Command Line Interface Guide

P/N 093-0011-000
Rev C
Version 2.5

Copyright Notice

Licenses, Copyrights, and Trademarks

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a light commercial installation. This equipment generates, uses and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

PRODUCT LICENSE AGREEMENT

PLEASE READ THIS LICENSE AGREEMENT ("AGREEMENTS") CAREFULLY BEFORE USING THIS PRODUCT. BY INSTALLING AND OPERATING, YOU INDICATE YOUR ACCEPTANCE OF THE TERMS OF THIS LEGAL AND BINDING AGREEMENT AND ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PART TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT START THE INSTALLATION PROCESS.

1. License Grant. This is a license, not a sales agreement, between you, the end user, and NetScreen Technologies, Inc. ("NetScreen"). The term "Firmware" includes all NetScreen and third party Firmware provided to you with the NetScreen product, and includes any accompanying documentation, any updates and enhancements of the Firmware provided to you by NetScreen, at its option. NetScreen grants to you a non-transferable (except as provided in section 3 ("Transfer") below, non-exclusive license to use the Firmware in accordance with the terms set forth in this License Agreement. The Firmware is "in use" on the product when it is loaded into temporary memory (i.e. RAM)

2. Limitation on Use. You may not attempt and if you are a corporation, you will use best efforts to prevent your employees and contractors from attempting to, (a) modify, translate, reverse engineer decompile, disassemble, create, derivative works based on, sublicense, or distribute the Firmware or the accompanying documentation; (b) rent or lease any rights in the Firmware or accompanying documentation in any form to any person; or (c) remove any proprietary notice, labels, or marks on the Firmware, documentation, and containers.

3. Transfer. You may transfer (not rent or lease) the Firmware to the end user on a permanent basis, provided that: (I) the end user receives a copy of this Agreement and agrees in writing to be bound by its terms and conditions, and (ii) you at all times comply with all applicable United States export control laws and regulations.

4. Proprietary Rights. All rights, title, interest, and all copyrights to the Firmware, documentation, and any copy made by you remain with NetScreen. You acknowledge that no title to the intellectual property in the Firmware is transferred to you and you will not acquire any rights to the Firmware except for the license as expressly set forth herein.

5. Term and Termination. The term of the license is for the duration of NetScreen's copyright in the Firmware. NetScreen may terminate this Agreement immediately without notice if you breach or fail to comply with any of the terms and conditions of this Agreement. You agree that, upon such termination, you will either destroy all copies of the documentation or return all materials to NetScreen. The provisions of this Agreement, other than the license granted in Section 1 ("License Grant") shall survive termination.

Limited Warranty. For a period of one (1) year after delivery to Customer, NetScreen will repair or replace any defective product shipped to Customer, provided it is returned to Netscreen at Customer's expense within that period. For a period of ninety (90) days after the initial delivery of a particular product, NetScreen warrants to Customer that such product will substantially conform with NetScreen's published specifications for that product if properly used in accordance with the procedures described in documentation supplied by NetScreen. NetScreen's exclusive obligation with respect to non-conforming product shall be, at NetScreen's option, to replace the product or use diligent efforts to provide Customer with a correction of the defect, or to refund to customer the purchase price paid for the unit. Defects in the product will be

reported to NetScreen in a form and with supporting information reasonably requested by NetScreen to enable it to verify, diagnose, and correct the defect. for returned product, the customer shall notify NetScreen of any nonconforming product during the warranty period, obtain a return authorization for the nonconforming product, from NetScreen, and return the nonconforming product to NetScreen's factory of origin with a statement describing the nonconformance.

NOTWITHSTANDING ANYTHING HERIN TO THE CONTRARY, THE FOREGOING IS CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR BREACH OF WARRANTY BY NETSCREEN WITH RESPECT TO THE PRODUCT.

The warranties set forth above shall not apply to any Product or Hardware which has been modified, repaired or altered, except by NetScreen, or which has not been maintained in accordance with any handling or operating instructions supplied by NetScreen, or which has been subjected to unusual physical or electrical stress, misuse, abuse, negligence or accidents.

THE FOREGOING WARRANTIES ARE THE SOLE AND EXCLUSIVE WARRANTIES EXPRESS OR IMPLIED GIVEN BY NETSCREEN IN CONNECTION WITH THE PRODUCT AND HARDWARE, AND NETSCREEN DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. NETSCREEN DOES NOT PROMISE THAT THE PRODUCT IS ERROR-FREE OR WILL OPERATE WITHOUT INTERRUPTION.

7. Limitation of Liability. IN NO EVENT SHALL NETSCREEN OR ITS LICENSORS BE LIABLE UNDER ANY THEORY FOR ANY INDIRECT, INCIDENTAL, COLLATERAL, EXEMPLARY, CONSEQUENTIAL OR SPECIAL DAMAGES OR LOSSES SUFFERED BY YOU OR ANY THIRD PARTY, INCLUDING WITHOUT LIMITATION LOSS OF USE, PROFITS, GOODWILL, SAVINGS, LOSS OF DATA, DATA FILES OR PROGRAMS THAT MAY HAVE BEEN STORED BY ANY USER OF THE FIRMWARE. IN NO EVENT WILL NETSCREEN'S OR ITS LICENSORS' AGGREGATE LIABILITY CLAIM BY YOU, OR ANYONE CLAIMING THROUGH OR ON BEHALF OF YOU, EXCEED THE ACTUAL AMOUNT PAID BY YOU TO NETSCREEN FOR FIRMWARE. Some jurisdictions do not allow the exclusions and limitations of incidental, consequential or special damages, so the above exclusions and limitations may not apply to you.

