways:

- Configuring keep-alive settings for the VPN site
- Displaying and exporting keep-alive settings for the VPN site

You can configure the Embedded NGX appliance to keep the tunnel to a VPN site alive even if there is no network traffic between the Embedded NGX appliance and the VPN site. The Embedded NGX appliance keeps the tunnel alive by periodically pinging up to three IP addresses at the VPN site.

These settings are only relevant for Site-to-Site VPNs. For information on configuring Site-to-Site VPNs, see ***vpn sites*** on page 740.

SYNTAX

When used with `set`:

set vpn sites *number* keepalive-settings [mode *mode*] [ip1 *ip1*] [ip2 *ip2*] [ip3 *ip3*]

When used with `show`:

show vpn sites *number* keepalive-settings [mode | ip1 | ip2 | ip3]

FIELDS

`number`	Integer. The VPN site's row in the VPN Sites table.
`mode`	String. Indicates whether to enable keep the tunnel to the VPN site alive. This can have the following values: • `enabled` - The tunnel will be kept alive. • `disabled` - The tunnel will not be kept alive. The default value is `disabled.`

`ip1, ip2, ip3`	IP Address or String. An IP address that the Embedded NGX appliance should ping in order to keep the tunnel to the VPN site alive. This field can have the following values: • An IP address • `undefined` - No IP address is defined. The default value is `undefined`.

Example 1

The following command enables keeping the tunnel to VPN site 1 alive by pinging the IP address 1.2.3.4:

```
set vpn sites 1 keepalive-settings mode enabled ip1 1.2.3.4
```

EXAMPLE 2

The following command displays the keep-alive settings for VPN site 1:

```
show vpn sites 1 keepalive-settings
```

vpn sites ospf

PURPOSE

The `vpn sites ospf` variable is used for working with OSPF (Open Shortest Path First) settings for VPN sites in the following ways:

- Configuring OSPF settings for the VPN site
- Displaying and exporting OSPF settings for the VPN site, including authentication settings

  For information on configuring, displaying, and exporting specific authentication settings, see ***vpn sites ospf authentication*** on page 758.

These settings are only relevant if OSPF is enabled and the VPN site is route-based. For information on configuring OSPF, see ***ospf*** on page 470. For information on configuring route-based VPNs, see ***vpn sites*** on page 740.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set vpn sites *number* ospf [cost *cost*] [passive-interface *passive-interface*] [hello-interval *hello-interval*] [dead-interval *dead-interval*] [retransmit-interval *retransmit-interval*] [transmit-delay *transmit-delay*]

When used with `show`:

show vpn sites *number* ospf [cost | passive-interface | hello-interval | dead-interval | retransmit-interval | transmit-delay]

FIELDS

`number`	Integer. The VPN site's row in the VPN Sites table.
`cost`	Integer. The OSPF cost of sending a packet through the VPN site's VTI. OSPF routers send a packet to the route that matches the packet's destination and has the lowest cost. The default value is 0.
`passive-interface`	String. Indicates whether to define the VPN site as a passive interface. A passive interface is included in the AS topology, but it does not generate or accept OSPF traffic. This can have the following values: • `enabled` - Define the VPN site as a passive interface. • `disabled` - Do not define the VPN site as a passive interface. The default value is `disabled`.
`hello-interval`	Integer. The interval of time (in seconds) between transmissions of hello packets on this interface. The default value is 10 seconds.
`dead-interval`	Integer. The interval of time (in seconds) after which the OSPF neighbor will be considered "dead", if it does not send hello packets. The default value is 40 seconds.

`retransmit-interval`	Integer. The interval of time (in seconds) after which the gateway will send an LSA to a neighbor, if the neighbor does not respond to the previous transmission. The default value is 5 seconds.
`transmit-delay`	Integer. The amount of time (in seconds) required to transmit an LSA packet. This value is added to the LSA packet's age before transmission. When specifying this value, take into account the interface's transmission and propagation delays. Slower Internet connections will require a higher value. The default value is 1 second.

EXAMPLE 1

The following command sets the OSPF cost for VPN site 1:

```
set vpn sites 1 ospf cost 10
```

EXAMPLE 2

The following command displays the OSPF settings for VPN site 1:

```
show vpn sites 1 ospf
```

vpn sites ospf authentication

PURPOSE

The `vpn sites ospf authentication` variable is used for working with OSPF authentication settings for VPN sites in the following ways:

- Configuring OSPF authentication settings for the VPN site
- Displaying and exporting OSPF authentication settings for the VPN site

These settings are only relevant if OSPF is enabled and the VPN site is route-based. For information on configuring OSPF, see ***ospf*** on page 470. For information on configuring route-based VPNs, see ***vpn sites*** on page 740.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set vpn sites *number* ospf authentication [simple-text-password *simple-text-password*] [md5-key *md5-key*] [md5-password *md5-password*] [mode *mode*]

When used with `show`:

show vpn sites *number* ospf authentication [simple-text-password | md5-key | md5-password | mode]

FIELDS

`number`	Integer. The VPN site's row in the VPN Sites table.
`simple-text-password`	String. The password to use for clear-text authentication. Passwords need not be the identical throughout an OSPF area, but they must be the same for OSPF neighbors.
`md5-key`	Integer. The key ID to use for MD5 authentication.

`md5-password`	String. The password to use for MD5 authentication. Passwords need not be the identical throughout an OSPF area, but they must be the same for OSPF neighbors.
`mode`	String. The authentication scheme to use for OSPF connections. This can have the following values: • `none` - Do not use authentication. • `md5` - Use the MD5 authentication scheme. • `simple-text` - Use the clear-text authentication scheme. The default value is `none`.

EXAMPLE 1

The following command enables MD5 authentication for OSPF connections for VPN site 1:

```
set vpn sites 1 ospf authentication md5-key 1 md5-password thepassword
mode md5
```

EXAMPLE 2

The following command displays the OSPF authentication settings for VPN site 1:

```
show vpn sites 1 ospf authentication
```

vpn sites rip

PURPOSE

The `vpn sites rip` variable is used for working with RIP (Routing Information Protocol) settings for VPN sites in the following ways:

- Configuring RIP settings for the VPN site
- Displaying and exporting RIP settings for the VPN site, including authentication settings

  For information on configuring, displaying, and exporting specific authentication settings, see ***vpn sites rip authentication*** on page 762.

These settings are only relevant if RIP is enabled and the VPN site is route-based. For information on configuring RIP, see ***rip*** on page 541. For information on configuring route-based VPNs, see ***vpn sites*** on page 740.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set vpn sites *number* rip passive-interface *passive-interface*

When used with `show`:

show vpn sites *number* rip [passive-interface]

FIELDS

`passive-interface`	String. Indicates whether to define the VPN site as a passive interface. A passive interface does not generate or accept RIP traffic. This can have the following values: • `enabled` - Define the VPN site as a passive interface. • `disabled` - Do not define the VPN site as a passive interface. The default value is `disabled`.

EXAMPLE 1

The following command configures VPN site 1 as a passive interface for RIP traffice:

```
set vpn sites 1 rip passive-interface enabled
```

EXAMPLE 2

The following command displays the RIP settings for VPN site 1:

```
show vpn sites 1 rip
```

vpn sites rip authentication

PURPOSE

The `vpn sites rip authentication` variable is used for working with RIP authentication settings for VPN sites in the following ways:

- Configuring RIP authentication settings for the VPN site
- Displaying and exporting RIP authentication settings for the VPN site

These settings are only relevant if RIP is enabled and the VPN site is route-based. For information on configuring RIP, see ***rip*** on page 541. For information on configuring route-based VPNs, see ***vpn sites*** on page 740.

These settings are only available through the command line.

