D-Link NetDefend

Internet Security Firewall

CLI Reference Guide

Version 1.0

Revised: 01/17/06

COPYRIGHT & TRADEMARKS

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright © 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

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 supply 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 supply 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 supply 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 office network with the highest level of security. However, no single security product can provide you with absolute protection against a determined effort to break into your system. We recommend using additional security measures to secure highly valuable or sensitive information.

Contents

Chapter 1

Introduction

This chapter introduces the D-Link NetDefend Firewall and this guide.

This chapter includes the following topics:

About Your D-Link NetDefend Firewall

The D-Link NetDefend firewall is a unified threat management (UTM) appliance that enables secure high-speed Internet access from the office. Incorporating software by SofaWare Technologies, an affiliate of Check Point Software Technologies, the worldwide leader in securing the Internet, the NetDefend Secured by Check Point Product Family includes both wired and wireless models. The D-Link 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.

The NetDefend firewall also allows sharing your Internet connection among several PCs or other network devices, enabling advanced office networking and saving the cost of purchasing static IP addresses.

With the NetDefend firewall, you can subscribe to additional security services available from select service providers, including firewall security and software updates, Antivirus, Web Filtering, reporting, and VPN management. By supporting integrated VPN capabilities, the NetDefend firewall allows teleworkers and road warriors to securely connect to the office network, and enables secure interconnection of branch offices.

Using This Reference

This reference guide explains how to use CLI commands to control your NetDefend firewall.

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 115. 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 14. For information on Informational commands, see ***Informational Commands*** on page 44.

Examples — One or more examples that illustrate the command or variable's usage

Note: The information in this guide is relevant for both NetDefend firewalls. For information on specific NetDefend firewall models, refer to your NetDefend firewall's User Guide (see ***Related Publications*** on page 4).

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:

- *NetDefend Secured by Check Point User Guide*

Chapter 2

Using the Serial Console

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

Note: Your terminal emulation software must be set to 57600 bps, N-8-1.

To run commands using a console

1. Connect the serial console to your NetDefend firewall's serial port, using an RS-232 Null modem cable.
2. Log on to the NetDefend 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. In the **RS232** drop-down list, select **Console**.
5. Click **Apply**.

   You can now control the NetDefend firewall from the serial console.

Chapter 3

Using the NetDefend 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 NetDefend firewall, follow these guidelines:

- NetDefend 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 type:

  ```
  sh 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 NetDefend Portal tab, export the NetDefend firewall 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 49.

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.
- 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 NetDefend model, you can control your appliance via the command line in the following ways:

- Using the NetDefend Portal's command line interface.

  See ***Using the NetDefend Portal*** on page 10.
- Using a console connected to the NetDefend firewall.

  For information, see ***Using the Serial Console*** on page 5.
- Using an SSH client.

  See ***Using SSH*** on page 11.
- Importing CLI scripts

See ***Importing CLI Scripts*** on page 13.

Using the NetDefend Portal

You can run commands using the NetDefend Portal.

To run commands using the NetDefend Portal

1. Log on to the NetDefend 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

NetDefend users can control the firewall 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 NetDefend firewall 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 NetDefend 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 12 for information.

Warning: If remote SSH is enabled, your NetDefend firewall settings can be changed remotely, so it is especially important to make sure all NetDefend firewall 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 NetDefend firewall using an SSHv2 client.

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 NetDefend 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 NetDefend configuration file.

      For information on exporting configuration files, refer to the User Guide.

2. Log on to the NetDefend 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 NetDefend firewall 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.

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 2: 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.
`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.

Value	Explanation
`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 NetDefend firewall. 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 NetDefend firewall
- **Informational Commands.** CLI commands for displaying information about your NetDefend firewall, its settings

Several CLI commands use CLI variables. For information on CLI variables, see ***CLI Variables*** on page 115.

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 115.

add

PURPOSE

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

- A self-signed certificate
- DHCP scopes
- Firewall rules
- Network objects
- OSPF areas
- OSPF networks
- QoS classes
- RADIUS servers
- Static routes
- SmartDefense worm patterns
- SmartDefense blocked and allowed FTP commands
- Users
- VLAN networks
- VPN sites
- VStream Antivirus policy rules

SYNTAX

add *variable*

PARAMETERS

`variable`

String. The type of variable you want to add. This can be any of the following:

- `certificate` - A self-signed certificate
- `dhcp scopes` - A DHCP scope
- `fw rules` - A firewall 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
- `routes` - A static route
- `smartdefense ai cifs file-sharing patterns` - A worm pattern that SmartDefense should detect
- `smartdefense ai ftp command` - An FTP command that SmartDefense should allow or block
- `users` - A NetDefend Portal user
- `vlan` - A VLAN network
- `vpn sites` - A VPN site
- `vstream policy rules` - A VStream Antivirus policy rule

For information on these variables and how to use them with the `add` command, see ***CLI Variables*** on page 115.

RETURN VALUES

See ***Typical Return Values*** on page 14.

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:

- A certificate
- DHCP scopes
- Firewall rules
- Network objects
- OSPF areas
- OSPF networks
- QoS classes
- RADIUS servers
- Static routes
- SmartDefense worm patterns
- SmartDefense blocked and allowed FTP commands
- Users
- VLAN networks
- VPN sites
- VStream Antivirus policy rules

Note: You cannot delete the admin user (user 1), the Default QoS class (QoS class 1), or the Default static route (static route 1).

SYNTAX

clear *variable*

PARAMETERS

`variable`	String. The type of variables in the table you want to clear. This can be any of the following: • `certificate` - A certificate • `dhcp scopes` - DHCP scopes • `fw rules` - Firewall rules • `netobj` - Network objects • `ospf area` - OSPF areas • `ospf network` - OSPF networks • `qos classes` - QoS classes • `radius servers` - RADIUS servers • `routes` - Static routes • `smartdefense ai cifs file-sharing patterns` - Worm patterns detected by SmartDefense • `smartdefense ai ftp command` - FTP commands that SmartDefense allows or blocks • `users` - NetDefend Portal users • `vlan` - VLAN networks • `vpn sites` - VPN sites • `vstream policy rules` - VStream Antivirus policy rules For information on these variables and how to use them with the `clear` command, see ***CLI Variables*** on page 115.

RETURN VALUES

See ***Typical Return Values*** on page 14.

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:

- DHCP scopes
- Firewall rules
- Firewall servers
- Network objects
- OSPF areas
- OSPF networks
- QoS classes
- RADIUS servers
- Static routes
- SmartDefense worm patterns
- SmartDefense blocked and allowed FTP commands
- Users
- VLAN networks
- VPN sites
- VStream Antivirus policy rules

Note: You cannot delete the admin user (user 1), the Default QoS class (QoS class 1), or the Default static route (static route 1).

SYNTAX

delete *variable*

PARAMETERS

`variable`

String. The type of variable you want to delete. This can be any of the following:

- `dhcp scopes` - A DHCP scope
- `fw rules` - A firewall rule
- `fw servers` - A firewall server 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
- `routes` - A static route
- `smartdefense ai cifs file-sharing patterns` - A worm pattern that SmartDefense should detect
- `smartdefense ai ftp command` - An FTP command that SmartDefense should allow or block
- `users` - A NetDefend Portal user
- `vlan` - A VLAN network
- `vpn sites` - A VPN site
- `vstream policy rules` - A VStream Antivirus policy rule

For information on these variables and how to use them with the `delete` command, see ***CLI Variables*** on page 115.

RETURN VALUES

See ***Typical Return Values*** on page 14.

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 admin user (user 1), the Default QoS class (QoS class 1), or the Default static route (static route 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 115.

RETURN VALUES

See ***Typical Return Values*** on page 14.

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 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 115.

RETURN VALUES

The desired variables and their fields.

Note: The following information is displayed in encrypted format:

- NetDefend 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

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 NetDefend firewall in the following ways:

- Log out of the current session, when connected to the NetDefend Portal via SSH or serial console
- Replace the installed certificate with a new self-signed certificate
- Reset the NetDefend firewall to its default settings
- Reset the NetDefend firewall to the firmware version that shipped with the appliance
- Reboot the NetDefend firewall
- Clear the Event Log
- Reboot the my.firewall Web service
- Reset the SmartDefense list of worm patterns to its defaults
- Clear Traffic Monitor reports
- Uninstall the VStream Antivirus signature databases
- Check for new security and software updates

quit

Purpose

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

Effect

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

Syntax

```
quit
```

Parameters

None.

Return Values

None.

reset certificate

PURPOSE

The `reset certificate` command is used to replace the installed certificate with a new self-signed certificate.

Note: If your NetDefend firewall 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 NetDefend firewall generates a new self-signed certificate, and replaces the old certificate with the new one. This may take a few seconds.

SYNTAX

```
reset certificate
```

PARAMETERS

None.

RETURN VALUES

A message indicating that the certificate was replaced successfully.

reset defaults

PURPOSE

The `reset defaults` command is used to reset the NetDefend firewall to its default settings. When you reset your NetDefend firewall, 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 36.

⚠ Warning: This operation erases all your settings and password information. You will have to set a new password and reconfigure your NetDefend firewall for Internet connection.

EFFECT

After you run this command, the NetDefend firewall is restarted, and the PWR/SEC LED flashes quickly. This may take a few minutes.

SYNTAX

```
reset defaults
```

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 14.

reset firmware

PURPOSE

The `reset firmware` command is used to reset the NetDefend firewall to the firmware version that shipped with the appliance.

EFFECT

The NetDefend firewall is restarted, and the PWR/SEC LED flashes quickly. This may take a few minutes.

SYNTAX

```
reset firmware
```

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 14.

reset gateway

PURPOSE

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

EFFECT

The PWR/SEC LED flashes quickly. This may take a few minutes.

SYNTAX

```
reset gateway
```

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 14.

reset logs

PURPOSE

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

EFFECT

The logs in the Event Log are cleared.

SYNTAX

```
reset logs
```

PARAMETERS

None.

RETURN VALUES

A message indicating that the Event Log was reset successfully.

reset services

PURPOSE

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

EFFECT

The NetDefend Service Center connection is restarted.

SYNTAX

```
reset services
```

PARAMETERS

None.

RETURN VALUES

See ***Typical Return Values*** on page 14.

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 worm patterns to its defaults.

For information on configuring this list, see ***smartdefense ai cifs file-sharing patterns*** on page 271.

EFFECT

The list of 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 worm patterns was reset successfully.

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 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 43.

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.

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 NetDefend firewall automatically checks for software updates and installs them without user intervention, in the following cases:

- Your NetDefend firewall is remotely managed.
- Your NetDefend firewall 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 14.

Informational Commands

The commands in this section enable you to display information about your NetDefend firewall and its settings. You can display any of the following:

- Certificate details
- Currently active computers on your network
- Currently active connections to and from your network
- Device details
- Firewall statistics for incoming and outgoing traffic
- Event logs
- NAT rules that are currently in effect
- Your appliance's network interfaces
- Your appliance's general OSPF settings
- OSPF database details
- The OSPF mode each for network interface and VTI (Virtual Tunnel Interface)
- OSPF neighbors
- OSPF routes
- The status of the NetDefend firewall's ports, including each Ethernet connection's duplex state
- Network printers details
- Connection probing results for the WAN and WAN2 interfaces
- General traffic reports
- Traffic reports for specific traffic types and network interfaces
- Traffic reports for specific QoS classes

- Currently established VPN tunnels
- Information about VStream Antivirus signature databases
- VStream Antivirus virus signatures
- Information about the defined Internet connections
- Information about your wireless access point
- Information about wireless stations in the WLAN

You can also do the following:

- 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.

`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 NetDefend Portal.

`vpnaccess`

Indicates whether the user is allowed to connect to the NetDefend firewall 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.

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 read true vpnaccess true
filteroverride true ]
```

export

PURPOSE

The `export` command is used to display NetDefend firewall settings.