8. Export Law Assurance. You understand that the Firmware is subject to export control laws and regulations. YOU MAY NOT DOWNLOAD OR OTHERWISE EXPORT OR RE-EXPORT THE FIRMWARE OR ANY UNDERLYING INFORMATION OR TECHNOLOGY EXCEPT IN FULL COMPLIANCE WITH ALL UNITED STATES AND OTHER APPLICABLE LAWS AND REGULATIONS.

9. U.S. Government Restricted Rights. If this Product is being acquired by the U.S. Government, the Product and related documentation is commercial computer Product and documentation developed exclusively at private expense, and (a) if acquired by or on behalf of civilian agency, shall be subject to the terms of this computer Firmware, and (b) if acquired by or on behalf of units of the Department of Defense ("Odd") shall be subject to terms of this commercial computer Firmware license Supplement and its successors.

Table of Contents

Preface

The *Command Line Interface Guide* describes the commands needed to configure and manage a NetScreen device from a console interface. The Command Line Interface Guide is an ongoing publication, published several times a year.

Note: *Screen OS will soon support the NetScreen-1000 in an upcoming release. Inclusion of NetScreen-1000 commands in this manual anticipates that release.*

WHO SHOULD READ THIS MANUAL?

This document is for system and network administrators who already have experience configuring a NetScreen device using the Web interface. Using a command line interface requires familiarity with command syntax, arguments, and variables, as there is no "friendly" interface to guide you. Only experienced users should configure a NetScreen device using the console or Telnet.

The command line interface provides more detailed system information than the Web interface, and hence is very useful for troubleshooting purposes.

ORGANIZATION

The NetScreen Command Line Reference Guide is organized into the following chapters:

Chapter 1, "Getting Started" on page 1-1 provides an introduction and instructions on how to connect a PC to the NetScreen device. It also provides a summary of the commands in this book.

Chapter 2, "Set and Unset Commands" on page 2-1 describes each command available for configuring the NetScreen device.

Chapter 3, "Get Commands" on page 3-1 describes the commands you use to display system configuration parameters and data.

Chapter 4, "Clear Commands" on page 4-1 describes the commands you use to remove or clear the data collected in various tables, buffers, and memory.

Chapter 5, "Miscellaneous Commands" on page 5-1 includes descriptions for the commands that do not fit into any other category.

RELATED PUBLICATIONS

These publications provide information on how to configure NetScreen devices using the Web interface:

NetScreen-5 User's Guide P/N 093-0007-000

NetScreen-10/100 User's Guide P/N 093-0002-000

NetScreen-1000 User's Guide P/N 093-0012-000

This publication describes the NetScreen-Global Manager software application, which allows you to manage and configure many NetScreen devices from a central location:

NetScreen-Global Manager User's Guide P/N 093-0015-000

Getting Started 1

This chapter provides information on how to connect a PC (Personal Computer) to the NetScreen device so that you can use a console (the command line interface) to configure the device.

Use any software that emulates a VT100 terminal to configure the NetScreen device. The terminal emulator allows you to configure the NetScreen device using a console from any operating system, including Windows™, UNIX™, LINUX™, or Macintosh™.

If you are configuring the NetScreen device from a remote location, use Telnet to access the console.

In this guide, the examples display the results from an IBM-compatible PC running the Windows operating system.

Before You Begin

Gain access to the NetScreen device you wish to configure, and obtain these items before you start setup:

- a PC to connect to the NetScreen device
- an RS-232 male-to-female serial cable
- a copy of Microsoft's Hyperterminal software, available on the PC

  If you are using a different operating system, you need a VT100 terminal emulator on that system.

To communicate with the NetScreen device using a console, use a 9600 Baud rate, 8 bits, no parity, 1 stop-bit, and no flow control.

Connect the NetScreen Device to the PC

You do not have to power off the PC or the NetScreen device, nor close any running applications on the PC before connecting it to the NetScreen device.

To connect the NetScreen device to the PC:

1. Connect the female end of the RS-232 cable to the serial port on the PC.
2. Connect the male end of the RS-232 cable to the serial port on the NetScreen device. This port is labeled “Diagnostics.”

Starting the Terminal Emulator

To start the terminal emulator and open a console window:

1. Click **Start**, highlight **Programs**, highlight **Accessories**, highlight **Communications**, and click **HyperTerminal**.

   The HyperTerminal window opens.

2. Double-click the **Hypertrm.exe** icon to open a console window.
3. Click **Enter** to see the login prompt.
4. At the login prompt, enter **netscreen**.
5. At the password prompt, enter **netscreen**.