SYNTAX

When used with `set`:

set vpn sites *number* rip authentication [simple-text-password *simple-text-password*] [md5-key *md5-key*] [md5-password *md5-password*] [mode *mode*]

When used with `show`:

show vpn sites *number* rip authentication [simple-text-password | md5-key | md5-password | mode]

FIELDS

`number`	Integer. The VPN site's row in the VPN Sites table.
`simple-text-password`	String. The password to use for clear-text authentication.
`md5-key`	Integer. The key ID to use for MD5 authentication.
`md5-password`	String. The password to use for MD5 authentication.

`mode`

String. The authentication scheme to use for RIP connections.

This can have the following values:

- `none` - Do not use authentication.
- `md5` - Use the MD5 authentication scheme.
- `simple-text` - Use the clear-text authentication scheme.

The default value is `none`.

EXAMPLE 1

The following command enables MD5 authentication for RIP connections for VPN site 1:

```
set vpn sites 1 rip authentication md5-key 1 md5-password thepassword
mode md5
```

EXAMPLE 2

The following command displays the RIP authentication settings for VPN site 1:

```
show vpn sites 1 rip authentication
```

vstream

PURPOSE

The `vstream` variable is used for working with VStream Antivirus in the following ways:

- Enabling/disabling VStream Antivirus
- Displaying and exporting the VStream Antivirus mode
- Displaying and exporting all VStream Antivirus settings, including archive-handling options, advanced options, and policy rules

  For information on displaying and exporting specific archive-handling options, see ***vstream archive-options*** on page 767. For information on displaying and exporting specific advanced options, see ***vstream options*** on page 770. For information on displaying and exporting specific policy rules, see ***vstream policy rule*** on page 774.

The Embedded NGX appliance includes VStream Antivirus, an embedded stream-based antivirus engine based on Check Point Stateful Inspection and Application Intelligence technologies, that performs virus scanning at the kernel level.

VStream Antivirus scans files for malicious content on the fly, without downloading the files into intermediate storage. This means minimal added latency and support for unlimited file sizes; and since VStream Antivirus stores only minimal state information per connection, it can scan thousands of connections concurrently. In order to scan archive files on the fly, VStream Antivirus performs real-time decompression and scanning of ZIP, TAR, and GZ archive files, with support for nested archive files.

If you are subscribed to the VStream Antivirus subscription service, VStream Antivirus virus signatures are automatically updated, so that security is always up-to-date, and your network is always protected.

For more information on VStream Antivirus, refer to the User Guide.

Note: VStream Antivirus differs from the Email Antivirus subscription service (part of the Email Filtering service) in the following ways:

- Email Antivirus is centralized, redirecting traffic through the Service Center for scanning, while VStream Antivirus scans for viruses in the Embedded NGX gateway itself.
- Email Antivirus is specific to email, scanning incoming POP3 and outgoing SMTP connections only, while VStream Antivirus supports additional protocols, including incoming SMTP and outgoing POP3 connections.

You can use either antivirus solution or both in conjunction. For information on Email Antivirus, see ***mailfilter antivirus*** on page *358*.

SYNTAX

When used with `set`:

set vstream mode *mode*

When used with `show`:

show vstream [mode]

FIELDS

`mode`	String. Indicates whether VStream Antivirus is enabled. This can have the following values: • `enabled` - VStream Antivirus is enabled. • `disabled` - VStream Antivirus is disabled. The default value is `disabled`.

EXAMPLE 1

The following command enables VStream Antivirus:

```
set vstream mode enabled
```

EXAMPLE 2

The following command displays all VStream Antivirus settings, including archive-handling options, advanced options, and policy rules:

```
show vstream
```

vstream archive-options

PURPOSE

The `vstream archive-options` variable is used for working with VStream Antivirus archive-handling settings in the following ways:

- Configuring VStream Antivirus archive-handling settings
- Displaying and exporting the Email Antispam archive-handling settings

SYNTAX

When used with `set`:

set vstream archive-options [nesting-level *nesting-level*] [compression-ratio *compression-ratio*] [archive-failure-action *archive-failure-action*] [password-protected-action *password-protected-action*]

When used with `show`:

show vstream archive-options [nesting-level | compression-ratio | archive-failure-action | password-protected-action]

FIELDS

`nesting-level`	Integer. The maximum number of nested content levels that VStream Antivirus should scan. Setting a higher number increases security. Setting a lower number prevents attackers from overloading the gateway by sending extremely nested archive files. The default value is 5.

`compression-ratio` Integer. The value `X` in 1:`X`, which represents the maximum compression ratio of files that VStream Antivirus should scan.

For example, to specify a 1:150 maximum compression ratio, set this field to 150.

Setting a higher number allows the scanning of highly compressed files, but creates a potential for highly compressible files to create a heavy load on the appliance. Setting a lower number prevents attackers from overloading the gateway by sending extremely compressible files.

The default value is 100.

`archive-failure-action` String. Indicates how VStream Antivirus should handle files that exceed the `nesting-level` value or the `compression-ratio` value, and files for which scanning fails. This can have the following values:

- `pass` - Scan only the number of levels specified, and skip the scanning of more deeply nested archives. Furthermore, skip scanning highly compressible files, and skip scanning archives that cannot be extracted because they are corrupt.
- `block` - Block the file.

The default value is `pass`.

`password-protected-action` String. Indicates how VStream Antivirus should handle password-protected files inside archives. VStream Antivirus cannot extract and scan such files.

This can have the following values:

- `pass` - Accept the file without scanning it.
- `block` - Block the file.

The default value is `pass`.

EXAMPLE 1

The following command sets the VStream Antivirus nesting level to 5:

```
set vstream archive-options nesting-level 5
```

EXAMPLE 2

The following command displays the VStream Antivirus archive-handling settings:

```
show vstream archive-options
```

vstream options

PURPOSE

The `vstream archive-options` variable is used for working with VStream Antivirus advanced settings in the following ways:

- Configuring VStream Antivirus advanced settings
- Displaying and exporting the Email Antispam advanced settings

SYNTAX

When used with `set`:

set vstream options [unsafe-attachments *unsafe-attachments*] [safe-filetypes *safe-filetypes*] [http-ranges *http-ranges*] [decode-failure-action *decode-failure-action*]

When used with `show`:

show vstream options [unsafe-attachments | safe-filetypes | http-ranges | decode-failure-action]

FIELDS

`unsafe-attachments`

String. Indicates whether to block all emails containing potentially unsafe attachments. Unsafe file types are:

- DOS/Windows executables, libraries and drivers
- Compiled HTML Help files
- VBScript files
- Files with {CLSID} in their name
- The following file extensions: ade, adp, bas, bat, chm, cmd,com, cpl, crt, exe, hlp, hta, inf, ins, isp, js, jse, lnk, mdb, mde, msc, msi, msp, mst, pcd, pif, reg, scr, sct, shs,shb, url, vb, vbe, vbs, wsc, wsf, wsh.

This field can have the following values:

- `scan` - Scan the attachment.
- `block` - Block the email.

The default value is `scan`.

`safe-filetypes`

String. Indicates whether to accept common file types that are known to be safe, without scanning them. Safe files types are:

- MPEG streams
- RIFF Ogg Stream
- MP3
- PDF
- PostScript
- WMA/WMV/ASF
- RealMedia
- JPEG - only the header is scanned, and the rest of the file is skipped

This field can have the following values:

- `scan` - Scan the file.
- `pass` - Accept the file without scanning it. This option reduces the load on the gateway by skipping safe file types.

The default value is `pass`.

`http-ranges`

String. Indicates whether to block partial files.

A client might attempt to download partial files in the following situations:

- The client starts downloading a file, and the download is interrupted. The client then reconnects and downloads the rest of the file.
- A download accelerator causes the client to download parts of a desired file from different sources.