This is useful in the following cases:

- You are troubleshooting a problem and need to examine the firewall settings.
- You want to change the firewall 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 NetDefend firewalls.

  For information on importing configuration files, refer to the User Guide.
- You want to backup the NetDefend firewall 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 115.

If you do not include this parameter, all settings are exported.

RETURN VALUES

The desired NetDefend Portal firewall settings.

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

EXAMPLE

The following command exports the NetDefend Portal firewall user database:

```
export
```

Running this command results in information such as the following:

```
    export
# Configuration script
# License: D-Link NetDefend (10 nodes)
# Gateway MAC: 00:08:da:77:70:70
# firmware version: 6.0.45x

# Device settings
set device productkey 7a747a-a77a4a-79a8bf hostname "" behindnat undefined

# Clock settings
set clock timezone GMT-08:00 ntp1 "" ntp2 ""
...

# High availability settings
set ha mode disabled syncinterface lan priority 0 groupid 55
```

```
# lower priority when not connected
set ha track wan1 0 wan2 0

# Effect other modules according to current status
set ha effect vpn enabled
# END Configuration script
```

help

PURPOSE

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

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:

```
add                    Add an item to a table
subcommands:
---------------------
fw                     Firewall settings
vpn                    VPN settings
users                  User database
routes                 Static routes database
radius                 RADIUS settings
qos                    Quality of Service
netobj                 Network Objects
certificate            Certificate Creation
vlan                   VLAN Networks
ospf                   OSPF router setting
dhcp                   DHCP settings
vstream                Vstream 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:

```
users               User database

subcommands:

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

name                Username

password            Password for user authentication

adminaccess         Administrator access level

vpnaccess           Allow user to login using VPN client

filteroverride      Allow user to override Web Filtering

hotspotaccess       Allow HotSpot access

expire              Expiration date
```

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, reset,
updatenow, quit, info
```

info certificate

PURPOSE

The `info certificate` command is used to display information about the 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 Dec  3 08:47:42 2005


Validity End Time:   Sat Nov 29 08:47:42 2025


Certificate DN:      /O=EmbeddedNG/OU=Gateways/CN=00:07:d7:77:70:70
Fingerprint:         FEET DAB BODY HULL LYNN VARY GOSH SETS DOT DAR
DOME PAT
```

```
CA Certificate
==============
GMT:                    GMT+02:00
Validity Start Time: Sat Dec  3 08:47:39 2005


Validity End Time:   Sat Nov 29 08:47:39 2025


Certificate DN:      /O=EmbeddedNG/OU=LocalCA/CN=CA-
00:07:d7:77:70:70
Fingerprint:         NO THAT JUST SUM MENU SLAM DING GURU MICE HUGO
WOK VASE
```

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 network device in the LAN, DMZ, WLAN, and OfficeMode network:

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):

`rate` The current transmission rate in Mbps

`signal` The signal strength in dB

`rx rate` The current reception rate in Mbps

`tx rate` The current transmission rate in Mbps

`WLAN mode` The wireless client's operation mode, indicating the client's maximum speed. Possible values are B, G, and 108G

`signal` The signal strength in dB

`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.

`wpa was negotiated` Indicates whether WPA was negotiated with the wireless client. Possible values are:

- `yes.` WPA was negotiated.
- `no.` WPA was not negotiated.

`wpa2 was negotiated` Indicates whether WPA2 was negotiated with the wireless client. Possible values are:

- `yes.` WPA2 was negotiated.
- `no.` WPA2 was not negotiated.

`cipher` The security protocol used for the connection with the wireless client

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

`errors` The total number of transmitted and received frames for which an error occurred

`discard frames` The total number of discarded frames received

`dropped frames` The total number of dropped frames transmitted

`unicast frames` The number of unicast frames transmitted and received

`broadcast frames` The number of broadcast frames transmitted and received

`multicast frames` The number of multicast frames transmitted and received

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
  192.168.10.12:
    mac:                00:0c:6e:41:5d:6a
    type:               computer
    name:               HOME
    license:            licensed
wlan:
  192.168.252.1:
    mac:                00:20:ed:08:7a:e0
    type:               firewall
    name:               Gateway
    license:            N/A
  192.168.252.106:
    mac:             00:40:05:60:97:5a
    type:            computer
    name:            laptop
    license:         N/A
    rx rate:         2 Mbps
    tx rate:         11 Mbps
    WLAN mode:       B
    signal:          22 dB
    XR:              no
    wpa was negotiated: no
    wpa2 was negotiated: no
    cipher:          WEP
    receive:
        frames ok:   159
        errors:      0
        discarded frames: 0
        unicast frames: 93
        broadcast frames: 57
        multicast frames: 9
    transmit:
        frames ok:   76
        errors:      0
        dropped frames: 0
        unicast frames: 76
```

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.
- `Scanned` - The connection is being scanned by VStream Antivirus.

`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

`MAC Address` The appliance's WAN MAC address.

`Bootcode version` The version of the NetDefend bootloader.

`Hardware version` The version of the hardware.

`Appliance Type` The type of the current NetDefend firewall hardware.

`Product Key` The installed Product Key.

`Product Name` The licensed software and the number of allowed nodes.

`Used Nodes` The number of nodes used.

`Uptime` The time that elapsed from the moment the unit was turned on.

`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.

`Free Memory`

Displays the amount of free memory in kilobytes:

- `User` - The amount of free memory in the user module.
- `Kernel` - The amount of free memory in the kernel module.

`Running Firmware`

The version of the firmware that is currently in use.

`Backup Firmware`

The version of the backup firmware.

If no backup firmware is available, this field displays `N/A`.

`VStream database (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

`VStream database (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 value for file verification

EXAMPLE

Running this command results in information such as the following:

```
[700000] Device Information:
MAC Address:         00:08:da:77:70:70
Bootcode version:    19
Hardware version:    1.1
Appliance Type:      SBox-200
Product Key:         747478-22234-e5d66f
Product Name:        D-Link NetDefend, 10 nodes
Used Nodes:          1
Uptime:              45 days, 02:05:53
Debug Firmware:      No
Free Memory:         User 914K
                     Kernel 1829K
Running Firmware:    6.0.45x
Primary Firmware:    6.0.45x
Backup Firmware:     N/A
VStream database (Main):     Sep 13, 2005 12:20 GMT. Version: 1.1.0
Size: 703312 bytes  CRC: 0x823d70ef
VStream database (Daily):     Dec 04, 2005 06:29 GMT. Version:
1.1.46   Size: 175754 bytes  CRC: 0x6d7368d2
```

info fw

PURPOSE

The `info fw` command is used to display firewall statistics for incoming and outgoing traffic.

SYNTAX

```
info fw
```

PARAMETERS

None.

RETURN VALUES

The displayed firewall statistics is divided into information on he following:

`Inbound packets` - Statistics for incoming data packets in the active connection

`Total`	The total number of incoming data packets
`Accepted`	The number of incoming data packets received
`Dropped`	The number of incoming data packets that were blocked by the firewall

`Outbound packets` - Statistics for outgoing data packets in the active connection

`Total`	The total number of outgoing data packets
`Accepted`	The number of data packets sent
`Dropped`	The number of outgoing data packets that were blocked by the firewall

EXAMPLE

Running this command results in information such as the following:

```
[700000] Firewall statistics:
Inbound packets:
  Total:             35867
  Accepted:          14919
  Dropped:           20948
Outbound packets:
  Total:             13641
  Accepted:          13477
  Dropped:           164
```

info logs

PURPOSE

The `info logs` command is used to display information about the most recent events, including the date and the time that each event occurred, and its type.

SYNTAX

info logs

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

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.

EXAMPLE

Running this command results in information such as the following:

```
Event Logs:

00299   4/12 09:33:22 Log 60031: User admin logged in
(Source IP: 192.168.10.12)

00298   4/12 09:32:44 Log 50000: Dropped Inbound packet
(Policy rule) Src:217.132.249.147 SPort:1339
Dst:217.132.214.83 DPort:139 IPP:6 Rule: 15

00297   4/12 09:32:34 Log 50000: Dropped Inbound packet
(Cisco IOS DoS) Src:212.143.205.164 SPort:8192
Dst:224.0.0.13 DPort:51393 IPP:103

...
```

info nat

PURPOSE

The `info nat` command is used to display the NAT (Network Address Translation) rules that are currently in effect. The NetDefend firewall supports the following types of 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 network computers behind the network's single Internet IP address. For information on configuring Hide NAT for an internal network, see ***net lan*** on page 181, ***net dmz*** on page 168, ***net wlan*** on page 219, and ***vlan*** on page 350.
- Static NAT - Allows the mapping of Internet IP addresses or address ranges to hosts inside the internal network. For information on configuring Static NAT for a network object, see ***netobj*** on page 226.