Note: *If you changed the user name and password for the NetScreen device, enter these at the console prompt instead of the defaults.*

Conventions

These conventions apply to all NetScreen commands:

- To remove a single character, press BACKSPACE or CTRL+H.
- To remove an entire line, press CTRL+U.
- To traverse up to 16 lines forward in the command history buffer, press CTRL+F or the DOWN ARROW key.

Important: *To use the arrow keys for navigating among commands in a Telnet session on Windows 95, 98, NT, or 2000: On the Terminal menu, click* ***Preferences...****, select the* ***VT100 Arrows*** *check box, and click the* ***OK*** *button.*

- To traverse up to 16 lines backward in the command history buffer, press CTRL+B or the UP ARROW key.
- To see the next available keyword or input, and a brief description of usage, type a question mark (?).
- A parameter inside [ ] (square brackets) is optional.
- A parameter inside { } (braces) is required.
- Anything inside < > is a variable.
- If there is more than one choice for a parameter inside [ ] and { }, they are separated by *a pipe* (|). For example, [auth {md5 | sha-1}] means "choose either MD5 or SHA-1 as your authentication method."
- IP addresses are represented by <a.b.c.d> and <w.x.y.z>.
- A subnet mask is represented by <A.B.C.D>.
- The console times out and the connection is broken if no keyboard activity is detected for 10 minutes.
- Items you enter into the system appear in **bold** text.

Command Summary

NetScreen device commands are grouped into four categories: Set and Unset, Get, Clear, and Miscellaneous.

Set and Unset Commands

Use the Set commands to define system parameters. The Set commands are saved in non-volatile memory.

Each Set command has a counterpart Unset command to remove the parameters or to restore the NetScreen device to its default parameters.

Table 1-1 Summary of Set and Unset Commands

Command and Page	Supported on These NetScreen Device Models
address on page 2-2	All models
admin on page 2-4	All models
arp on page 2-9	All models

Table 1-1 Summary of Set and Unset Commands (continued)

Command and Page	Supported on These NetScreen Device Models
auth on page 2-11	All models
clock on page 2-14	All models
console on page 2-16	All models
dbuf on page 2-18	All models
dhcp client on page 2-20	NetScreen-5 at version 1.65 or later
dhcp server on page 2-22	NetScreen-5 at version 1.65 or later
dialup-group on page 2-25	All models
dip on page 2-27	All models
domain on page 2-30	All models
dns on page 2-29	All models
envar on page 2-31	All models except the NetScreen-5
ffilter on page 2-32	All models
firewall on page 2-34	All models
flow on page 2-39	NetScreen-1000
ftp data-port any on page 2-41	All models at version 1.66 or later
global on page 2-42	All models (future release for the NetScreen-1000)
global-pro on page 2-46	NetScreen-5, -10, and -100
group on page 2-49	All models at version 2.0 or later
hostname on page 2-60	All models
ha on page 2-53	NetScreen-100 and NetScreen-1000
ike on page 2-62	All models
interface on page 2-71	All models
ippool on page 2-79	All models
mip on page 2-81	All models
ntp on page 2-83	NetScreen-5 at version 1.65 or later
pki on page 2-85	All models at version 2.0 or later
policy on page 2-89	All models
pppoe on page 2-94	NetScreen-5

Table 1-1 Summary of Set and Unset Commands (continued)

Command and Page	Supported on These NetScreen Device Models
route on page 2-96	All models
scheduler on page 2-98	All models
scs on page 2-101	NetScreen-100 and NetScreen-1000 (future release)
service on page 2-102	All models
snmp on page 2-105	All models
ssl on page 2-110	All models
syn-threshold on page 2-108	All models
syslog on page 2-111	All models
timer on page 2-115	NetScreen-5, NetScreen-10, and NetScreen-100 only
traffic-shaping mode on page 2-116	All models
udp-threshold on page 2-117	NetScreen-1000
url on page 2-118	All models
user on page 2-120	All models
vip on page 2-124	All models; load balancing on NetScreen-100 and NetScreen-1000 only
vsys on page 2-132	NetScreen-1000
vlan on page 2-127	NetScreen-1000
vpn on page 2-128	All models with some exceptions

Get Commands

Use Get commands to display system configuration parameters and data.

Table 1-2 Summary of Get Commands

Command and Page	Supported on These NetScreen Device Models
address on page 3-3	All models
admin on page 3-5	All models
active-user on page 3-2	NetScreen-5
alarm on page 3-7	All models except the NetScreen-1000

Table 1-2 Summary of Get Commands (continued)

Command and Page	Supported on These NetScreen Device Models
arp on page 3-12	All models
auth on page 3-13	All models
chassis on page 3-16	NetScreen-1000
clock on page 3-17	All models
config on page 3-18	All models
console on page 3-20	All models
counter on page 3-21	All models
dhcp client on page 3-25	NetScreen-5 and -10 at version 1.65 or later
dhcp server on page 3-26	NetScreen-5 and -10 at version 1.65 or later
dialup-group on page 3-28	All models
dip on page 3-29	All models
domain on page 3-30	All models
envar on page 3-31	All models except the NetScreen-5
file on page 3-32	All models
firewall on page 3-33	All models
global on page 3-34	All models (future release for the NetScreen-1000)
group on page 3-35	All models at version 2.0 or later
hostname on page 3-36	All models
ha on page 3-37	NetScreen-100 and NetScreen-1000
icmp-threshold on page 3-39	NetScreen-1000
ike on page 3-40	All models
interface on page 3-42	All models
ipsweep-threshold on page 3-45	NetScreen-1000
log on page 3-46	All models except the NetScreen-1000
mac-count on page 3-50	NetScreen-1000
mac-learn on page 3-51	All models
memory on page 3-52	NetScreen-1000