VStream Antivirus might not detect a virus signature in a partial file.

This field can have the following values:

- `scan` - Scan partial files.
- `block` - Block partial files. The client must re-download the entire file.

The default value is `scan`.

`decode-failure-action`

String. Indicates whether to block corrupt files and protocol anomalies.

This field can have the following values:

- `scan` - Log the corrupt file or protocol anomaly, and scan the information on a best-effort basis.
- `block` - Block and log the corrupt file or protocol anomaly.

The default value is `scan`.

EXAMPLE 1

The following command configures VStream Antivirus to skip safe file types:

```
set vstream options safe-filetypes pass
```

EXAMPLE 2

The following command displays the VStream Antivirus advanced settings:

```
show vstream options
```

vstream policy rule

PURPOSE

The `vstream policy rule` variable is used for working with VStream Antivirus rules in the following ways:

- Adding new VStream Antivirus rules
- Modifying VStream Antivirus rules
- Deleting VStream Antivirus rules
- Displaying and exporting VStream Antivirus rules
- Clearing the Vstream Antivirus Policy Rule table

VStream Antivirus includes a flexible mechanism that allows the user to define exactly which traffic should be scanned, by specifying the protocol, ports, and source and destination IP addresses.

VStream Antivirus processes policy rules in the order they appear in the VStream Antivirus Policy Rule table, so that rule 1 is applied before rule 2, and so on. This enables you to define exceptions to rules, by placing the exceptions higher up in the table.

SYNTAX

When used with `add`:

add vstream policy rule type *type* [service *service*] [src *src*] [dest *dest*] [ports *ports*] [protocol *protocol*] [index *index*] [disabled *disabled*] [direction *direction*] [description *description*] [time *time*]

When used with `set`:

set vstream policy rule *number* [type *type*] [service *service*] [src *src*] [dest *dest*] [ports *ports*] [protocol *protocol*] [index *index*] [disabled *disabled*] [direction *direction*] [description *description*] [time *time*]

When used with `delete`:

delete vstream policy rule *number*

When used with `show`:

show vstream policy rule [*number*] [type | service | src | dest | ports | protocol | index | disabled | direction | description | time]

When used with `clear`:

clear vstream policy rule

FIELDS

`number` — Integer. The VStream Antivirus rule's row in the VStream Antivirus Policy Rule table.

`type` — String. The type of rule you want to create. This can have the following values:

- `pass` - Enables you to specify that VStream Antivirus should not scan traffic matching the rule.
- `scan` - Enables you to specify that VStream Antivirus should scan traffic matching the rule. If a virus is found, it is blocked and logged.

`service`

Integer or String. The service to which the rule should apply.

This can have the following values:

- `custom` - The rule should apply to a specific non-standard service. You must include the `protocol` and `ports` fields.
- `0` or `any` - The rule should apply to any service.
- `80` or `web`
- `21` or `ftp`
- `23` or `telnet`
- `25` or `smtp`
- `110` or `pop3`
- `137` or `nbt`
- `500` or `vpn`
- `1720` or `h323`
- `1723` or `pptp`
- The name of a network service object

The default value is `0` or `any`.

`src`

IP Address or String. The source of the connections you want to scan or pass. This can have the following values:

- An IP address
- An IP address range - To specify a range, use the following format:
  `<Start IP Address>-<End IP Address>`
- `any` - The rule should apply to any source.
- `wan`
- `lan`
- `dmz`
- `vpn`
- `notvpn` - Not VPN
- The name of a VPN site
- The name of a network object
- The name of a bridge
- The name of a VLAN
- The name of a VAP
- The name of a WDS link

The default value is `any`.

`dest`

IP Address or String. Select the destination of the connections you want to scan or pass. This can have the following values:

- An IP address
- An IP address range - To specify a range, use the following format:
  `<Start IP Address>-<End IP Address>`
- `any` - The rule should apply to any destination.
- `wan`
- `lan`
- `dmz`
- `vpn`
- `notvpn` - Not VPN
- The name of a VPN site
- The name of a network object
- The name of a bridge
- The name of a VLAN
- The name of a VAP
- The name of a WDS link

The default value is `any`.

`ports`

Integer. The ports to which the rule applies. This can have the following values:

- A port number - The rule will apply to this port only.
- A port range - To specify a range, use the following format:
  `<Start Port Number>-<End Port Number>`

Note: If you do not enter a port or port range, the rule will apply to all ports.

`protocol`

String. The protocol for which the rule should apply. This can have the following values:

- `any` - The rule should apply to any protocol.
- `tcp`
- `udp`

The default value is `any`.

`index`

Integer. The VStream Antivirus rule's row in the VStream Antivirus Policy Rules table.

Use this field to move the rule up or down in the VStream Antivirus Policy Rules table. The appliance processes rules higher up in the table (lower indexes) before rules lower down in the table (higher indexes).

If you do not include this field when adding a rule, the rule is automatically added to the bottom of the VStream Antivirus Policy Rules table.

`disabled`

String. Indicates whether the rule is disabled. This can have the following values:

- `true` - The rule is disabled.
- `false` - The rule is enabled.

The default value is `false`.

`direction`

String. Indicates the direction of connections to which the rule should apply. This can have the following values:

- `any` - The rule applies to downloaded and uploaded data.
- `download` - The rule applies to downloaded data, that is, data flowing from the destination of the connection to the source of the connection.
- `upload` - The rule applies to uploaded data, that is, data flowing from the source of the connection to the destination of the connection.

The default value is `any`.

`description`

String. A description of the rule.

`time`

String. The time range during which the rule should be applied.

This can have the following values:

- `always` - The rule is applied at all times.
- A specific time range in the format:
  `hh[:mm][meridian]-hh[:mm][meridian]`
  where:
  `hh` = hours, either in 24-hour or 12-hour clock notation; when using 12-hour clock notation, you must specify the meridian.
  `mm` = minutes
  `meridian` = am or pm; applicable *only* when using 12-hour clock notation.
  For example, both of the following time ranges are acceptable: "3:30pm-6:30pm" and "15:30-18:30". However, "15:30pm-18:30pm" is not acceptable.

EXAMPLE 1

The following command creates a Scan rule for FTP connections from the WAN to the LAN:

```
add vstream policy rule type scan service ftp src wan dest lan
```

EXAMPLE 2

The following command modifies rule 1 in the VStream Antivirus Policy Rule table, so that it becomes a Pass rule:

```
set vstream policy rule 1 type pass
```

EXAMPLE 3

The following command deletes rule 1 in the VStream Antivirus Policy Rule table:

```
delete vstream policy rule 1
```

EXAMPLE 4

The following command displays the destination IP address for rule 1 in the VStream Antivirus Policy Rule table:

```
show vstream policy rule 1 dest
```

EXAMPLE 5

The following command deletes all rules in the VStream Antivirus Policy Rule table:

```
clear vstream policy rule
```

webfilter blocked-page

PURPOSE

The `webfilter blocked-page` variable is used for working with the Access Denied page in the following ways:

- Customizing the Access Denied page settings
- Displaying and exporting Access Denied page settings

The Access Denied page appears when a user attempts to access a page that is blocked either by a Web rule or by the Web Filtering service. For information on Web rules, see ***webfilter rule*** on page 790. Fro information on the Web Filtering service, see ***webfilter service*** on page 796.

SYNTAX

When used with `set`:

set webfilter blocked-page [frame-handling *frame-handling*] [message *message*] [usehttps *usehttps*]

When used with `show`:

show webfilter blocked-page [frame-handling | message | usehttps]

FIELDS

`frame-handling`	String. Indicates whether the Access Denied page will appear when a single frame is blocked or when a page is blocked. This can have the following values: • `block-page` - The Access Denied page will appear for whole pages. • `block-frame` - The Access Denied page will appear for individual frames. The default value is `block-frame`.
`message`	String. The text that appears in the Access Denied page. You can use HTML tags as needed.