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. This can be the following:

- An internal network
- An IP address
- An IP range
- `any` - Any source

`original destination` The original destination. 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. This can be the following:

- An internal network
- An IP address
- An IP range
- `original` - The original destination

`translated destination` The translated destination. This can be the following:

- An internal network
- An IP address
- An IP range
- `original` - The original destination

`translated ports` The translated ports. This can be the following:

- A port
- A range of ports
- `original` - The original port

`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 an Allow & Forward rule, Hide NAT for an internal network, or Static NAT for a network object.
- `management` - The rule was downloaded 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: 217.132.233.250
    translated destination: original
    translated ports: original
    type: hide
    source: local
   2 :
    original source: dmz
    original destination: any
    original ports: any
    translated source: 217.132.233.250
    translated destination: original
    translated ports: original
    type: hide
    source: local
```

info net

PURPOSE

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

SYNTAX

info net [*interface*]

PARAMETERS

`interface`

Integer. The network interface for which to display information. This parameter can have the following values:

- `1` - Display information for the WAN interface
- `2` - Display information for the LAN interface
- `3` - Display information about the DMZ interface
- 4 - Display information about the WLAN interface
- 5 - Display information about the OfficeMode interface

If you do not include this parameter, information is displayed for all networks.

RETURN VALUES

The following information is displayed for each network interface:

`name`

The network interface's name.

Note: The OfficeMode network's name is `office`.

`ip`

The appliance's current IP address on the specified interface.

`mac`

The appliance's MAC address on the specified interface.

Note: The OfficeMode network's MAC address is `undefined`.

EXAMPLE

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

```
net:
 1:
  name wan
  ip 217.132.214.83
  mac 00:08:da:77:70:70
 2:
  name lan
  ip 192.168.10.1
  mac 00:08:da:77:70:6e
 3:
  name dmz
  ip 192.168.253.1
  mac 00:08:da:77:70:6f
 4:
  name wlan
  ip 192.168.252.1
  mac 00:20:ed:08:7a:e0
 5:
  name office
  ip 192.168.254.1
  mac undefined
```

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: 1.2.3.4
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
SPF schedule delay 1 secs, Hold time between two SPFs 1 secs
Refresh timer 10 secs
Number of external LSA 0
Number of areas attached to this router: 5
```

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 Pri State` The OSPF neighbor's router ID.

`Dead Time Address` 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 NetDefend firewall'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 NetDefend firewall 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 NetDefend firewall. For example, LAN
`R`	An RIP route.
`O`	An OSPF route. OSPF routes are routes learned via OSPF.
`I`	An ISIS route.
`>`	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 NetDefend firewall'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 can’t see the LEDs on front of the appliance.

Note: In the NetDefend model SBX-166LHG-2, port status information is only available for the WAN and DMZ ports, and not for LAN ports 1-4.

SYNTAX

info ports

PARAMETERS

None.

RETURN VALUES

A list of the enabled ports and their statuses.

Note: LAN ports 1-4 appear under `lan`, each on a different line.

A port's status can be either of 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

EXAMPLE

Running this command results in information such as the following:

```
     info ports
wan:
     speed: 100 mbps mode: full duplex
lan:
     no link
     no link
     no link
     speed: 100 mbps mode: full duplex
dmz:
     speed: 100 mbps mode: full duplex
```

info printers

Purpose

The `info 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 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:

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

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 NetDefend firewall's configuration. For information on configuring connection probing for the WAN port, see ***net wan probe*** on page 210. For information on configuring connection probing for the WAN2 port, see ***net wan2 probe*** on page 218.

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 statistics

PURPOSE

The `info statistics` command enables you to view Traffic Monitor reports for incoming and outgoing traffic for all enabled network interfaces 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 99. For information on displaying traffic reports for specific QoS classes, see ***info statistics qos*** on page 102.

SYNTAX

```
info statistics
```

PARAMETERS

None.

RETURN VALUES

A list of traffic reports for all currently enabled networks. 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 341.

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
...


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 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, 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 If you do not include this parameter, information is displayed for all types of traffic on the specified interface.

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 341.

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 341.

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 tunnels

PURPOSE

The `info 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 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 NetDefend firewall supports AES, 3DES, and DES encryption schemes, and MD5 and SHA authentication schemes.

`duration`

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.

EXAMPLE

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

```
site     src            dst            encryption   duration
username  status

office   212.150.8.84   192.114.68.8   3DES/SHA1    0:00:02:01 JohnS
ok

office_2 212.150.8.84   212.150.8.81   AES-256/SHA1 0:00:00:22 N/A
ok
```

info vstream

Purpose

The `info vstream` command is used to display 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 appliance will next check for updates to the VStream Antivirus database.

`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: Sep 13, 2005 02:20:30 PM GMT Version: 1.1.0
Daily database: Dec 4, 2005 08:29:22 AM GMT Version: 1.1.46
Next update: Not Subscribed for Updates Service
Status: OK
```

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 ap

PURPOSE

The `info wireless ap` command is used to display information about your appliance's wireless access point.

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

SYNTAX

```
info wireless ap
```

PARAMETERS

None.

RETURN VALUES

`Operation Mode`

The operation mode used for the wireless connection. This can be any of the following:

- `11b`
- `11g`
- `11bg`
- `108g-static`
- `108g-dynamic`

For information about the operation modes, see ***wireless*** on page 404.

`MAC`

The MAC address of the appliance's wireless interface.

`Region` The region within which the NetDefend firewall 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 NetDefend firewall outside of the certified region may result in the violation of government regulations.

`Country` The country where you are located.

`Channel` The channel currently used for the wireless connection, followed by the exact frequency in parenthesis.

EXAMPLE

Running this command results in information such as the following:

```
Operation Mode: 11b
MAC: 00:20:ed:08:7a:e0
Region: WORLD
Country: United States
Channel: 6 (2437 Mhz)
```

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:

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 NetDefend firewall 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 NetDefend firewall 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 NetDefend firewall should have a unique certificate. Do not use the same certificate for more than one gateway.

Note: If your NetDefend firewall 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 423.

`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, 2006, 12:00 PM:

```
set clock time 12:00:00PM day 2 month 1 year 2006
```

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
- Displaying and exporting device details

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. This value indicates whether or not 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.

`hostname`

String. The hostname for authentication.

Note: Most ISPs do not require a specific hostname. The ISP will supply you with the proper hostname, if required.

`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
```

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*]

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*]

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]

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. Indicates whether the gateway should act as a DNS relay server and automatically pass its own IP address to DHCP clients. This can have the following values:

- `automatic` - The gateway should act as an automatic DNS relay server. This is the default and recommended value.
- `manual` - The gateway should not act as a DNS relay server. If this field is set to `manual`, the `dns1` and `dns2` fields must be specified.

The default value is `automatic`.

`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. Indicates whether DHCP clients should be automatically assigned the same WINS servers as specified by the Internet connection. This can have the following values:

- `automatic` - DHCP clients should be automatically assigned the WINS servers specified by the Internet connection.
- `manual` - DHCP clients should not be automatically assigned the WINS servers specified by the Internet connection.

The default value is `automatic`.

`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 DHCP clients. 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 DHCP clients. 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.

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 dialup modem settings in the following ways:

- Setting up a dialup modem
- Displaying and exporting dialup modem settings

You can use a 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 NetDefend firewall 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 dialup modem, you must connect it to your NetDefend firewall's serial port. You can use either a regular or ISDN dialup 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 214.

SYNTAX

When used with `set`:

set dialup [type *type*] [speed *speed*] [dialmode *dialmode*] [custominit *custominit*]

When used with `show`:

set dialup [type | speed | dialmode | 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.

`speed`

Integer. The modem's port speed (in bits per second). This can have the following values:

- `9600`
- `19200`
- `38400`
- `57600`
- `115200`

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`.

`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 a port speed of 57600 bps, and the installation string AT&F. The dial mode is tone.

```
set dialup type "Hayes Accura 56K" speed 57600 dialmode tone
```

EXAMPLE 2

The following command displays all dialup modem settings:

```
show dialup
```

fw

Purpose

The `fw` variable is used for working with firewall settings in the following ways:

- Defining an exposed host

  The NetDefend firewall allows you to define an exposed host, which is a computer that is not protected by the firewall. This is useful for setting up a public server. It allows unlimited incoming and outgoing connections between the Internet and the exposed host computer. The exposed host 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

  For information on displaying and exporting specific firewall rules and server rules, see ***fw rules*** on page 137 and ***fw servers*** on page 145.

Warning: Defining an exposed host may make the designated computer vulnerable to hacker attacks. Defining an exposed host is not recommended unless you are fully aware of the security risks.

Note: If you are remotely managed, contact your Service Center to change the firewall level.

Syntax

When used with `set`:

set fw [exposedhost *exposedhost*] [level *level*]

When used with `show`:

show fw [exposedhost | level]

FIELDS

`exposedhost`

IP Address. The IP address of the computer you wish to define as an exposed host.

`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 NetDefend firewall 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.

Note: The definitions of firewall security levels provided here represent the NetDefend firewall’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 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 NetDefend firewall 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 NetDefend firewall 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 NetDefend firewall 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*] [**ports** *ports*] [**protocol** *protocol*] [**qosclass** *qosclass*] [**redirectport** *redirectport*] [**index** *index*] [**log** *log*] [**disabled** *disabled*]

When used with `set`:

set fw rules *number* [**action** *action*] [**service** *service*] [**src** *src*] [**dest** *dest*] [**ports** *ports*] [**protocol** *protocol*] [**qosclass** *qosclass*] [**redirectport** *redirectport*] [**index** *index*] [**log** *log*] [**disabled** *disabled*]

When used with `delete`:

delete fw rules *number*

When used with `show`:

show fw rules [*number*] [**action** | **service** | **src** | **dest** | **ports** | **protocol** | **qosclass** | **redirectport** | **index** | **log** | **disabled**]

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 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`
- `lan`
- `dmz`
- `officemode`
- `vpn`
- `notvpn` - Not VPN
- The name of a VPN site
- The name of a network object

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`
- `lan`
- `dmz`
- `officemode`
- `vpn`
- `notvpn` - Not VPN
- The name of a VPN site
- The name of a network object

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`
- `icmp`
- `udp`
- `gre`
- `esp`

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`.

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 (Web Server, Mail Server etc.) in your network.

Note: Configuring servers allows you to create simple Allow and Forward rules for common services, and it is equivalent to creating Allow and Forward rules in the Rules page. For information on creating rules, see ***fw rules*** on page 137.

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 154. For information on configuring, displaying, and exporting specific IHigh Availability effect settings, see ***ha effect*** on page 152.

You can create a High Availability cluster consisting of two or more NetDefend firewalls. For example, you can install two NetDefend firewalls 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 an NetDefend firewall and connected to the Internet.