Table 1-2 Summary of Get Commands (continued)

Command and Page	Supported on These NetScreen Device Models
mip on page 3-54	All models
mpsess on page 3-53	NetScreen-1000
ntp on page 3-55	NetScreen-5
pki on page 3-56	All models
policy on page 3-58	All models
route on page 3-63	All models
sa on page 3-65	All models
scheduler on page 3-67	All models
service on page 3-69	All models
session on page 3-70	All models
snmp on page 3-72	All models
scs on page 3-68	Future release for the NetScreen-100 and NetScreen-1000
syn-flood on page 3-73	All models
syslog on page 3-74	All models
system on page 3-76	All models
tech-support on page 3-77	All models
timer on page 3-78	NetScreen-5, NetScreen-10, and NetScreen-100 only
traffic-shaping interface on page 3-79	NetScreen-5, NetScreen-10, and NetScreen-100 only.
udp-threshold on page 3-80	NetScreen-1000
url on page 3-81	All models
user on page 3-82	All models
vip on page 3-83	All models
vsys on page 3-84	NetScreen-1000
vlan on page 3-85	NetScreen-1000
vpn on page 3-87	All models

Clear Commands

Use the Clear commands to remove data stored in log tables, remove information stored in memory, and remove information stored on the flash card.

Table 1-3 Summary of Clear Commands

Command and Page	Supported on These NetScreen Device Models
active-user on page 4-2	NetScreen-5
admin on page 4-3	All models
alarm on page 4-4	All models except the NetScreen-1000
arp on page 4-6	All models
auth on page 4-7	All models
counter on page 4-8	All models
dbuf on page 4-9	All models
dhcp on page 4-10	NetScreen-5 and -10 at version 1.65 or later
dns on page 4-11	All models
file on page 4-12	All models
ike cookie on page 4-13	All models
log on page 4-14	All models except the NetScreen-1000
mac-count on page 4-16	NetScreen-1000
mac-learn on page 4-17	All models
node_secret on page 4-18	All models
sa on page 4-20	All models
sa-statistics on page 4-21	All models
session on page 4-22	All models

Miscellaneous Commands

The miscellaneous commands include save, exit, ping, and reset.

Table 1-4 Summary of Miscellaneous Commands

Command and Page	Supported on These NetScreen Device Models
enter vsys on page 5-2	NetScreen-1000
exec dhcp client renew on page 5-4	NetScreen-5
exec dns on page 5-3	All models
exec ha file-sync on page 5-5	NetScreen-100 at version 2.0 or later, and the NetScreen-1000
exec ntp update on page 5-6	NetScreen-5
exec pki on page 5-7	All models except the Netscreen-1000
exit on page 5-10	All models
ping on page 5-11	All models
reset on page 5-12	All models
save on page 5-13	All models
unset all on page 5-20	All models

Set and Unset Commands 2

Use the Set commands to define system parameters. The Set commands are saved in non-volatile memory.

Each Set command has a counterpart Unset command to remove the parameters or to restore the NetScreen device to its default parameters.

address

Description: Use the **set address** command to define an Address Book entry.

Syntax

set address {trust | untrust | dmz} <address_name> {<a.b.c.d> <A.B.C.D>|<domain name>} [<comment>]

unset address {trust | untrust | dmz} <address_name>

Arguments

trust	Specifies the Trust interface.
untrust	Specifies the Untrust interface.
dmz	Specifies the DMZ interface.
<address_name>	Defines the name of the address entry.
a.b.c.d	Defines the IP Address.
A.B.C.D	Defines the subnet mask
<domain name>	Defines the domain name.
[comment <string>]	Use to add comments.

Availability

This feature is supported on all NetScreen device models. However, the argument, “dmz” is not supported on the NetScreen-5 model.

Defaults

There are four system-defined Address Book entries:

- Inside Any – any hosts connected to the Trust interface
- Outside Any – any hosts connected to the Untrust interface
- DMZ Any – any hosts connected to the DMZ interface
- Dial-Up VPN – any dialup hosts to the Untrust interface

Examples

To define an address book entry for a web server named “webserver” with an IP address 184.2.50.9 and a netmask 255.255.255.0 connected to the DMZ interface:

```
ns -> set address dmz webserver 184.2.50.9 255.255.255.255
```

To define an address book entry for a desktop machine named “odie” with an IP address 172.16.10.1 and a netmask 255.255.255.255 connected to the trust interface with a comment of “Mary’s desktop”:

```
ns-> set address trust odie 172.16.10.1 255.255.255.255 Mary’s desktop
```

To delete an address book entry for a partner site named “my-partner” which is connected to the Untrust interface:

```
ns-> unset address untrust my-partner
```

See Also

See the **get address** command.

admin

Description: Use the **set admin** command to configure the administrative parameters for the NetScreen device.