`usehttps`

String. Indicates whether the Access Denied page should be displayed using HTTPS. This can have the following values:

- `true` - The Access Denied page is displayed using HTTPS.
- `false` - The Access Denied page is not displayed using HTTPS.

The default value is `false`.

EXAMPLE 1

The following command configures the Access Denied page to open using HTTPS:

```
set webfilter blocked-page usehttps true
```

EXAMPLE 2

The following command displays the Access Denied page text:

```
show webfilter blocked-page "This text message will be shown"
```

webfilter categories

PURPOSE

The `webfilter categories` variable is used for working with Web Filtering categories in the following ways:

- Defining which Web Filtering categories should be considered appropriate for your family or office members
- Displaying and exporting Web Filtering category settings

If you enable the Web Filtering service for a category, Web sites in that category will remain visible. If you disable the Web Filtering service for a category, Web sites in that category will be blocked and will require the administrator password for viewing.

For information on enabling the Web Filtering service, see ***webfilter service*** on page 796.

Note: The Web Filtering service is only available if you are connected to a Service Center and subscribed to this service.

Note: The list of supported categories may vary, depending on the Service Center to which the Embedded NGX appliance is connected.

SYNTAX

When used with `set`:

set webfilter categories [adult *adult*] [advertisements *advertisements*] [art-entertainment *art-entertainment*] [auction *auction*] [careers *careers*] [chat *chat*] [computing *computing*] [consumer-info *consumer-info*] [criminal *criminal*] [dating *dating*] [drugs *drugs*] [file-sharing *file-sharing*] [finance *finance*] [forum *forum*] [gambling *gambling*] [gambling-related *gambling-related*] [game-violence *game-violence*] [games *games*] [glamour *glamour*] [gruesome-content *gruesome-content*] [hacking *hacking*] [hate *hate*] [health *health*] [hosting *hosting*] [humor *humor*] [instant-messaging *instant-messaging*] [interactive-webapps *interactive-webapps*] [lifestyle *lifestyle*] [malicious-sites *malicious-sites*] [media-downloads *media-downloads*] [messaging *messaging*] [mobile-phone *mobile-phone*] [news *news*] [non-profit-organizations *non-profit-organizations*] [personal-network-storage *personal-network-storage*] [photo-search *photo-search*] [politics *politics*] [portal-sites *portal-sites*] [profanity *profanity*] [proxy *proxy*] [reference *reference*] [religion *religion*] [remote-access *remote-access*] [resource-sharing *resource-sharing*] [search *search*] [shareware *shareware*] [shopping *shopping*] [sport *sport*] [streaming-media

streaming-media] [technical-forums *technical-forums*] [tobacco *tobacco*] [travel *travel*] [usenet *usenet*] [violence *violence*] [weapons *weapons*] [web-mail *web-mail*] [web-phone *web-phone*]

When used with `show`:

show webfilter categories [adult | advertisements | art-entertainment | auction | careers | chat | computing | consumer-info | criminal | dating | drugs | file-sharing | finance | forum | gambling | gambling-related | game-violence | games | glamour | gruesome-content | hacking | hate | health | hosting | humor | instant-messaging | interactive-webapps | lifestyle | malicious-sites | media-downloads | messaging | mobile-phone | news | non-profit-organizations | personal-network-storage | photo-search | politics | portal-sites | profanity | proxy | reference | religion | remote-access | resource-sharing | search | shareware | shopping | sport | streaming-media | technical-forums | tobacco | travel | usenet | violence | weapons | web-mail | web-phone]

FIELDS

`adult/advertisements/ art-entertainment/ auction/careers/chat/ computing/consumer-info/criminal/dating/drugs/file-sharing/ finance/forum/gambling/gambling-related/game-violence/games/ glamour/gruesome-content/ hacking/hate/health/hosting/humor/instant-messaging/ interactive-webapps/lifestyle/ malicious-sites/media-downloads/ messaging/mobile-phone/ news/non-profit-organizations/`	String. Indicates whether Web sites that deal with the specified content category should be blocked. This can have the following values: • `allow` - Do not block the sites • `block` - Block the sites The default value is `allow`. Note: The list of supported categories may vary.

```
personal-network-storage/
photo-search/politics/
portal-sites/profanity/
proxy/reference/religion/
remote-access/resource-sharin
g/
search/shareware/shopping/
sport/streaming-media/
technical-forums/
tobacco/travel/usenet/
violence/weapons/
web-mail/web-phone
```

`unknown`

String. Indicates whether unknown Web sites should be blocked. This can have the following values:

- `allow` - Do not block unknown sites
- `block` - Block all unknown sites

The default value is `allow`.

EXAMPLE 1

If Web Filtering is enabled, you can use the following command to block websites dealing with hate speech and violence:

```
set webfilter categories hate block violence block
```

For information on enabling the Web Filtering service, see webfilter.

EXAMPLE 2

The following command displays all Web Filtering category settings:

```
show webfilter categories
```

webfilter logging

PURPOSE

The `webfilter logging` variable is used for configuring how URLs that are filtered by the Web Filtering service and/or by Web rules are logged:

- Customizing URL logging settings
- Displaying and exporting URL logging settings

By default, only URLs that are blocked by the Web Filtering service and/or by Web rules are logged in the appliance's Security Log. You can specify that allowed content should be logged, as well. For information on Web rules, see ***webfilter rule*** on page 790. For information on the Web Filtering service, see ***webfilter service*** on page 796.

SYNTAX

When used with `set`:

set webfilter logging mode *mode*

When used with `show`:

show webfilter logging [mode]

FIELDS

`mode`	String. Indicates whether full URL logging is enabled. This can have the following values: • `enabled` - Full URL logging is enabled. Both blocked and allowed content will be logged. • `disabled` - Full URL logging is disabled. Only blocked content will be logged. The default value is `disabled`.

EXAMPLE 1

The following command enables full URL logging:

```
set webfilter logging mode enabled
```

EXAMPLE 2

The following command displays the URL logging settings:

```
show webfilter logging
```

webfilter rule

PURPOSE

The `webfilter rule` variable is used for working with Web rules in the following ways:

- Adding new Web rules
- Modifying Web rules
- Deleting Web rules
- Displaying and exporting Web rules
- Clearing the Web Rules table

You can block or allow access to specific Web pages, by defining Web rules. Authorized users will be able to view Web pages with no restrictions, only after they have provided their username and password via the Access Denied page. For information on customizing this page, see ***webfilter blocked-page*** on page 782.

The Embedded NGX appliance processes Web rules in the order they appear in the Web Rules table, so that rule 1 is applied before rule 2, and so on. This enables you to define exceptions to rules, by placing the exceptions higher up in the Web Rules table.

Note: Web rules affect outgoing traffic only and cannot be used to allow or limit access from the Internet to internal Web servers.

Note: Web rules differ from the Web Filtering subscription service in the following ways:

- The Web Filtering service is subscription-based and requires a connection to the Service Center, while Web rules are included with the Embedded NGX appliance.
- The Web Filtering service is centralized, extracting URLs from HTTP requests and sending the URLs to the Service Center to determine whether they should be blocked or allowed. With Web rules, HTTP requests are analyzed in the gateway itself.
- The Web Filtering service is category based; that is, it filters Web sites based on the category to which they belong. In contrast, Web rules allow and block specific URLs.