The NetDefend firewall 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 for which you want to enable High Availability. For instructions, see ***net dmz ha*** on page 175, ***net lan ha*** on page 187, ***net wlan ha*** on page 225, and ***vlan*** on page 350.

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
- `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
- 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 148.

SYNTAX

When used with `set`:

set ha effect vpn *vpn*

When used with `show`:

show ha effect [**vpn**]

FIELDS

`vpn`	String. Indicates whether the gateways' 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`.

EXAMPLE 1

The following command disables the High Availability effect on VPN tunnels:

```
set ha effect vpn disabled
```

EXAMPLE 2

The following command displays the gateway's High Availability effect setting:

```
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 lan1 / port lan2 / port lan3 / port lan4*** on page 245 and ***port dmz*** on page 243.

For information on configuring High Availability, see ***ha*** on page 148.

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
```

https

PURPOSE

The `https` variable is used for working with HTTPS in the following ways:

- Enabling and configuring HTTPS access to the NetDefend Portal
- Displaying and exporting HTTPS settings

When HTTPS Remote Access is enabled, NetDefend firewall users can securely access the NetDefend Portal from the Internet, by accessing the URL https://X.X.X.X:981, where X.X.X.X is the NetDefend 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 NetDefend 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 NetDefend 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 NetDefend firewall settings can be changed remotely, so it is especially important to make sure all NetDefend firewall 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 NetDefend users to access the NetDefend 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
```

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

You can enable your NetDefend firewall 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 NetDefend username and password. The users may then access the Internet.

For information on enabling Secure HotSpot for specific networks, see ***net dmz*** on page 168, ***net lan*** on page 181, and ***net wlan*** on page 219.

For information on granting HotSpot access to users, see ***users*** on page 345.

You can choose to exclude specific network objects from HotSpot enforcement. For information, see ***netobj*** on page 226.

Important: 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: 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*] [multiplelogin *multiplelogin*] [usehttps *usehttps*]

When used with `show`:

show hotspot [**title** | **terms** | **auth** | **multiplelogin** | **usehttps**]

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`.

`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`.

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
```

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: Email Antispam is only available if you are connected to a Service Center and subscribed to this service.

Note: If you are remotely managed, contact your Service Center to enable/disable the Email Antispam service.

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 166.

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 NetDefend 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 382.

Note: Email Antivirus is only available if you are connected to a Service Center and subscribed to this service.

Note: If you are remotely managed, contact your Service Center to enable/disable the Email Antivirus service.

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 166.

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 NetDefend firewall 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 you are remotely managed, contact your Service Center to change the Email Filtering protocol 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
```

net dmz

PURPOSE

The `net dmz` variable is used for working with Demilitarized Zone (DMZ) network settings in the following ways:

- Configuring your NetDefend firewall'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
- Displaying and exporting the above DMZ network settings
- Displaying and exporting all DMZ network settings, including High Availability settings and OSPF settings.

  For information on configuring, displaying, and exporting specific DMZ High Availability settings, see ***net dmz ha*** on page 175. For information on configuring, displaying, and exporting specific DMZ OSPF settings, see ***net dmz ospf*** on page 177 and ***net dmz ospf md5*** on page 179.

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 137. 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 NetDefend firewall, 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*] [**dhcprelayip** *dhcprelayip*] [**hotspot** *hotspot*]

When used with `show`:

show net dmz [**mode** | **hidenat** | **address** | **netmask** | **dhcpserver** | **dhcprange** | **dhcprelayip** | **hotspot**]

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. 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 NetDefend DHCP server is enabled. This can have the following values:

- `enabled` - The NetDefend DHCP server is enabled.
- `disabled` - The NetDefend DHCP server is disabled.
- `relay` - DHCP relay is enabled.

The default value is `enabled`.

By default, the NetDefend firewall operates as a DHCP server. This allows the NetDefend firewall 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 NetDefend DHCP server, you must disable the NetDefend 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 NetDefend DHCP server, you can configure DHCP relay. When in DHCP relay mode, the NetDefend firewall 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 NetDefend DHCP server automatically sets the DHCP address range.
- A DHCP address range - Relevant only if the NetDefend DHCP server is enabled.
  To specify a range, use the following format:
  `<Start IP Address>-<End IP Address>`

The default value is `automatic`.

`dhcprelayip`

IP Address or String. The IP address of the desired relay DHCP server. This can have the following values:

- An IP address
- `undefined` - No relay DHCP 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`.

EXAMPLE 1

The following command enables Hide NAT for the DMZ network:

```
set net dmz hidenat enabled
```

EXAMPLE 2

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 NetDefend firewalls. For more information on High Availability, see ***ha*** on page 148.

SYNTAX

When used with `set`:

```
set net dmz ha virtualip virtualip
```

When used with `show`:

```
show net dmz ha [virtualip]
```

FIELDS

`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 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 OSPF cost 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 md5*** on page 179.

This variable is only relevant if OSPF is enabled. For information, see ***ospf*** on page 231.

SYNTAX

When used with `set`:

set net dmz ospf cost *cost*

When used with `show`:

show net dmz ospf [cost]

FIELDS

`cost`	Integer. The cost of this sending a packet on the DMZ interface. Routers send a packet to the route that matches the packet's destination and has the lowest cost. The default value is 0.

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 md5

PURPOSE

The `net dmz ospf md5` variable is used for working with OSPF MD5 authentication settings for the DMZ in the following ways:

- Configuring OSPF MD5 authentication settings for the DMZ
- Displaying and exporting OSPF MD5 authentication settings for the DMZ

This variable is only relevant if OSPF is enabled. For information, see ***ospf*** on page 231.

SYNTAX

When used with `set`:

set net dmz ospf md5 [enabled *enabled*] [key *key*] [password *password*]

When used with `show`:

show net dmz ospf md5 [enabled | key | password]

FIELDS

`enabled`

String. Indicates whether to use the MD5 authentication scheme for OSPF connections. This can have the following values:

- `true` - Use the MD5 authentication scheme.
- `false` - Do not use the MD5 authentication scheme.

The default value is `disabled`.

`key`

Integer. The key ID to use for authentication.

`password`

String. The password to use for authentication.

Passwords need not be the identical throughout an OSPF area, but they must be the same for OSPF neighbors.

EXAMPLE 1

The following command enables authentication for OSPF connections:

```
set net dmz ospf md5 enabled true key 1 password thepassword
```

EXAMPLE 2

The following command displays the DMZ's OSPF MD5 authentication settings:

```
show net dmz ospf md5
```

net lan

PURPOSE

The `net lan` variable is used for working with your Local Area Network (LAN) settings in the following ways:

- Configuring your NetDefend firewall's LAN settings, including:
  - Hide Network Address Translation (NAT)
  - Your NetDefend firewall’s internal IP address
  - The range of IP addresses in your internal network
  - DHCP settings
  - Secure HotSpot access
- Displaying and exporting the above LAN settings
- Displaying and exporting all LAN settings, including High Availability settings and OSPF settings.

  For information on configuring, displaying, and exporting specific LAN High Availability settings, see ***net lan ha*** on page 187. For information on configuring, displaying, and exporting specific LAN OSPF settings, see ***net lan ospf*** on page 188 and ***net lan ospf md5*** on page 189.

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 NetDefend 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 [**hidenat** *hidenat*] [**address** *address*] [**netmask** *netmask*] [**dhcpserver** *dhcpserver*] [**dhcprange** *dhcprange*] [**dhcprelayip** *dhcprelayip*] [**hotspot** *hotspot*]

When used with `show`:

show net lan [**hidenat** | **address** | **netmask** | **dhcpserver** | **dhcprange** | **dhcprelayip** | **hotspot**]

FIELDS

`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 computers behind the NetDefend firewall’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 NetDefend firewall’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 NetDefend firewall’s internal IP address and by the subnet mask.
For example, if the NetDefend firewall’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.*.

`dhcpserver`

String. Indicates whether the NetDefend DHCP server is enabled. This can have the following values:

- `enabled` - The NetDefend DHCP server is enabled.
- `disabled` - The NetDefend DHCP server is disabled.
- `relay` - DHCP relay is enabled.

The default value is `enabled`.

By default, the NetDefend firewall operates as a DHCP server. This allows the NetDefend firewall to automatically configure all the devices on your network with their network configuration details.

If you already have a DHCP server in your internal network, and you want to use it instead of the NetDefend DHCP server, you must disable the NetDefend 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 NetDefend DHCP server, you can configure DHCP relay. When in DHCP relay mode, the NetDefend firewall relays information from the desired DHCP server to the devices on your 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 NetDefend DHCP server automatically sets the DHCP address range.
- A DHCP address range - Relevant only if the NetDefend DHCP server is enabled.
  To specify a range, use the following format:
  `<Start IP Address>-<End IP Address>`

The default value is `automatic`.

`dhcprelayip`

IP Address. The IP address of the desired relay DHCP server. This can have the following values:

- An IP address
- `undefined` - No relay DHCP 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 LAN network. This can have the following values:

- `enabled` - Secure HotSpot is enabled for the LAN.
- `disabled` - Secure HotSpot is disabled for the LAN.

The default value is `disabled`.

Example 1

The following command enables Hide NAT for the LAN:

```
set net lan hidenat enabled
```

Example 2

The following command displays the LAN DHCP range:

```
show net lan dhcprange
```

net lan ha

See ***net dmz ha*** on page 175.

net lan ospf

See ***net dmz ospf*** on page 177.

net lan ospf md5

See ***net dmz ospf md5*** on page 179.

net officemode

PURPOSE

The `net officemode` variable is used for working with OfficeMode network settings in the following ways:

- Configuring your NetDefend firewall'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 NetDefend 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 NetDefend 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 selected 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 NetDefend DHCP server is enabled. This can have the following values: • `enabled` - The NetDefend DHCP server is enabled. • `disabled` - The NetDefend DHCP server is disabled. • `relay` - DHCP relay is enabled. The default value is `enabled`. By default, the NetDefend firewall operates as a DHCP server. This allows the NetDefend firewall 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 NetDefend DHCP server, you must disable the NetDefend 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 NetDefend DHCP server, you can configure DHCP relay. When in DHCP relay mode, the NetDefend firewall 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 NetDefend DHCP server automatically sets the DHCP address range.
- A DHCP address range - Relevant only if the NetDefend 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 NetDefend firewall's primary Internet connection
- Displaying and exporting the primary Internet connection's settings, including OSPF settings and connection probing settings.

  For information on configuring, displaying, and exporting specific WAN OSPF settings, see ***net wan ospf*** on page 208 and ***net wan ospf md5*** on page 209. For information on configuring, displaying, and exporting specific connection probing settings, see ***net wan probe*** on page 210.

For information on configuring a secondary connection, see ***net wan2*** on page 214.

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*] [ppoeservice *ppoeservice*] [mtu *mtu*] [externalip *externalip*] [phonenumber *phonenumber*] [clonedmac *clonedmac*] [usedhcp *usedhcp*] [staticwins *staticwins*] [connectonlyactive *connectonlyactive*] [staticdns *staticdns*] [disabled *disabled*] [dns1 *dns1*] [dns2 *dns2*] [wins *wins*] [uprate *uprate*] [downrate *downrate*] [connectondemand *connectondemmand*] [idletimeout *idletimeout*] [avoidgateway *avoidgateway*]

When used with `show`:

show net wan [mode | gateway | address | netmask | password | username | pptpserver | pptpclientip | pptpclientmask | pptpservice | pppoeservice | mtu | phonenumber | externalip | clonedmac | usedhcp | staticwins | connectonlyactive | staticdns | disabled | dns1 | dns2 | wins | uprate | downrate | connectondemand | idletimeout | avoidgateway]

FIELDS

`mode`

String. The Internet connection type.

- `lan`
- `cable`
- `pppoe`
- `pptp`
- `bpa`
- `none`
- `dialup`

`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 NetDefend firewall. 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 NetDefend firewall. 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 NetDefend firewall. 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 NetDefend firewall. 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.

`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.

`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 NetDefend firewall 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 NetDefend firewall should automatically configure the WINS server. This can have the following values:

- `enabled` - The NetDefend firewall will not automatically configure the WINS server.
  You must provide a value for the `wins` field.
- `disabled` - The NetDefend firewall will automatically configure the WINS server.

`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 148.

`staticdns` String. Indicates whether the NetDefend firewall should automatically automatically configure DNS servers. This can have the following values:

- `enabled` - The NetDefend firewall will not automatically configure DNS servers.. You must provide values for the `dns1` and `dns2` fields.
- `disabled` - The NetDefend firewall will automatically configure the DNS servers.

`disabled`

String. Indicates whether the connection is enabled. 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 NetDefend firewall to use a particular connection, by disabling the other connection.

Note: The Internet connection’s Enabled/Disabled status is persistent through NetDefend firewall 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 253.
- `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 253.

`connectondemand`

String. Indicates whether the dialup modem should connect to the Internet on demand.

- `disable` - The modem is constantly connected to the Internet.
- `immediate` - The dialup modem should only dial a connection if no other connection exists, and the NetDefend firewall is not acting as a Backup appliance.
  If another connection opens, or if the NetDefend firewall becomes a Backup appliance, the dialup modem will disconnect.
  For information on configuring the appliance as a Backup or Master, refer to the User Guide.
- `activity` - The dialup modem should only dial 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 dialup modem will disconnect.

The default value is `disable`.

This field is useful when configuring a dialup backup connection. For information, see refer to the User Guide.

This field is only relevant for the Dialup connection type.

`idletimeout`

Integer. The amount of time (in minutes) that the connection can remain idle. Once this period of time has elapsed, the dialup modem will disconnect.

The default value is 15.

This field is only relevant for the Dialup connection type.

`avoidgateway`

String. This variable 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 226.

The default value is `false`.

EXAMPLE 1

The following command configures the NetDefend firewall for a PPTP primary Internet connection:

```
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
```

EXAMPLE 2

The following command configures the NetDefend firewall for a LAN primary Internet connection with DHCP:

```
set net wan mode lan disabled false
```

EXAMPLE 3

The following command configures the NetDefend firewall 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 NetDefend firewall 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 displays the NetDefend firewall's cloned MAC address:

```
show net wan clonedmac
```

net wan ospf

See ***net dmz ospf*** on page 177.

net wan ospf md5

See ***net dmz ospf md5*** on page 179.

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 NetDefend firewall'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.

The 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 wan2

PURPOSE

The `net wan2` variable is used for doing the following:

- Configuring your NetDefend firewall's secondary Internet connection
- Displaying and exporting the secondary Internet connection's settings, including OSPF settings and connection probing settings.

  For information on configuring, displaying, and exporting specific WAN2 OSPF settings, see ***net wan2 ospf*** on page 216 and ***net wan2 ospf md5*** on page 217. For information on configuring, displaying, and exporting specific connection probing settings, see ***net wan2 probe*** on page 218.

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 NetDefend firewall remains connected to the Internet.

Note: You can configure different DNS servers for the primary and secondary connections. The NetDefend firewall 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 firewall for different types of secondary Internet connections, refer to the User Guide.

SYNTAX

See ***net wan*** on page 195.

FIELDS

See ***net wan*** on page 195.

EXAMPLE 1

The following command configures the NetDefend firewall for a dialup secondary Internet connection:

```
set net wan2 mode dialup username JohnS.myisp.com password 123456
phonenumber 96909111 disabled false
```

EXAMPLE 2

The following command configures the NetDefend firewall 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 3

The following command configures the NetDefend firewall 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 4

The following command displays the secondary Internet connection's uprate:

```
show net wan2 uprate
```

net wan2 ospf

See ***net dmz ospf*** on page 177.

net wan2 ospf md5

See ***net dmz ospf md5*** on page 179.

net wan2 probe

See ***net wan probe*** on page 210.

net wlan

PURPOSE

The `net wlan` variable is used for working with wireless network (WLAN) settings in the following ways:

- Configuring your NetDefend firewall's WLAN settings, including:
    - Hide Network Address Translation (NAT)
    - The WLAN network's default gateway
    - The WLAN network’s internal network range
    - DHCP (Dynamic Host Configuration Protocol) settings
    - Secure HotSpot access
- Displaying and exporting the above WLAN network settings
- Displaying and exporting all WLAN network settings, including WLAN High Availability settings.

    For information on configuring, displaying, and exporting specific WLAN High Availability settings, see ***net wlan ha*** on page 225.

When using wireless NetDefend models, you can define a wireless internal network called a WLAN network.

For information on configuring wireless connection settings, including the operation mode, security settings, and wireless transmitter settings, see ***wireless*** on page 404. For information on default security policy rules controlling traffic to and from the WLAN, refer to the User Guide.

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

Note: It is recommended to configure the 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*] [**dhcprelayip** *dhcprelayip*] [**hotspot** *hotspot*]

When used with `show`:

show net wlan [**mode** | **hidenat** | **address** | **netmask** | **dhcpserver** | **dhcprange** | **dhcprelayip** | **hotspot**]

FIELDS

`mode`

String. The WLAN network mode. This can have the following values:

- `enabled` - The WLAN network is enabled.
- `disabled` - The WLAN 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 WLAN computers behind the WLAN 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 WLAN network's default gateway.

Note: The WLAN network must not overlap the LAN network.

`netmask`

IP Address. The WLAN's internal network range.

`dhcpserver`

String. Indicates whether the NetDefend DHCP server is enabled. This can have the following values:

- `enabled` - The NetDefend DHCP server is enabled.
- `disabled` - The NetDefend DHCP server is disabled.
- `relay` - DHCP relay is enabled.

The default value is `enabled`.

By default, the NetDefend firewall operates as a DHCP server. This allows the NetDefend firewall to automatically configure all the devices on the WLAN 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 NetDefend DHCP server, you must disable the NetDefend 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 NetDefend DHCP server, you can configure DHCP relay. When in DHCP relay mode, the NetDefend firewall relays information from the desired DHCP server to the devices on the WLAN 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 NetDefend DHCP server automatically sets the DHCP address range.
- A DHCP address range - Relevant only if the NetDefend DHCP server is enabled.
  To specify a range, use the following format:
  `<Start IP Address>-<End IP Address>`

The default value is `automatic`.

`dhcprelayip`

IP Address. The IP address of the desired relay DHCP server. This can have the following values:

- An IP address
- `undefined` - No relay DHCP 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 WLAN network. This can have the following values:

- `enabled` - Secure HotSpot is enabled for the WLAN.
- `disabled` - Secure HotSpot is disabled for the WLAN.

The default value is `disabled`.

EXAMPLE 1

The following command enables Hide NAT for the WLAN network:

```
set net wlan hidenat enabled
```

EXAMPLE 2

The following command displays the WLAN network's DHCP range:

```
show net wlan dhcprange
```

net wlan ha

See ***net dmz ha*** on page 175.

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.

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*]

When used with `set`:

set netobj *number* [**name** *name*] [**type** *type*] [**ip** *ip*] [**staticnat** *staticnat*] [**mac** *mac*] [**hotspotexclude** *hotspotexclude*]

When used with `delete`:

delete netobj *number*

When used with `show`:

show netobj *number* [**name** | **type** | **ip** | **staticnat** | **mac** | **hotspotexclude**]

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`.

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 OSPF (Open Shortest Path First) settings in the following ways:

- Setting the OSPF mode
- Specifying the OSPF router identifier
- Displaying and exporting the above OSPF settings
- Displaying and exporting all OSPF settings, including:
  - OSPF areas
  - OSPF networks
  - Routing information distribution settings

  For information on displaying and exporting specific OSPF areas, see ***ospf area*** on page 234. ***For informat***ion on displaying and exporting specific OSPF networks, see ospf network on page 236. For information on displaying and exporting specific routing information distribution settings, see ***ospf redistribute*** on page 238, ***ospf redistribute connected*** on page 239, and ***ospf redistribute kernel*** on page 241.

The NetDefend firewall 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 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 366.

Note: The NetDefend OSPF implementation is fully interoperable with the Check Point Advanced Routing Suite, as well as with any other RFC-compliant OSPF implementation.

SYNTAX

When used with `set`:

set ospf [mode *mode*] [router-id *router-id*]

When used with `show`:

show ospf [mode | router-id]

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`.

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.

SYNTAX

When used with `add`:

add ospf area id *id* **auth-md5** *auth-md5*

When used with `set`:

set ospf area *number* [**id** *id*] [**auth-md5** *auth-md5*]

When used with `delete`:

delete ospf area *number*

When used with `show`:

show ospf area *number* [**id** | **auth-md5**]

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.

`auth-md5` — String. Indicates whether to use the MD5 authentication scheme for this area. This can have the following values:

- `true` - Use the MD5 authentication scheme.
- `false` - Do not use the MD5 authentication scheme.

Example 1

The following command adds an OSPF area that uses the MD5 authentication scheme:

```
add ospf area id 1.2.3.4 auth-md5 true
```

Example 2

The following command modifies area 1 in the OSPF Areas table, so that it does not use the MD5 authentication scheme:

```
set ospf area 1 auth-md5 false
```

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 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 and OSPF network and assign it to an OSPF area.

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

PURPOSE

The `ospf` variable is used for working with OSPF settings in the following ways:

- Displaying and exporting all OSPF routing information distribution settings.

  For information on displaying and exporting specific routing information distribution settings, see ***ospf redistribute connected*** on page 239 and ***ospf redistribute kernel*** on page 241.

These settings control how OSPF external routing information is redistributed.

SYNTAX

When used with `show`:

show ospf redistribute

FIELDS

None.

EXAMPLE

The following command displays all OSPF redistribution settings:

```
show ospf redistribute
```

ospf redistribute connected

PURPOSE

The `ospf` 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

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 NetDefend firewall 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` 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 NetDefend Portal
- Displaying and exporting OSPF routing information distribution settings for routes updated in the NetDefend Portal

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 for routes updated in the NetDefend 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 NetDefend firewall supports metric types 1 and 2.

EXAMPLE 1

The following command enables redistributing routing information for for routes updated in the NetDefend 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 NetDefend Portal:

```
show ospf redistribute kernel
```

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

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 168.
- `wan2` - A second WAN connection. For information on setting up a backup Internet connection, refer to the User Guide and to ***net wan2*** on page 214.
- `trunk` - A VLAN trunk. For information on VLANs and VLAN trunks, see ***vlan*** on page 350.

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 lan1 / port lan2 / port lan3 / port lan4

PURPOSE

The `port lan1`, `port lan2`, `port lan3`, and `port lan4` variables are used for working with the appliance's LAN1, LAN2, LAN3, and LAN4 ports, respectively, in the following ways:

- Modifying the relevant LAN port's settings
- Displaying and exporting the relevant LAN port's settings

SYNTAX

When used with `set`:

set port lan1 [network *network*] [hatrack *hatrack*] [link *link*]

set port lan2 [network *network*] [hatrack *hatrack*] [link *link*]

set port lan3 [network *network*] [hatrack *hatrack*] [link *link*]

set port lan4 [network *network*] [hatrack *hatrack*] [link *link*]

When used with `show`:

show port lan1 [network | hatrack | link]

show port lan2 [network | hatrack | link]

show port lan3 [network | hatrack | link]

show port lan4 [network | hatrack | link]

FIELDS

`network`	String. The port's assignment. This can have the following values: • `lan` - The LAN network • Any existing VLAN. For information on adding VLANs, see ***vlan*** on page 350. 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 serial

PURPOSE

The `port serial` variable is used for working with the appliance's RS232 port in the following ways:

- Modifying the RS232 port's assignment
- Displaying and exporting the RS232 port's assignment

SYNTAX

When used with `set`:

set port serial mode *mode*

When used with `show`:

show port serial [mode]

FIELDS

`mode`	String. The RS232 port's assignment. This can have the following values: • `auxiliary` - A dialup modem. For information on configuring a dialup modem, see ***dialup*** on page 131. • `console` - A serial console. For information on using a serial console, refer to the User Guide. The default value is `auxiliary`.

EXAMPLE 1

The following command assigns the RS232 port for use with a serial console:

```
set port serial mode console
```

EXAMPLE 2

The following command displays the RS232 port's assignment:

```
show port serial
```

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 link speed and duplex
- Displaying and exporting the WAN port's speed and duplex

SYNTAX

When used with `set`:

set port wan link *link*

When used with `show`:

show port wan [**link**]

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`.

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 dmz
```

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 NetDefend 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 NetDefend firewall. 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.

This variable is 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 NetDefend firewall 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 137.
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*] [weight *weight*] [uplimit *uplimit*] [downlimit *downlimit*] [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 | weight | uplimit | downlimit | 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".

`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 you 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.

`uplimit`

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`.

`downlimit`

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`.

`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 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

You can use RADIUS to authenticate both NetDefend firewall users and Remote Access VPN Clients trying to connect to the NetDefend firewall. When a user accesses the NetDefend Portal and tries to log on, the NetDefend firewall sends the entered user name and password 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 and assigned specific permissions.

SYNTAX

When used with `set`:

set radius permissions [adminaccess *adminaccess*] [vpnaccess *vpnaccess*] [filteroverride *filteroverride*] [hotspotaccess *hotspotaccess*]

When used with `show`:

show radius permissions [adminaccess | vpnaccess | filteroverride | hotspotaccess]

FIELDS

`adminaccess`

String. The level of access to the NetDefend Portal to assign to all users authenticated by the RADIUS server. This can have the following values:

- `none` - The user cannot access the NetDefend Portal.
- `readonly` - The user can log on to the NetDefend Portal, but cannot modify system settings.
- `readwrite` - The user can log on to the NetDefend 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 NetDefend Remote Access VPN Server is enabled. See ***vpn server*** on page 361.

`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 159.

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*]

When used with `set`:

set radius servers *number* [address *address*] [secret *secret*] [port *port*] [realm *realm*] [timeout *timeout*] [tries *tries*]

When used with `show`:

show radius servers [*number*] [address | secret | port | realm | timeout | tries]

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 NetDefend Portal, the NetDefend firewall 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.

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
```

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 for packets originating in a certain subnet and/or destined for a certain subnet. Packets with a source and destination that does not match any defined static route will be routed to the default gateway.

A static route can be based on the packet's destination IP address, or based on the source IP address, in which case it is a source route.

Note: You cannot delete or modify the Default static route (route 1).

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. The IP address of the gateway (next hop router) to which to route the packets destined for this network.

`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.

EXAMPLE 1

The following command adds the a 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 271.

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.

You can configure how CIFS worms should be handled.

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.
- `log` - 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 268.

You can reset the CIFS worm patterns to their defaults. See ***reset smartdefense ai cifs file-sharing patterns*** on page 40.

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 `false`.

`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 CFS Worm Patterns table:

```
set smartdefense ai cifs file-sharing patterns 1 active false
```

EXAMPLE 3

The following command deletes worm pattern 1 in the CFS 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 CFS 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 277. For information on configuring specific FTP Command settings, see ***smartdefense ai ftp commands*** on page 279.

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 279.

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 274.

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 274.

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 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*]

When used with `show`:

show smartdefense ai im icq [enforce | log | block-proprietary]

FIELDS

`enforce`

String. Indicates whether to enable ICQ connection blocking.

This can have the following values:

- `enabled` - ICQ connection blocking is enabled.
- `disabled` - ICQ 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 ICQ connections.
- `disabled` - Do not log ICQ 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`.

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 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*]

When used with `show`:

show smartdefense ai im skype [**enforce** | **log** | **block-proprietary**]

FIELDS

See ***smartdefense ai im icq*** on page 282.

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*]

When used with `show`:

show smartdefense ai im yahoo [enforce | log | block-proprietary]

FIELDS

See ***smartdefense ai im icq*** on page 282.

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*]

When used with `show`:

show smartdefense ai p2p bittorrent [**enforce** | **log** | **block-proprietary**]

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`.

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 286.

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*]

When used with `show`:

show smartdefense ai p2p gnutella [enforce | log | block-proprietary]

FIELDS

See ***smartdefense ai p2p bittorrent*** on page 286.

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*]

When used with `show`:

show smartdefense ai p2p kazaa [enforce | log | block-proprietary]

FIELDS

See ***smartdefense ai p2p bittorrent*** on page 286.

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 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 `disabled`.

`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 `disabled`.

`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 NetDefend firewall 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 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 0.

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 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.

SYNTAX

When used with `set`:

set smartdefense network-security ip-icmp cisco-ios [enforce *enforce*] [log *log*] [num-hops *num-hops*] [proto-103 *proto-103*] [proto-53 *proto-53*] [proto-55 *proto-55*] [proto-77 *proto-77*]

When used with `show`:

show smartdefense network-security ip-icmp cisco-ios [enforce | log | num-hops | proto-103 | proto-53 | proto-55 | proto-77]

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-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`.

`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`.

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 NetDefend firewall 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 NetDefend firewall 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 connections 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 NetDefend firewall 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 NetDefend firewall 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 NetDefend firewall will drop packets that fail the UDP length verification check.
- `false` - Do not disable relaxed UDP length verification. The NetDefend firewall 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 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 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 NetDefend 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 size 250
```

EXAMPLE 2

The following command displays all Strict TCP settings:

```
show smartdefense network-security tcp strict-tcp
```

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 NetDefend firewall 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 NetDefend firewall.

`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.

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 NetDefend Portal
- Displaying and exporting SNMP settings

NetDefend firewall users can monitor the NetDefend firewall, 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 NetDefend firewall 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 ssh [mode | iprange | community | location | contact | port]

FIELDS

`mode`

String. Indicates from where SNMP access to the NetDefend 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 NetDefend firewall.

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 NetDefend users to access the NetDefend 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
```

ssh

PURPOSE

The `ssh` variable is used for working with SSH in the following ways:

- Enabling and configuring SSH access to the NetDefend Portal
- Displaying and exporting SSH settings

NetDefend firewall users can control the firewall 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 NetDefend firewall with SSH-based management systems.

Note: The NetDefend firewall 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 NetDefend 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 NetDefend firewall settings can be changed remotely, so it is especially important to make sure all NetDefend firewall 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 NetDefend users to access the NetDefend 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 NetDefend firewall 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 NetDefend firewall should collect traffic data.

The default value is 18000.

EXAMPLE 1

The following command configures the NetDefend firewall to collect traffic data every 2 minutes:

```
set statistics interval 7200
```

Example 2

The following command displays the Traffic Monitor settings:

```
show statistics
```

syslog

PURPOSE

The `syslog` variable is used for working with NetDefend firewall Syslog settings in the following ways:

- Configuring Syslog settings
- Displaying and exporting Syslog settings

You can configure the NetDefend firewall 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 NetDefend firewall 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
```

users

PURPOSE

The `users` variable is used for working with local users in the following ways:

- Adding NetDefend firewall users
- Modifying NetDefend firewall users details
- Deleting NetDefend firewall users
- Displaying and exporting NetDefend firewall users details
- Clearing the Users table

Note: You cannot change the following details for the admin user (user 1):

- Name
- 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*] [**expire** *expire*]

When used with `set`:

set users *number* [**name** *name*] [**password** *password*] [**adminaccess** *adminaccess*] [**vpnaccess** *vpnaccess*] [**filteroverride** *filteroverride*] [**hotspotaccess** *hotspotaccess*] [**expire** *expire*]

When used with `delete`:

delete users *number*

When used with `show`:

show users [*number*] [**adminaccess** | **vpnaccess** | **filteroverride** | **hotspotaccess** | **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 NetDefend Portal. This can have the following values:

- `none` - The user cannot access the NetDefend Portal.
- `readonly` - The user can log on to the NetDefend Portal, but cannot modify system settings.
- `readwrite` - The user can log on to the NetDefend Portal and modify system settings.