Syntax

set admin {name <name> | password <password>}

set admin user <user_name> password <password> privilege {all | read-only}

set admin manager-ip <a.b.c.d> [<A.B.C.D>]

set admin sys-ip <a.b.c.d>

set admin port <number>

set admin mail {alert | traffic-log | mail-addr1 {<a.b.c.d> | <server_name>} | mail-addr2 {<a.b.c.d> | <server_name>} | server-name {<a.b.c.d> | <server_name>}}

set admin format {dos | unix}

unset admin {name | port | sys-ip | user | password | format}

unset admin manager-ip {<a.b.c.d> | all}

unset admin mail {alert | traffic-log | mail-addr1 | mail-addr2 | server-name}

Arguments

name	The login name of the root user for the NetScreen device. The maximum length of the name is 31 characters, including all symbols except “?.” The name is case-sensitive. Also, the root administrator of a Virtual System issues the **name** command to assign the login name for that Virtual System.
password	The password of the root user of the NetScreen device. The maximum length of the password is 31 characters, including all symbols except “?.” The password is case-sensitive. Also, the root administrator of a Virtual System issues the **name** command to assign the login name for that Virtual System.
user	The login name of non-root users for the NetScreen device. The maximum length of the user name is 31 characters, including all symbols except “?.” The user name is case-sensitive.
privilege	Defines the administrative privilege level: • “all” is for a level-2 user, who can execute all commands except those that modify those of the root user (level 1) or those of other level-2 users. Also, a level-2 user cannot change his or her user name. • “read-only” is for a level-3 user, who can only execute **trace-route**, **exit**, **get**, and **ping** commands.
format {dos | unix}	Applies to all NetScreen devices. Use to select the format the device uses to generate a configuration file. Files can be downloaded via the Web.
manager-ip <a.b.c.d> [<A.B.C.D>]	Use this IP address for the remote system to log in, configure, and manage the NetScreen device. The <a.b.c.d> represents the IP address, and the <A.B.C.D> represents the subnet mask. The default IP address is 0.0.0.0, which allows management from any station. All NetScreen devices allow you to specify up to six hosts or subnets, one at a time.

manager-ip {<a.b.c.d> | <all>}	When using **unset**, specifies one or all of the six possible management IP addresses.
sys-ip	Use this IP address to manage the NetScreen device.
port <number>	Sets the port number for listening for configuration changes when logging on to the Web. Use any number between 0 and 65,535, or use the default port number—80. Changing the admin port number on the NetScreen-5 and -10 requires resetting the device. See the **reset** command on page 5-12.
alert	Collects system alarms from the device for sending to an e-mail address.
mail	Enables e-mail for sending alerts and traffic logs.
mail-addr1 <a.b.c.d> | <server_name>	Sets the first e-mail address for sending alert and traffic logs.
mail-addr2 <a.b.c.d> | <server_name>	Sets a second e-mail address for sending alert and traffic logs.
traffic-log	Collects a log of network traffic handled by the NetScreen device. The traffic log can contain a maximum of 4,096 entries. A copy of the log file is sent to the e-mail addresses specified whenever the log is full or every 24 hours, depending upon which happens first.
server-name <a.b.c.d> | <server_name>	This is the IP address or name of the Simple Mail Transfer Protocol (SMTP) server that receives e-mail notification of system alarms and traffic logs.

Availability

This feature is supported on all NetScreen device models.

Defaults

These are the system defaults:

- The admin name and password are “netscreen.”
- The manager-ip is 0.0.0.0, and the default subnet mask is 255.255.255.255. If no other subnet mask is specified, the system assigns this default.
- The sys-ip is 192.168.1.1 (it is 209.125.148.254 before firmware 1.61).

- The admin port is 80.
- The mail alert is off.
- The mail server-name and the mail addresses are empty strings.

Examples

To change the root administrator user name to paul:

```
ns-> set admin name paul
```

To change the root administrator login password to build4you:

```
ns-> set admin password build4you
```

To assign a level-2 administrator named joe with the password “angel”:

```
ns-> set admin user joe password angel privilege all
```

To generate the configuration file in unix format:

```
ns-> set admin format unix
```

To change the port number for the Web administrative interface to 8000:

```
ns-> set admin port 8000
```

To enable e-mail notification for system alarms:

```
ns-> set admin mail alert
```

To enable e-mail notification of traffic logging:

```
ns-> set admin mail traffic-log
```

To configure john@abc.com as the e-mail address to receive updates on administrative issues:

```
ns-> set admin mail mail-addr1 john@abc.com
```

To specify 209.12.34.100 as the e-mail server to receive administrative e-mail notification:

```
ns-> set admin mail server-ip 209.12.34.100
```

To set the administrator password back to “netscreen”:

```
ns-> unset admin password
```

To disable e-mail notification of system alarms:

```
ns-> unset admin mail alert
```

See Also

See the **get admin** command.

arp

Description: Use the **set arp** command to create an entry in the ARP (Address Resolution Protocol) table.