You can use either content filtering solution or both in conjunction. When a user attempts to access a Web site, the Embedded NGX appliance first evaluates the Web rules. If the site is not blocked or allowed by the Web rules, the Web Filtering service is then consulted. For information on the Web Filtering service, see ***webfilter service*** on page *796*.

SYNTAX

When used with `add`:

add webfilter rule action *action* url *url* [src *src*] [track *track*] [index *index*] [time *time*]

When used with `set`:

set webfilter rule *number* [action *action*] [url *url*] [src *src*] [track *track*] [index *index*] [time *time*]

When used with `delete`:

delete webfilter rule *number*

When used with `show`:

show webfilter rule [*number*] [action | url | src | track | index | time]

When used with `clear`:

clear webfilter rule

FIELDS

`number`

Integer. The Web rule's row in the Web Rules table.

`action`

String. The type of rule you want to create. This can have the following values:

- `allow` - The specified Web page should be allowed.
- `block` - The specified Web page should be blocked.

`url`

IP Address or String. The Web page to which the rule should apply. This can have the following values:

- An IP address
- A URL

Wildcards (*) are supported. For example, to block all URLs that start with "http://www.casino-", set this field's value to: `http://www.casino-*`

Note: If you block a Web site based on its domain name (http://<domain_name>), the Web site is not automatically blocked when surfing to the Web server's IP address (http://<IP_address>). Likewise, if you block a Web site based on its IP address, the Web site is not automatically blocked when surfing to the domain name. To prevent access to both the domain name and the IP address, you must block both.

`src`

IP Address or String. The source of the connections you want to allow/block. This can have the following values:

- An IP address
- An IP address range - To specify a range, use the following format:
  `<Start IP Address>-<End IP Address>`
- `any` - The rule should apply to any source.
- `wan`
- `lan`
- `dmz`
- `officemode`
- `vpn`
- `notvpn` - Not VPN
- The name of a VPN site
- The name of a network object
- The name of a bridge
- The name of a VLAN
- The name of a VAP
- The name of a WDS link

The default value is `any`.

`track`

String. Indicates whether to log the specified blocked or allowed connections to the Web page. This can have the following values:

- `log` - Log the specified connections.
- `none` - Do not log the specified connections.

By default, accepted connections are not logged, and blocked connections are logged.

`index`

Integer. The Web rule's row in the Web Rules table.

Use this field to move the rule up or down in the Web Rules table. The appliance processes rules higher up in the table (lower indexes) before rules lower down in the table (higher indexes).

If you do not include this field when adding a rule, the rule is automatically added to the bottom of the Web Rules table.

`time`

String. The time range during which the rule should be applied. This can have the following values:

- `always` - The rule is applied at all times.
- A specific time range in the format:
  `hh[:mm][meridian]-hh[:mm][meridian]`
  where:
  `hh` = hours, either in 24-hour or 12-hour clock notation; when using 12-hour clock notation, you must specify the meridian.
  `mm` = minutes
  `meridian` = am or pm; applicable *only* when using 12-hour clock notation.
  For example, both of the following time ranges are acceptable: "3:30pm-6:30pm" and "15:30-18:30". However, "15:30pm-18:30pm" is not acceptable.

EXAMPLE 1

The following command creates a Block rule for the URL casino.com:

```
add webfilter rule action block url casino.com
```

EXAMPLE 2

The following command modifies rule 1 in the Web Rules table, so that it becomes an Allow rule:

```
set webfilter rule 1 action allow
```

EXAMPLE 3

The following command deletes rule 1 in the Web Rules table:

```
delete webfilter rule 1
```

EXAMPLE 4

The following command displays the log settings of rule 1 in the Web Rules table:

```
show webfilter rule 1 track
```

EXAMPLE 5

The following command deletes all Web rules in the Web Rules table:

```
clear webfilter rule
```

webfilter service

PURPOSE

The `webfilter service` variable is used for working with the category-based Web Filtering service in the following ways:

- Enabling/disabling the Web Filtering service
- Configuring advanced Web Filtering service settings
- Displaying and exporting the above Web Filtering service settings

When the Web Filtering service is enabled, access to Web content is restricted according to the categories specified using the `webfilter categories` variable. Authorized users will be able to view Web pages with no restrictions, only after they have provided their username and password via the Access Denied page.

For information on configuring Web Filtering category settings, see ***webfilter categories*** on page 785. For information on configuring Access Denied page settings, see ***webfilter blocked-page*** on page 782.

Note: The Web Filtering service is only available if you are connected to a Service Center and subscribed to this service.

Note: If the Embedded NGX appliance is remotely managed, contact your Service Center administrator to change these settings.

Note: The Web Filtering subscription service differs from Web rules in the following ways:

- The Web Filtering service is subscription-based and requires a connection to the Service Center, while Web rules are included with the Embedded NGX appliance.
- The Web Filtering service is centralized, extracting URLs from HTTP requests and sending the URLs to the Service Center to determine whether they should be blocked or allowed. With Web rules, HTTP requests are analyzed in the gateway itself.
- The Web Filtering service is category based; that is, it filters Web sites based on the category to which they belong. In contrast, Web rules allow and block specific URLs.

You can use either content filtering solution or both in conjunction. When a user attempts to access a Web site, the Embedded NGX appliance first evaluates the Web rules. If the

site is not blocked or allowed by the Web rules, the Web Filtering service is then consulted. For information on Web rules, see ***webfilter rule*** on page *790*.

For information on temporarily disabling the Web Filtering service, refer to the User Guide.

SYNTAX

When used with `set`:

set webfilter service [mode *mode*] [onfailure *onfailure*] [time *time*]

When used with `show`:

show webfilter service [mode | onfailure | time]

FIELDS

mode

String. The Web Filtering service mode. This can have the following values:

- `enabled` - Enables the service for all internal network computers.
- `disabled` - Disables the service for all internal network computers.

The default value is `disabled`.

onfailure

String. Indicates how the gateway should handle Web Filtering when the service is enabled and the Service Center is unavailable.

This can have the following values:

- `fail-closed` - Temporarily block all connections to the Internet. This ensures that users will not gain access to undesirable Web sites, even when the Service Center is unavailable.
- `fail-open` - Temporarily allow all connections to the Internet. This ensures continuous access to the Internet.

The default value is `fail-closed`.

`time`

String. Indicates whether Automatic Snooze should be used to temporarily disable the Web Filtering service during certain hours of the day. This can have the following values:

- `always` - The Web Filtering service is always enabled.
- A specific time range - Automatic Snooze is used to disable Web Filtering during the specified time range.
  The time range must be in the format:
  `hh[:mm][meridian]-hh[:mm][meridian]`
  where:
  `hh` = hours, either in 24-hour or 12-hour clock notation; when using 12-hour clock notation, you must specify the meridian.
  `mm` = minutes
  `meridian` = am or pm; applicable *only* when using 12-hour clock notation.
  For example, both of the following time ranges are acceptable: "3:30pm-6:30pm" and "15:30-18:30". However, "15:30pm-18:30pm" is not acceptable.

EXAMPLE 1

The following command enables the Web Filtering service:

```
set webfilter service mode enabled
```

EXAMPLE 2

The following command displays all Web Filtering service settings, as well as Web rules and Access Denied page settings:

```
show webfilter service
```

wireless

PURPOSE

The `wireless` variable is used for working with global wireless settings in the following ways:

- Configuring your Embedded NGX appliance's wireless connection settings, including:
  - The wireless connecton's country, operation mode, and channel
  - The antenna to use for communicating with wireless stations
  - Wireless transmitter power
- Displaying and exporting global wireless settings

These settings apply to all wireless networks, including:

- The primary WLAN
- All virtual access points (VAPs)
- All wireless distribution system (WDS) links

For information on configuring the primary WLAN, see ***net wlan*** on page 442. For information on configuring VAPs, see ***vlan*** on page 686. For information on configuring WDS links, see ***vlan*** on page 686.