The default level is `none`.

`vpnaccess`

String. Indicates whether to allow the user to connect to this NetDefend firewall 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 NetDefend Remote Access VPN Server or internal VPN Server is enabled. See ***vpn externalserver*** on page 361 and ***vpn internalserver*** on page 364.

`filteroverride`

String. Indicates whether to allow the user to override Web Filtering. This can have the following values:

- `true` - The user can override Web Filtering.
- `false` - The user cannot override Web Filtering.

This option only appears if the Web Filtering service is defined. See webfilter mode.

`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 159.

`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 NetDefend firewall.

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 Web Filtering:

```
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
- Deleting VLAN networks
- Displaying and exporting the above VLAN network settings
- Displaying and exporting all VLAN network settings, including VLAN OSPF settings

  For information on configuring, displaying, and exporting specific VLAN OSPF settings, see ***vlan ospf*** on page 357 and ***vlan ospf md5*** on page 359.
- Clearing the VLAN Networks table

Your NetDefend firewall allows you partition your network into several virtual LAN networks (VLANs). A VLAN is a logical network behind the NetDefend firewall. 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 137. For information on the default security policy for VLANs, refer to the User Guide.

The NetDefend firewall 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.

You can define up to ten VLAN networks (port-based and tag-based combined).

SYNTAX

When used with `add`:

add vlan name *name* type *type* [tag *tag*] [address *address*] [netmask *netmask*] [dhcpserver *dhcpserver*] [dhcprange *dhcprange*] [dhcprelayip *dhcprelayip*] [virtualip *virtualip*] [hidenat *hidenat*] [hotspotaccess *hotspotaccess*]

When used with `set`:

set vlan *number* [name *name*] [type *type*] [tag *tag*] [address *address*] [netmask *netmask*] [dhcpserver *dhcpserver*] [dhcprange *dhcprange*] [dhcprelayip *dhcprelayip*] [virtualip *virtualip*] [hidenat *hidenat*] [hotspotaccess *hotspotaccess*]

When used with `delete`:

delete vlan *number*

When used with `show`:

show vlan *number* [**name** | **type** | **tag** | **address** | **netmask** | **dhcpserver** | **dhcprange** | **dhcprelayip** | **virtualip** | **hidenat** | **hotspotaccess**]

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.

`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 port-based VLANs is 0.

`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 NetDefend DHCP server is enabled. This can have the following values:

- `enabled` - The NetDefend DHCP server is enabled.
- `disabled` - The NetDefend DHCP server is disabled.
- `relay` - DHCP relay is enabled.

The default value is `enabled`.

By default, the NetDefend firewall operates as a DHCP server. This allows the NetDefend firewall 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 NetDefend DHCP server, you must disable the NetDefend 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 NetDefend DHCP server, you can configure DHCP relay. When in DHCP relay mode, the NetDefend firewall 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 NetDefend DHCP server automatically sets the DHCP address range.
- A DHCP address range - Relevant only if the NetDefend DHCP server is enabled.
  To specify a range, use the following format:
  `<Start IP Address>-<End IP Address>`

The default value is `automatic`.

`dhcprelayip`

IP Address. The IP address of the desired relay DHCP server. This can have the following values:

- An IP address
- `undefined` - No relay DHCP 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 148.

`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.

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.

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 sets the tag of the first VLAN network in the VLAN Networks table to 10, and disables the DHCP server:

```
set vlan 1 tag 10 dhcpserver disabled
```

EXAMPLE 3

The following command deletes the first VLAN network in the VLAN Networks table:

```
delete vlan 1
```

EXAMPLE 4

The following command displays the DHCP range of the first VLAN in the VLAN Networks table:

```
show vlan 1 dhcprange
```

EXAMPLE 5

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 cost 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 md5*** on page 359.

This variable is only relevant if OSPF is enabled. For information, see ***ospf*** on page 231.

SYNTAX

When used with `set`:

set vlan *number* **ospf cost** *cost*

When used with `show`:

show vlan *number* **ospf** [**cost**]

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.

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 md5

PURPOSE

The `vlan ospf md5` variable is used for working with OSPF MD5 authentication settings for VLAN networks in the following ways:

- Configuring OSPF MD5 authentication settings for the VLAN
- Displaying and exporting OSPF MD5 authentication settings for the VLAN

This variable is only relevant if OSPF is enabled. For information, see ***ospf*** on page 231.

SYNTAX

When used with `set`:

set vlan *number* ospf md5 [enabled *enabled*] [key *key*] [password *password*]

When used with `show`:

show vlan *number* ospf md5 [enabled | key | password]

FIELDS

`number` Integer. The VLAN network's row in the VLAN table.

`enabled` String. Indicates whether to use the MD5 authentication scheme for OSPF connections. This can have the following values:

- `true` - Use the MD5 authentication scheme.
- `false` - Do not use the MD5 authentication scheme.

The default value is `disabled`.

`key` Integer. The key ID to use for authentication.

`password`

String. The password to use for authentication.

Passwords need not be the identical throughout an OSPF area, but they must be the same for OSPF neighbors.

EXAMPLE 1

The following command enables authentication for OSPF connections for VLAN network 1:

```
set vlan 1 ospf md5 enabled true key 1 password thepassword
```

EXAMPLE 2

The following command displays the OSPF MD5 authentication settings for VLAN network 1:

```
show vlan 1 ospf md5
```

vpn externalserver

PURPOSE

The `vpn externalserver` variable is used for doing the following:

- Configuring the NetDefend Remote Access VPN Server
- Displaying and exporting NetDefend Remote Access VPN Server settings

You can set up your NetDefend firewall as a 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 SecuRemote or a via NetDefend firewall in Remote Access VPN mode.

Note: The Check Point SecuRemote Remote Access VPN Client can be downloaded for free via the NetDefend Portal. For instructions, refer to the User Guide.

Note: After you have set up the Remote Access VPN Server, you can grant users permission to access your network via VPN. For information, see ***users*** on page 345.

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 Remote Access VPN Server mode. This can have the following values:

- `enabled` - The NetDefend Remote Access VPN Server is enabled.
- `disabled` - The NetDefend Remote Access VPN Server is disabled.

The default value is `disabled`.

Note: Disabling the 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 connecting from the Internet to bypass the firewall and access your internal network without restriction. This can have the following values:

- `enabled` - Authenticated users connecting from the Internet can bypass the firewall.
- `disabled` - Authenticated users connecting from the Internet cannot bypass the firewall.

The default value is `disabled`.

EXAMPLE 1

The following command enables the Remote Access VPN Server and specifies that authenticated users should be allowed to bypass NAT, but not the firewall:

```
set vpn externalserver mode enabled bypassnat enabled bypassfw
disabled
```

EXAMPLE 2

The following command displays the Remote Access VPN Server Bypass NAT settings:

```
show vpn externalserver bypassnat
```

vpn internalserver

PURPOSE

The `vpn internalserver` variable is used for doing the following:

- Configuring the NetDefend internal VPN Server
- Displaying and exporting NetDefend internal VPN Server settings

You can make your network available to authorized users connecting from your internal networks, by setting up your NetDefend firewall as an internal VPN Server. Users can connect to the Remote Access VPN Server via Check Point SecuRemote or a via NetDefend firewall 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 internal VPN Server, refer to the User Guide.

Note: The Check Point SecuRemote Remote Access VPN Client can be downloaded for free via the NetDefend Portal. For instructions, refer to the User Guide.

Note: After you have set up the internal VPN Server, you can grant users permission to access your network via VPN. For information, see ***users*** on page 345.

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 internal VPN Server mode. This can have the following values:

- `enabled` - The NetDefend internal VPN Server is enabled.
- `disabled` - The NetDefend 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 firewall and access your internal network without restriction. This can have the following values:

- `enabled` - Authenticated users connecting from internal networks can bypass the firewall.
- `disabled` - Authenticated users connecting from internal networks cannot bypass the firewall.

The default value is `disabled`.

Example 1

The following command enables the internal VPN Server and specifies that authenticated users should be allowed to bypass NAT, but not the firewall:

```
set vpn internalserver mode enabled bypassfw disabled
```

Example 2

The following command displays the internal VPN Server Bypass Firewall settings:

```
show vpn internalserver bypassfw
```

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 settings

  For information on configuring, displaying, and exporting specific VPN site OSPF settings, see ***vpn sites ospf*** on page 378 and ***vpn sites ospf md5*** on page 380.

- 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* [disabled *disabled*] [gateway2 *gateway2*] [loginmode *loginmode*] [configmode *configmode*] [authmethod *authmethod*] [keepalive *keepalive*] [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*] [vtilocalip *vtilocalip*] [vtiremoteip *vtiremoteip*]

When used with `set`:

set vpn sites [*number*] [name *name*] [type *type*] [gateway *gateway*] [disabled *disabled*] [gateway2 *gateway2*] [loginmode *loginmode*] [configmode *configmode*] [authmethod *authmethod*] [keepalive *keepalive*] [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*] [vtilocalip *vtilocalip*] [vtiremoteip *vtiremoteip*]

When used with `delete`:

delete vpn sites *number*

When used with `show`:

show vpn sites [*number*] [name | type | gateway | disabled | gateway2 | loginmode | configmode | authmethod | keepalive | bypassnat | bypassfw | user | password | topopass | servicename | net1 | netmask1 | net2 | netmask2 | net3 | netmask3 | usepfs | phase1ikealgs | phase1exptime | phase1dhgroup | phase2ikealgs | phase2exptime | phase2dhgroup | dnsname | 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.

`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 is enabled.

The default value is `false`.

You can only connect to VPN sites that are enabled.

`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`.

`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 NetDefend firewall 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 NetDefend 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 231. For information on configuring the VPN site's OSPF settings, see ***vpn sites ospf*** on page 378 and ***vpn sites ospf md5*** on page 380.
  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.`

`keepalive`

String. Indicates whether to keep the tunnel to the VPN site alive even if there is no network traffic between the NetDefend firewall and the VPN site. 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.`

This field is only relevant for Site-to-Site VPNs.

`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 firewall and access your internal network without restriction. This can have the following values:

- `enabled` - The VPN site can bypass the firewall.
- `disabled` - The VPN site cannot bypass the firewall.

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 be used 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 addresses 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 NetDefend firewall 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 NetDefend firewall 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 NetDefend firewall 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 NetDefend firewall 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 NetDefend firewall resolves the DNS name to the IP address.

`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 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 cost 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 md5*** on page 380.

This variable is only relevant if OSPF is enabled and the VPN site is route-based. For information on configuring OSPF, see ***ospf*** on page 231. For information on configuring route-based VPNs, see ***vpn sites*** on page 366.

SYNTAX

When used with `set`:

set vpn sites *number* ospf cost *cost*

When used with `show`:

show vpn sites *number* ospf [cost]

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.

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 md5

PURPOSE

The `vpn sites ospf md5` variable is used for working with OSPF MD5 authentication settings for VPN sites in the following ways:

- Configuring OSPF MD5 authentication settings for the VPN site
- Displaying and exporting OSPF MD5 authentication settings for the VPN site

This variable is only relevant if OSPF is enabled and the VPN site is route-based. For information on configuring OSPF, see ***ospf*** on page 231. For information on configuring route-based VPNs, see ***vpn sites*** on page 366.

SYNTAX

When used with `set`:

set vpn sites *number* ospf md5 [enabled *enabled*] [key *key*] [password *password*]

When used with `show`:

show vpn sites *number* ospf md5 [enabled | key | password]

FIELDS

`number`	Integer. The VPN site's row in the VPN Sites table.
`enabled`	String. Indicates whether to use the MD5 authentication scheme for OSPF connections. This can have the following values: • `true` - Use the MD5 authentication scheme. • `false` - Do not use the MD5 authentication scheme. The default value is `disabled`.
`key`	Integer. The MD5 key ID to use for authentication.

`password`	String. The MD5 password to use for authentication.

EXAMPLE 1

The following command enables authentication for OSPF connections for VPN site 1:

```
set vpn sites 1 ospf md5 enabled true key 1 password thepassword
```

EXAMPLE 2

The following command displays the OSPF MD5 authentication settings for VPN site 1:

```
show vpn sites 1 ospf md5
```

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 385. For information on displaying and exporting specific advanced options, see ***vstream options*** on page 388. For information on displaying and exporting specific policy rules, see ***vstream policy rule*** on page 392.

The NetDefend firewall 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 NetDefend 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 164.

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*]

When used with `show`:

show vstream options [unsafe-attachments | safe-filetypes | http-ranges]

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`.

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*]

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*]

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]

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 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 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 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 `true`.

`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`.

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 action allow 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 action 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

PURPOSE

The `webfilter` variable is used for working with the Web Filtering service in the following ways:

- Enabling/disabling the Web Filtering service
- Displaying and exporting all Web Filtering service settings, including:
  - Web Filtering mode
  - Web Filtering category settings

  For information on displaying and exporting specific Web Filtering category settings, see ***webfilter categories*** on page 402.

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 the administrator password via the **Web Filtering** pop-up window.

Note: Web Filtering is only available if you are connected to a Service Center and subscribed to this service.

Note: If you are remotely managed, contact your Service Center to change these settings.

For information on temporarily disabling the Web Filtering service, refer to the User Guide.

SYNTAX

When used with `set`:

set webfilter mode *mode*

When used with `show`:

show webfilter [**mode**]

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`.

EXAMPLE 1

The following command enables the Web Filtering service:

```
set webfilter mode enabled
```

EXAMPLE 2

The following command displays all Web Filtering service settings, including the service mode and the categories for which the service is enabled:

```
show webfilter
```

See ***webfilter categories*** on page 402 for information about Web Filtering categories.

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.

Note: Web Filtering is only available if you are connected to a Service Center and subscribed to this service.

Note: If you are remotely managed, contact your Service Center to change these settings.

SYNTAX

When used with `set`:

set webfilter categories [gambling *gambling*] [adult *adult*] [criminal *criminal*] [hate *hate*] [violence *violence*] [drugs *drugs*] [unknown *unknown*]

When used with `show`:

show webfilter categories [gambling | adult | criminal | hate | violence | drugs | unknown]

Fields

`gambling/`
`adult/`
`criminal/`
`hate/`
`violence/`
`drugs`

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`.

`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
```

wireless

PURPOSE

The `wireless` variable is used for working with wireless connection settings in the following ways:

- Configuring your NetDefend firewall's wireless connection settings, including:
    - The WLAN network's SSID, country, operation mode, and channel
    - The security protocol
    - Advanced security settings
    - Wireless transmitter settings
- Displaying and exporting the above wireless connection settings
- Displaying and exporting all wireless connection settings, including the WEP and WPA-PSK settings.

  For information on configuring, displaying, and exporting WEP settings, see ***wireless wep*** on page 416. For information on configuring, displaying, and exporting WPA2 settings, see ***wireless wpa*** on page 419. For information on configuring, displaying, and exporting WPA-PSK settings, see ***wireless wpapsk*** on page 421.

For information on enabling and configuring the WLAN network, see ***net wlan*** on page 219.

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

SYNTAX

When used with `set`:

set wireless [netname *netname*] [hidenetname *hidenetname*] [country *country*] [opmode *opmode*] [macfilter *macfilter*] [xr *xr*] [wmm *wmm*] [channel *channel*] [xmitpower *xmitpower*] [datarate *datarate*] [fragthreshold *fragthreshold*] [rtsthreshold *rtsthreshold*] [antenna *antenna*] [security *security*] [groupkeyupdateinterval *groupkeyupdateinterval*]

When used with `show`:

show wireless [netname | hidenetname | country | opmode | macfilter | xr | wmm | channel | xmitpower | datarate | fragthreshold | rtsthreshold | security | antenna | groupkeyupdateinterval]

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 using the wireless network discovery features of some products, such as Microsoft Windows XP, 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.

`country`

String. The country code of the country in which you are located. For a list of country codes, see ***Country Codes*** on page 423.

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.
- `108g-static` - Operates in the 2.4 GHz range, and offers a maximum theoretical rate of 108 Mbps. When using this mode, only 802.11g Super stations will be able to connect.
- `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.

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.

`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 226.
- `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.

`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.

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`.

`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 NetDefend firewall 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`.

`channel`

Integer or String. The radio frequency to use for the wireless connection. This can have the following values:

- `auto` - The NetDefend firewall 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.

`datarate`

Integer or String. The transmission rate. This can have the following values:

- `auto` - The NetDefend firewall automatically selects a rate.
- A specific rate: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54, 72, 96, or 108

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.

`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.

NetDefend firewalls 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 NetDefend firewall 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.

`security`

String. The security protocol to use. This can have the following values:

- `none`
- `wep`
- `802.1x`
- `wpa`
- `wpapsk`

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 ***wireless wep*** on page 416. The wireless stations must be configured with the same key as well.

If you choose `wpapsk`, you must configure a passphrase. For information on configuring the passphrase, see ***wireless wpapsk*** on page 421. The wireless stations must be configured with this passphrase as well.

`groupkeyupdateinterval`

Integer. The interval (in seconds) between periodic WPA and WPA-PSK key changes.

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-PSK.

```
set wireless netname MyOffice hidenetname yes security wpapsk
```

EXAMPLE 2

The following command displays the wireless connection's operation mode:

```
show wireless opmode
```

wireless wep

PURPOSE

The `wireless wep` variable is used for working with WEP settings in the following ways:

- Configuring WEP keys
- Displaying and exporting WEP keys

This variable is only relevant when a WLAN network is configured, and the selected security protocol is WEP. For information on enabling and configuring the WLAN network, see ***net wlan*** on page 219. For information on setting the security protocol, see ***wireless*** on page 404.

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

SYNTAX

When used with `set`:

set wireless wep [defkey *defkey*] [key1 *key1*] [key2 *key2*] [key3 *key3*] [key4 *key4*]

When used with `show`:

show 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 wireless wep defkey 2 key1 4FC0046169 key2 D8462C0BA9
```

EXAMPLE 2

The following command displays the WEP settings:

```
show wireless wep
```

wireless wpa

PURPOSE

The `wireless wpa` variable is used for working with WPA2 settings in the following ways:

- Configuring the WPA2 settings
- Displaying and exporting WPA2 settings

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 or WPA-PSK security methods, the NetDefend enables you to restrict access to the WLAN network to wireless stations that support the WPA2 security method.

This variable is only relevant when a WLAN network is configured, and the selected security protocol is WPA or WPA-PSK. For information on enabling and configuring the WLAN network, see ***net wlan*** on page 219. For information on setting the security protocol, see ***wireless*** on page 404.

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

SYNTAX

When used with `set`:

set wireless wpa wpa2only *wpa2only*

When used with `show`:

show wireless wpa [wpa2only]

FIELDS

`wpa2only`

String. Indicates whether wireless stations should be required to connect using WPA2 only. This can have the following values:

- `yes` - Only wireless stations using WPA2 can access the WLAN network.
- `no` - Wireless stations using either WPA or WPA2 can access the WLAN network.

The default value is `no`.

EXAMPLE 1

The following command configures the WLAN to allow only wireless station using WPA2 to connect:

```
set wireless wpa wpa2only yes
```

EXAMPLE 2

The following command displays the WPA2 settings:

```
show wireless wpa
```

wireless wpapsk

Purpose

The `wireless wpapsk` variable is used for working with WPA-PSK settings in the following ways:

- Configuring the WPA-PSK passphrase
- Displaying and exporting the WPA-PSK passphrase

This variable is only relevant when a WLAN network is configured, and the selected security protocol is WPA-PSK. For information on enabling and configuring the WLAN network, see ***net wlan*** on page 219. For information on setting the security protocol, see ***wireless*** on page 404.

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

Syntax

When used with `set`:

set wireless wpapsk passphrase *passphrase*

When used with `show`:

show 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-PSK passphrase:

```
set wireless wpapsk passphrase D@34462Crf3-4%-ehj
```

Example 2

The following command displays the WPA-PSK passphrase:

```
show wireless wpapsk
```

Chapter 6

Country Codes

Table 3: 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
Bulgaria	BG

Country	Code
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
Germany	DE

Country	Code
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
Latvia	LV

Country	Code
Lebanon	LB
Libya	LY
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	SR
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
Viet Nam	VN
Yemen	YE
Zimbabwe	ZW

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 NetDefend firewall.

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