Syntax

set arp <a.b.c.d> <xxxxyyyyzzzz> {trust | untrust | dmz}

set arp age <seconds>

set arp always-on-dest

set arp no-cache

unset arp <a.b.c.d>

unset arp always-on-dest

Arguments

<a.b.c.d>	Defines the IP address for the machine.
<xxxxyyyyzzzz>	Defines the 48-bit MAC address for the machine.
trust | untrust | dmz	Specifies the interface to which the ARP entry belongs. Each entry stays in the table for 960 seconds, and then is deleted.
age <seconds>	Sets the age-out value (in seconds) for ARP entries.
always-on-dest	For the NetScreen-10 and -100 at version 1.66 and later, and for the NetScreen-1000. This option enables the NetScreen device to send an ARP request to determine a return MAC address for any incoming packet whose heading contains a MAC address not yet listed in the NetScreen MAC address table. This option may be required when packets originate from devices using the Hot Standby Router Protocol/Virtual Router Redundancy Protocol (HSRP/VRRP) or from server load-balancing (SLB) switches.
no-cache	Turns off the cache capability.

Availability

This feature is supported on all NetScreen device models.

Defaults

On the NetScreen-5, -10, and -100 models at version 1.66 and later, and on the NetScreen-1000, the **always-on-dest** option is not enabled by default.

Examples

To create an entry in the ARP table for a machine with IP address 10.1.1.1 and MAC address 00104587bd22 connected to the Trusted interface:

```
ns-> set arp 10.1.1.1 00104587bd22 trust
```

To delete an ARP entry for a Trusted machine with IP address 192.1.9.23 and MAC address 00201034a98c connected to the DMZ interface:

```
ns-> unset arp 192.1.9.23
```

See Also

See the **clear arp** and **get arp** commands.

Notes

The status of the **always-on-dest** can be viewed via the **get arp** command.

auth

Description: Use the **set auth** command to configure the NetScreen device to use a method for user authentication. The four available methods are: a built-in database, a RADIUS server, SecurID, or Lightweight Directory Access Protocol (LDAP).

Syntax

set auth type {0 | 1 | 2 | 3}

set auth secret <string>

set auth server-name {<a.b.c.d> | <server_name_string>}

set auth securid {auth-port <number> | duress <number> | encr <number> | retries <number> | timeout <number> | master {<a.b.c.d> | <server_name_string>} | slave {<a.b.c.d> | <server_name_string>}}

set auth ldap server-name {{<a.b.c.d> | <server_name_string>} <port_number> <distinguished_name> <common_name_identifier>}

set auth timeout <number>

unset auth {secret | server-name | securid | ldap | timeout | type {0 | 1 | 2 | 3}}

Arguments

type <auth-type>	Specifies the type of authentication to use, where <auth-type> is a number: “0” for the built-in NetScreen database, “1” for a RADIUS server, “2” for SecurID, and “3” for a LDAP server.
secret <string>	Defines the password shared between the NetScreen device and the RADIUS server. It is used to authenticate all transactions between the two devices.
server-name {<a.b.c.d> | <server_name_string>}	Defines the RADIUS server for user authentication and specifies either the server IP address or name.
securid auth-port <number>	Specifies the port number to use for communications with the SecurID server.
securid duress <number>	Specifies whether the SecurID server is licensed to use duress mode or not. For <number>, a “0” defines False, and “1” defines True.
securid encr <number>	Specifies the encryption algorithm for SecurID network traffic. For <number>, a “0” specifies SDI and “1” specifies DES. The default type DES is recommended.
securid retries <number>	Specifies the number of retries allowed for attempting authentication with the SecurID server.
securid timeout <number>	Specifies the length of idle time in minutes before terminating authentication status.
securid master {<a.b.c.d> | <server_name_string>}	Specifies either the IP address or the name for the primary SecurID server.
securid slave {<a.b.c.d> | <server_name_string>}	Specifies either the IP address or the name for the secondary SecurID server.
ldap server-name {<a.b.c.d> | <server_name_string>}	Specifies the IP address or name for the LDAP server.
ldap server-name <port_number>	Specifies the listening port number of the LDAP server.
ldap server-name <distinguished_name>	Specifies the directory path where users are listed in the LDAP server.

ldap server-name <common_name_identifier>	Specifies the user name in the LDAP server directory.
timeout <number>	Specifies the length of idle time in minutes before terminating authentication status. Valid range is from 0-255 minutes.

Availability

This feature is supported on all NetScreen device models.

Defaults

The NetScreen built-in user database is used by default.

The SecurID authentication port is 5500 with DES encryption type. The number of client retries is 3 and timeout is 5 seconds.

The user authentication idle timeout is 10 minutes.

Examples

To define the RADIUS shared secret to “mysecret”:

```
ns-> set auth secret mysecret
```

To specify the SecurID server's IP address as 209.134.22.1 with authentication port 500, and using the Data Encryption Standard (DES) algorithm:

```
ns-> set auth securid master 209.134.22.1 auth-port 500 encr 1
```

To use the built-in user database of the NetScreen device for user authentication:

```
ns-> set auth type 0
```

Notes

When the NetScreen device is using SecurID to authenticate users and is not communicating properly with the ACE server, see the **clear node_secret** command on page 4-18.