These settings are only relevant for models supporting a wireless interface.

SYNTAX

When used with `set`:

set wireless [country *country*] [opmode *opmode*] [channel *channel*] [xmitpower *xmitpower*] [antenna *antenna*] [channel-width *channel-width*] [guard-interval *guard-interval*]

When used with `show`:

show wireless [country | opmode | channel | xmitpower | antenna | channel-width | guard-interval]

FIELDS

`country`

String. The country code of the country in which you are located. For a list of country codes, see ***Country Codes*** on page 807.

Warning: Choosing an incorrect country may result in the violation of government regulations.

`opmode`

String. The operation mode. This can have the following values:

- `11b` - Operates in the 2.4 GHz range and offers a maximum theoretical rate of 11 Mbps. When using this mode, only 802.11b stations will be able to connect.
- `11g` - Operates in the 2.4 GHz range, and offers a maximum theoretical rate of 54 Mbps. When using this mode, only 802.11g stations will be able to connect.
- `11bg` - Operates in the 2.4 GHz range, and offers a maximum theoretical rate of 54 Mbps. When using this mode, both 802.11b stations and 802.11g stations will be able to connect.
- `11n` - Operates in the 5 GHz or 2.4 GHz range, and offers a maximum theoretical rate of 300 Mbps. When using this mode, only 802.11n stations will be able to connect.
  This mode is relevant only for the following appliance models: Safe@Office 1000NW and UTM-1 Edge NW.
- `11ng` - Operates in the 5 GHz or 2.4 GHz range, and offers a maximum theoretical rate of 300 Mbps. When using this mode, 802.11g stations and and 802.11n stations will be able to connect.
  This mode is relevant only for the following appliance models: Safe@Office 1000NW and UTM-1 Edge NW.
- `54-108g` - Operates in the 2.4 GHz range, and offers a maximum theoretical rate of 108 Mbps. When using this mode, 802.11g stations and

802.11g Super stations will all be able to connect.
This mode is *not* relevant for the following appliance models: Safe@Office 1000NW and UTM-1 Edge NW.

- `108g-dynamic` - Operates in the 2.4 GHz range, and offers a maximum theoretical rate of 108 Mbps. When using this mode, 802.11b stations, 802.11g stations, and 802.11g Super stations will all be able to connect.
  This mode is *not* relevant for the following appliance models: Safe@Office 1000NW and UTM-1 Edge NW.

The list of modes is dependent on the country specified.

The default value is `11g`.

You can prevent older wireless stations from slowing down your network, by choosing an operation mode that restricts access to newer wireless stations.

Note: The actual data transfer speed is usually significantly lower than the maximum theoretical bandwidth and degrades with distance.

Important: The station wireless cards must support the selected operation mode. For a list of cards supporting 802.11g Super, refer to http://www.super-ag.com.

`channel`

Integer or String. The radio frequency to use for the wireless connection. This can have the following values:

- `auto` - The Embedded NGX appliance automatically selects a channel.
- A specific channel between 1 and 14

The list of channels is dependent on the selected country and operation mode.

The default value is `auto`.

Note: If there is another wireless network in the vicinity, the two networks may interfere with one another. To avoid this problem, the networks should be assigned channels that are at least 25 MHz (5 channels) apart. Alternatively, you can reduce the transmission power.

`xmitpower`

String. The transmitter power. This can have the following values:

- `min` - The minimum power
- `eighth` - One-eighth of full power
- `quarter` - One quarter of full power
- `half` - One half of full power
- `full` - Full power

Setting a higher transmitter power increases the access point's range. A lower power reduces interference with other access points in the vicinity.

The default value is `full`. It is not necessary to change this value, unless there are other access points in the vicinity.

`antenna`

String. The antenna to use for communicating with wireless stations.

Multipath distortion is caused by the reflection of Radio Frequency (RF) signals traveling from the transmitter to the receiver along more than one path. Signals that were reflected by some surface reach the receiver after non-reflected signals and distort them.

Embedded NGX appliances avoid the problems of multipath distortion by using an antenna diversity system. To provide antenna diversity, each wireless security appliance has two antennas.

This field can have the following values:

- `auto` - The Embedded NGX appliance receives signals through both antennas and automatically selects the antenna with the lowest distortion signal to use for communicating. The selection is made on a per-station basis.
- `left` - The ANT 1antenna is always used for communicating.
- `right` - The ANT 2 antenna is always used for communicating.

The default value is `auto`.

Use manual diversity control (`right` or `left`), if there is only one antenna connected to the appliance.

This attribute is not relevant for the following appliance models: Safe@Office 500W and UTM-1 Edge NW.

`channel-width`

String. The channel width. This can have the following values:

- `auto` - Automatically select the channel width: 20Mhz or 40Mhz.
- 20 - 20Mhz

Selecting `auto` can increase wireless performance, if a 40Mhz channel is available. However, in some cases it may interfere with other access points or wireless equipment in the area.

This attribute is only available for wireless N series appliances.

`guard-interval`

String. The guard interval, which is the amount of time between symbol transmissions (in nanoseconds). The guard interval allows reflections from the previous data transmission to settle before transmitting a new symbol. This can have the following values:

- `normal` - 800ns
- `short` - 400ns

Selecting `short` can increase throughput. However, in some cases it can also increase error rate, due to increased sensitivity to RF reflections.

This attribute is only available for wireless N series appliances.

EXAMPLE 1

The following command configures the Embedded NGX appliance to automatically select a channel and antenna:

```
set wireless channel auto antenna auto
```

EXAMPLE 2

The following command displays the wireless operation mode:

```
show wireless opmode
```

Appendix A

Country Codes

This appendix lists the codes for each country.

Table 4: Country Codes

Country	Code
No country set (default)	NA
Albania	AL
Algeria	DZ
Argentina	AR
Australia	AU
Austria	AT
Bahrain	BH
Belarus	BY
Belgium	BE
Belize	BZ
Bolivia	BO
Brazil	BR
Brunei Darussalam	BN

Country	Code
Bulgaria	BG
Canada	CA
Chile	CL
China	CN
Colombia	CO
Costa Rica	CR
Croatia	HR
Cyprus	CY
Czech Republic	CZ
Denmark	DK
Dominican Republic	DO
Ecuador	EC
Egypt	EG
El Salvador	SV
Estonia	EE
Finland	FI
France	FR
France RES	F2
Georgia	GE

Country	Code
Germany	DE
Greece	GR
Guatemala	GT
Honduras	HN
Hong Kong	HK
Hungary	HU
Iceland	IS
India	IN
Indonesia	ID
Iran	IR
Iraq	IQ
Ireland	IE
Israel	IL
Italy	IT
Jamaica	JM
Japan	JP
Jordan	JO
Kenya	KE
Kuwait	KW

Country	Code
Latvia	LV
Lebanon	LB
Liechtenstein	LI
Lithuania	LT
Luxembourg	LU
Macau	MO
Macedonia	MK
Malaysia	MY
Mexico	MX
Monaco	MC
Morocco	MA
Netherlands	NL
New Zealand	NZ
Nicaragua	NI
Norway	NO
Oman	OM
Pakistan	PK
Panama	PA
Paraguay	PY

Country	Code
Peru	PE
Philippines	PH
Poland	PL
Portugal	PT
Puerto Rico	PR
Qatar	QA
Romania	RO
Russia	RU
Saudi Arabia	SA
Serbia	CS
Singapore	SG
Slovak Republic	SK
Slovenia	SI
South Africa	ZA
South Korea	KR
Spain	ES
Sweden	SE
Switzerland	CH
Syria	SY

Country	Code
Taiwan	TW
Thailand	TH
Trinidad & Tobago	TT
Tunisia	TN
Turkey	TR
Ukraine	UA
United Kingdom	GB
United States	US
Uruguay	UY
Venezuela	VE
Vietnam	VN
Yemen	YE
Zimbabwe	ZW

Appendix B

ADSL Settings

This appendix lists the typical ADSL settings for each country and service provider.

Table 5: ADSL Settings

Country	Service Provider	Connection Type	VPI	VCI	Encapsulation
Argentina	Arnet	PPPoE	0	33	LLC
Argentina	Speedy	PPPoE	8	35	LLC
Australia	Most ISPs	PPPoE	8	35	LLC
Australia	Arachnet	PPPoA	8	35	VCMUX
Australia	Telestra	PPPoE	8	35	LLC
Austria	Most ISPs	PPPoA	8	48	VCMUX
Austria	AON	PPPoA	1	32	VCMUX
Belgium	ADSL Office	PPPoE	8	35	VCMUX
Belgium	Belgacom ADSL	PPPoA	8	35	VCMUX / LLC
Belgium	Turboline	PPPoA	8	35	LLC
Brazil	Brasil Telecom (brturbo)	PPPoE	0	35	LLC
Brazil	do rio grande do sul são	PPPoE	1	32	LLC

Country	Service Provider	Connection Type	VPI	VCI	Encapsulation
Brazil	Speedy da Telefonica	PPPoE	8	35	LLC
Brazil	Velox da Telemar	PPPoE	0	33	LLC
Bulgaria	BTK (ISDN)	PPPoE	1	32	LLC
Bulgaria	BTK (POTS)	PPPoE	0	35	LLC
Canada	Bell Sympatico	PPPoE	0	35	LLC
Czech Republic	Cesky Telecom (PPPoA)	PPPoA	8	48	VCMUX
Czech Republic	Cesky Telecom (PPPoE)	PPPoE	8	48	LLC
Denmark	Cybercity	PPPoA	0	35	VCMUX
Denmark	Tiscali	PPPoA	8	35	VCMUX
Denmark	Tiscali (World Online)	PPPoA	0	35	VCMUX
Egypt	Raya Telecom	PPPoA	8	80	VCMUX
France	9Online	PPPoA	8	35	VCMUX
France	AOL	PPPoA	8	35	VCMUX
France	Cegetel ADSL Max 8 Mb	PPPoA	8	35	VCMUX

Country	Service Provider	Connection Type	VPI	VCI	Encapsulation
France	Cegetel non dégroupé 512 IP/ADSL et dégroupé	PPPoA	8	35	VCMUX
France	Claranet	PPPoA	8	35	VCMUX
France	Club-Internet	PPPoA	8	35	VCMUX
France	EasyConnect	PPPoA	8	35	LLC
France	Free non dégroupé 512/128 & 1024/128	PPPoA	8	35	VCMUX
France	Free non dégroupé ADSL Max	PPPoA	8	35	VCMUX
France	Freesurf	PPPoA	8	35	VCMUX
France	FT	PPPoA	8	35	VCMUX
France	Generic Netissimo	PPPoA	8	35	LLC
France	HRNet	PPPoA	8	35	VCMUX
France	Nerim	PPPoA	8	35	VCMUX
France	Nordnet	PPPoA	8	35	VCMUX
France	Tiscali.fr (128k)	PPPoA	8	35	LLC
France	Tiscali.fr (512k)	PPPoA	8	35	VCMUX
France	Tiscaly Liberty Surf	PPPoA	8	35	LLC

Country	Service Provider	Connection Type	VPI	VCI	Encapsulation
France	Wanadoo	PPPoA	8	35	VCMUX
France	Worldnet	PPPoA	8	35	VCMUX
Germany	1&1 (Dun)	PPPoE	1	32	LLC
Germany	Alice DSL	PPPoE	1	32	LLC
Germany	Anderer Provider für T-DSL (Dun)	PPPoE	1	32	LLC
Germany	Arcor	PPPoE	1	32	LLC
Germany	DT	PPPoE	1	32	LLC
Germany	QSC	PPPoE	1	32	LLC
Germany	Tiscali	PPPoE	1	32	LLC
Germany	T-Online (Dun)	PPPoE	1	32	LLC
Germany	NetCologne	PPPoE	8	35	LLC
Germany	Mnet	PPPoE	1	32	LLC
Hungary	Matav	PPPoE	1	32	LLC
Iceland	Islandssimi	PPPoA	0	35	VCMUX
Iceland	Landssimi	PPPoA	8	48	VCMUX
India	Most ISPs	PPPoA	0	32	VCMUX
Ireland	Most ISPs	PPPoE	8	35	LLC
Israel	Bezeq	PPPoA	8	48	VCMUX

Country	Service Provider	Connection Type	VPI	VCI	Encapsulation
Italy	Albacom	PPPoA	8	35	VCMUX
Italy	Aruba	PPPoA	8	35	VCMUX
Italy	Liberto.it	PPPoA	8	35	VCMUX
Italy	MC-link	PPPoA	8	35	VCMUX
Italy	Nextra	PPPoA	8	35	VCMUX
Italy	Telecom Italia	PPPoA	8	35	VCMUX
Italy	Telvia	PPPoA	8	35	VCMUX
Italy	Tiscali	PPPoA	8	35	VCMUX
Italy	Wind	PPPoA	8	35	VCMUX / LLC
Mexico	Telmex Infinitum	PPPoE	8	35	LLC
Morocco	Maroc Telecom	PPPoA	8	35	VCMUX
Netherlands	Bbeyond (PPPoE)	PPPoE	0	33	LLC
Netherlands	Bbeyond (PPPoA)	PPPoA	0	35	VCMUX
Netherlands	KPN	PPPoA	8	48	VCMUX
New Zealand	New Zealand Telecom	PPPoA	0	100	VCMUX
Poland	NETIA	PPPoE	8	35	LLC
Poland	TPSA	PPPoA	0	35	VCMUX
Portugal	Portugal Telecom	PPPoA	0	35	VCMUX

Country	Service Provider	Connection Type	VPI	VCI	Encapsulation
Russia	MTU Intel	PPPoE	1	50	LLC
Singapore	SingNet Broadband	PPPoA	0	100	VCMUX
Slovenia	SiOL	PPPoE	1	32	LLC
Spain	Albura	PPPoA	1	32	VCMUX
Spain	Arrakis	PPPoA	0	35	VCMUX
Spain	Arsys	PPPoE	1	33	LLC
Spain	Auna	PPPoA	0	35	VCMUX
Spain	Colt Teecom	PPPoA	0	35	VCMUX
Spain	Communitel	PPPoA	0	33	VCMUX
Spain	ERES MAS	PPPoA	8	35	LLC
Spain	Euskatel	PPPoE	8	32	LLC
Spain	Jazztel	PPPoA	8	35	LLC
Spain	Telefonica	PPPoE	8	32	VCMUX / LLC
Spain	Telepac	PPPoE	0	35	LLC
Spain	Terra	PPPoE	8	32	LLC
Spain	Tiscali	PPPoA	1	32	VCMUX
Spain	Uni2	PPPoA	1	33	VCMUX
Spain	Wanadoo Spain	PPPoE	8	32	LLC

Country	Service Provider	Connection Type	VPI	VCI	Encapsulation
Spain	Ya.com	PPPoE	8	32	LLC
Sweden	Skanova	PPPoE	8	35	LLC
UAE	Etisalat Classical IP for Business	PPPoA	0	50	VCMUX
UAE	Etisalat Classical IP Single User	PPPoE	0	100	LLC
UAE	Etislat	PPPoA	0	50	LLC
UAE	UAE-Other	PPPoE	0	50	LLC
UK	Most ISPs	PPPoA	0	38	VCMUX
US	AOL	PPPoE	0	35	LLC
US	BellSouth	PPPoE	8	35	LLC
US	Covad	PPPoE	0	35	LLC
US	EarthLink	PPPoE	0	35	LLC
US	Qwest	PPPoE	0	32	LLC
US	SBC	PPPoE	0	35	LLC
US	Sprint	PPPoE	0	35	LLC
US	Verizon	PPPoE	0	35	LLC

Glossary of Terms

A

ADSL Modem

A device connecting a computer to the Internet via an existing phone line. ADSL (Asymmetric Digital Subscriber Line) modems offer a high-speed 'always-on' connection.