See Also

See the **clear auth**, **get auth**, and **clear node_secret** commands.

clock

Description: Use the **set clock** command to set the system time on the NetScreen device.

Syntax

set clock {<mm/dd/yyyy hh:mm> | dst-off | ntp | {zone <number>}

unset clock {dst-off | ntp}

Arguments

<mm/dd/yyyy hh:mm>	Specifies the month, day, and year. Specifies the hour and minutes in the 24-hour time format.
dst-off	Turns off the automatic time adjustment for daylight saving time.
ntp	NetScreen-5 devices at version 1.65 or later; NetScreen-10, -100, and -100p at version 2.0 or later. Configures the device for NTP, Network Time Protocol. NTP is used to synchronize computer clocks in the Internet.
zone <number>	Sets the current time zone offset compared to the GMT standard time. Set the <number> between -12 and 12.

Availability

This feature is supported on all NetScreen device models. The **dst-off** argument is available at version 1.64 and later. The **ntp** argument is available on all NetScreen device models except the NetScreen-1000.

Defaults

The NetScreen device automatically adjusts its system clock for daylight saving time.

Examples

To define the system time as November 3, 2001 at 1:30PM:

```
ns-> set clock 11/03/2001 13:30
```

To turn off daylight saving time:

```
ns-> set clock dst-off
```

See Also

See the **get clock**, **set ntp**, **get ntp**, and **exec ntp** commands.

console

Description: Use the **set console** command to define the console parameters.

Syntax

set console {dbuf | disable}

set console {page | timeout} <number>

unset console {dbuf | disable | page | timeout}

Arguments

dbuf	Stores the console messages in a buffer for later retrieval. The buffer size is 1 Mb for the NetScreen-100, 256 Kb for the NetScreen-10, and 4 Mb for the NetScreen-1000.
disable	Disables access to the console. Two confirmations are required to disable access to the console. Saves the current NetScreen configuration and closes the current login session.
page <number>	Specifies how many lines are displayed per page on the console, where <number> is an integer.
timeout <number>	Determines how much time (in minutes) the device waits before logging out the administrator from the console session if the administrator makes no keyboard entries for that length of time. A value of 0 for <number> means the console never times out.

Availability

This feature is supported on all NetScreen device models.

Defaults

Access to the console is enabled by default.

The console displays 22 lines per page.

The login timeout is set to 10 minutes.

The console messages are sent to the buffer by default.

Examples

To redirect all debugging messages to the buffer:

```
ns-> set console dbuf
```

To disable console access:

```
ns-> set console disable
```

To define 20 lines per page displayed on the console:

```
ns-> set console page 20
```

To define the console timeout value to 40 minutes:

```
ns-> set console timeout 40
```

See Also

See the **get console**, **clear dbuf**, and **get dbuf** commands.

Notes

When the debug mode is enabled on the NetScreen device, all debugging messages are displayed in the console. It may be too much information at once. Use the dbuf parameter to store the messages in a buffer so that you can later retrieve them with the **get dbuf** command.

Enable console access with the **unset disable** command through a Telnet connection.

dbuf

Description: Use the **set dbuf** command to adjust the system buffer size dynamically.

Syntax

set dbuf size <number>

unset dbuf size

Arguments

size <number>	Indicates the size of the system buffer in kilobytes

Availability

This command is supported on all platforms.

Defaults

The default buffer sizes for the various NetScreen devices are:

NetScreen-1000	1024 kilobytes
NetScreen-100p	1024 kilobytes
NetScreen-100	512 kilobytes
NetScreen-10	128 kilobytes
NetScreen-5	32 kilobytes
valid range: 32–4096 kilobytes	

Examples

To change the buffer size to the maximum size allowed:

```
ns-> set dbuf size 4096
```

See Also

See also the **get dbuf info** command.

Notes

The range of value for the buffer size is from 32 to 4096 kilobytes.

dhcp client

Description: First, use the **set interface untrust dhcp** command to define the NetScreen device as a Dynamic Host Configuration Protocol (DHCP) client. Then use the **set dhcp** client command to set the desired parameters. Once configured as a DHCP client, the NetScreen device obtains its IP address for the Untrusted interface from a DHCP server each time it is powered, and renews its IP address as needed.

Syntax

set dhcp client {server <a.b.c.d>| vendor | lease | autoconfig}

unset dhcp client {server | vendor | lease | autoconfig}

Arguments

server <a.b.c.d>	Defines the IP address (a.b.c.d) of the DHCP server from which the NetScreen device obtains its IP address.
vendor	Identifies the manufacturer of the device requesting the IP address.
lease	Defines how long, in minutes, the lease for the IP address lasts. There is no maximum lease time.
autoconfig	Determines whether to load configuration files automatically when an IP address is requested. The DHCP server must have a database of configuration information for the clients it serves.

Availability

This feature is available on NetScreen-5 and -10 devices at version 1.65 or later.

Defaults

The service is “off” (disabled) by default.

The default IP address for the DHCP server is “0.0.0.0.” It means that NetScreen device accepts its IP address from any DHCP server.

The default vendor identification is set to “netscreen-5” or “netscreen-10.”

The default lease time is seven days, which equals 10080 minutes.

The autoconfiguration feature is “off” (disabled) by default.