C

CA

The Certificate Authority (CA) issues certificates to entities such as gateways, users, or computers. The entity later uses the certificate to identify itself and provide verifiable information. For instance, the certificate includes the Distinguished Name (DN) (identifying information) of the entity, as well as the public key (information about itself), and possibly the IP address.

After two entities exchange and validate each other's certificates, they can begin encrypting information between themselves using the public keys in the certificates.

Cable Modem

A device connecting a computer to the Internet via the cable television network. Cable modems offer a high-speed 'always-on' connection.

Certificate Authority

The Certificate Authority (CA) issues certificates to entities such as gateways, users, or computers. The entity later uses the certificate to identify itself and provide verifiable information. For instance, the certificate includes the Distinguished Name (DN) (identifying information) of the entity, as well as the public key (information about itself), and possibly the IP address.

After two entities exchange and validate each other's certificates, they can begin encrypting information between themselves using the public keys in the certificates.

Cracking

An activity in which someone breaks into someone else's computer system, bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. The end result is that whatever resides on the computer can be viewed and sensitive data can be stolen without anyone knowing about it. Sometimes, tiny programs are 'planted' on the computer that are designed to watch out for, seize and then transmit to another computer, specific types of data.

D

DHCP
Any machine requires a unique IP address to connect to the Internet using Internet Protocol. Dynamic Host Configuration Protocol (DHCP) is a communications protocol that assigns Internet Protocol (IP) addresses to computers on the network.

DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer.

DMZ
A DMZ (demilitarized zone) is an internal network defined in addition to the LAN network and protected by the Embedded NGX appliance.

DNS
The Domain Name System (DNS) refers to the Internet domain names, or easy-to-remember "handles", that are translated into IP addresses.

An example of a Domain Name is 'www.sofaware.com'.

Domain Name System
Domain Name System. The Domain Name System (DNS) refers to the Internet domain names, or easy-to-remember "handles", that are translated into IP addresses.

An example of a Domain Name is 'www.sofaware.com'.

E

Exposed Host
An exposed host allows one computer to be exposed to the Internet. An example of using an exposed host would be exposing a public server, while preventing outside users from getting direct access form this server back to the private network.

F

Firmware
Software embedded in a device.

G

Gateway
A network point that acts as an entrance to another network.

H

Hacking
An activity in which someone breaks into someone else's computer system, bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. The end result is that whatever resides on the computer can be viewed and sensitive data can be stolen without anyone knowing about it. Sometimes, tiny programs are 'planted' on the computer that are designed to watch out for, seize and then transmit to another computer, specific types of data.

HTTPS

Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL.

A protocol for accessing a secure Web server. It uses SSL as a sublayer under the regular HTTP application. This directs messages to a secure port number rather than the default Web port number, and uses a public key to encrypt data

HTTPS is used to transfer confidential user information.

Hub

A device with multiple ports, connecting several PCs or network devices on a network.

I

IP Address

An IP address is a 32-bit number that identifies each computer sending or receiving data packets across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

IP Spoofing

A technique where an attacker attempts to gain unauthorized access through a false source address to make it appear as though communications have originated in a part of the network with higher access privileges. For example, a packet originating on the Internet may be masquerading as a local packet with the source IP address of an internal host. The firewall can protect against IP spoofing attacks by limiting network access based on the gateway interface from which data is being received.

IPSEC

IPSEC is the leading Virtual Private Networking (VPN) standard. IPSEC enables individuals or offices to establish secure communication channels ('tunnels') over the Internet.

ISP

An ISP (Internet service provider) is a company that provides access to the Internet and other related services.

L

LAN

A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single server within a small geographic area.

M

MAC Address
The MAC (Media Access Control) address is a computer's unique hardware number. When connected to the Internet from your computer, a mapping relates your IP address to your computer's physical (MAC) address on the LAN.

Mbps
Megabits per second. Measurement unit for the rate of data transmission.

MTU
The Maximum Transmission Unit (MTU) is a parameter that determines the largest datagram than can be transmitted by an IP interface (without it needing to be broken down into smaller units). The MTU should be larger than the largest datagram you wish to transmit un-fragmented. Note: This only prevents fragmentation locally. Some other link in the path may have a smaller MTU - the datagram will be fragmented at that point. Typical values are 1500 bytes for an Ethernet interface or 1452 for a PPP interface.

N

NAT
Network Address Translation (NAT) is the translation or mapping of an IP address to a different IP address. NAT can be used to map several internal IP addresses to a single IP address, thereby sharing a single IP address assigned by the ISP among several PCs.

Check Point FireWall-1's Stateful Inspection Network Address Translation (NAT) implementation supports hundreds of pre-defined applications, services, and protocols, more than any other firewall vendor.

NetBIOS
NetBIOS is the networking protocol used by DOS and Windows machines.

P

Packet
A packet is the basic unit of data that flows from one source on the Internet to another destination on the Internet. When any file (e-mail message, HTML file, GIF file etc.) is sent from one place to another on the Internet, the file is divided into "chunks" of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file at the receiving end.

PPPoE
PPPoE (Point-to-Point Protocol over Ethernet) enables connecting multiple computer users on an Ethernet local area network to a remote site or ISP, through common customer premises equipment (e.g. modem).

PPTP

The Point-to-Point Tunneling Protocol (PPTP) allows extending a local network by establishing private “tunnels” over the Internet. This protocol it is also used by some DSL providers as an alternative for PPPoE.

R

RJ-45

The RJ-45 is a connector for digital transmission over ordinary phone wire.

Router

A router is a device that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks.

S

Server

A server is a program (or host) that awaits and requests from client programs across the network. For example, a Web server is the computer program, running on a specific host, that serves requested HTML pages or files. Your browser is the client program, in this case.

Stateful Inspection

Stateful Inspection was invented by Check Point to provide the highest level of security by examining every layer within a packet, unlike other systems of inspection. Stateful Inspection extracts information required for security decisions from all application layers and retains this information in dynamic state tables for evaluating subsequent connection attempts. In other words, it learns!

Subnet Mask

A 32-bit identifier indicating how the network is split into subnets. The subnet mask indicates which part of the IP address is the host ID and which indicates the subnet.

T

TCP

TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

For example, when an HTML file is sent to you from a Web server, the Transmission Control Protocol (TCP) program layer in that server divides the file into one or more packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network.

At the other end (the client program in your computer), TCP reassembles the

individual packets and waits until they have arrived to forward them to you as a single file.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the underlying communication protocol of the Internet.

U

UDP

UDP (User Datagram Protocol) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end.

UDP is often used for applications such as streaming data.

URL

A URL (Uniform Resource Locator) is the address of a file (resource) accessible on the Internet. The type of resource depends on the Internet application protocol. On the Web (which uses the Hypertext Transfer Protocol), an example of a URL is 'http://www.sofaware.com'.

V

VPN

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

VPN tunnel

A secure connection between a Remote Access VPN Client and a Remote Access VPN Server.

Index

L

M

N

S

T

U

W

X