Examples

To designate a specific DHCP server on the network as the one for the NetScreen device, replace *a.b.c.d* with the IP address of the DHCP server:

```
ns-> set dhcp client server 10.0.0.1
```

Notes

If you have more than one DHCP server on the network and you do not designate which one to use, the NetScreen device obtains its IP address from the first DHCP server it finds.

If the IP address you define for a DHCP server is invalid, the NetScreen device is not able to obtain an IP address for its Untrusted interface, and it will be unable to manage network traffic. Check the Syslog or event log to verify that the DHCP server you designated is correct and is up and running.

See Also

See the **get dhcp client**, **clear dhcp client**, and **exec dhcp client renew** commands.

dhcp server

Description: Use the **set dhcp** server command to enable and configure the NetScreen device for Dynamic Host Configuration Protocol (DHCP).

Syntax

set dhcp server service

set dhcp server ip <a.b.c.d> [to <e.f.g.h> | mac <mac>]

set dhcp server option|lease <minutes>| gateway <a.b.c.d> | netmask <A.B.C.D> | dns1 <a.b.c.d> | dns2 <a.b.c.d> | dns3 <a.b.c.d> | domainname <domain> | smtp <a.b.c.d> | pop3 <a.b.c.d> | news <a.b.c.d> | wins1 <a.b.c.d> | wins2 <a.b.c.d>

unset dhcp server

unset dhcp server service

unset dhcp server option {lease | gateway | netmask | dns1 | dns2 | dns3 | domainname | smtp | pop3 | news | wins1 | wins2}

unset dhcp server ip {all | <a.b.c.d>)

Arguments

server service	Enables the DHCP server.
server ip <a.b.c.d> to <e.f.g.h>	In Dynamic mode, you can define a range of IP addresses to use when the DHCP server is filling client requests. Enter the starting IP address <a.b.c.d> and the ending IP address <e.f.g.h>. The IP pool can include up to 64 entries, and can support up to 255 IP addresses.
server ip <a.b.c.d> mac <mac>	In Reserved mode, the DHCP server assigns a designated IP address to a specific machine. Substitute the IP address of the machine for <a.b.c.d> and substitute the MAC address for the machine for <mac>.
server option lease <minutes>	An IP address supplied by the DHCP server is leased indefinitely, or for a limited amount of time. If the lease is limited, you must specify the limitation in minutes. For an unlimited lease, enter 0 for <minutes>.
server option gateway <a.b.c.d>	Specifies the IP address of the default Trusted gateway used by the clients.
server option netmask <A.B.C.D>	Specifies the Trusted netmask of the default gateway.
server option dns1 <a.b.c.d>	Specifies the IP address of the first Domain Name Server.
server option dns2 <a.b.c.d>	Specifies the IP address of the second Domain Name Server.
server option dns3 <a.b.c.d>	Specifies the IP address of the third Domain Name Server.
server option domainname <domain>	Specifies the registered domain name of the networks.
smtp <a.b.c.d>	Specifies the IP address of the SMTP mail server.
pop3 <a.b.c.d>	Specifies the IP address of the POP3 mail server.
news <a.b.c.d>	Specifies the IP address of the News server.
wins1 <a.b.c.d> **wins2 <a.b.c.d>**	Specifies the IP address of the WINS 1 or WINS 2 server.

Availability

This feature is supported on the NetScreen-5 and -10 at version 1.65 or later.

Defaults

The DHCP server is disabled by default.

Examples

To enable the DHCP server:

```
ns-> set dhcp server service
```

To reserve an IP address for a specific machine:

```
ns-> set dhcp server ip 10.10.10.23 mac aabbccddeeff
```

To assign a range of IP addresses for use in Dynamic mode:

```
ns -> set dhcp server ip 10.10.10.10 to 10.10.10.20
```

See Also

See the **clear dhcp** and **get dhcp** commands.

Notes

The DHCP server is a way for all computers on a network to get their TCP/IP settings from one server. Using DHCP to assign IP addresses ensures that duplicate addresses are not used. If you assign IP addresses manually, keep track of which IP addresses have been used.

Using a DHCP server has a minor impact on performance.

A lease time of 0 means the amount of leased time is unlimited.

Important: *If you unset the first IP address in an IP range, you unset the entire IP range.*

dialup-group

Description: Use the **set dialup-group** command to create a group of remote users.

Syntax

set dialup-group <string> [{+ | -} <string>]

unset dialup-group <string>

Arguments

<string>	Assigns a name to the dialup group.
{+ <string>}	Adds a remote VPN user to the group, where <string> is the name of the user.
{- <string>}	Deletes a remote VPN user from the group, where <string> is the name of the user.

Availability

This feature is supported on all NetScreen device models.

Defaults

None.

Examples

To define a dialup user group called “telecommuters”:

```
ns-> set dialup-group telecommuters
```

To add a remote VPN user named “john-home” to the telecommuters group:

```
ns-> set dialup-group telecommuters + john-home
```

To delete a remote VPN user named “amy-home” from the telecommuters group:

```
ns-> set dialup-group telecommuters - amy-home
```

To delete the telecommuters group:

```
ns-> unset dialup-group telecommuters
```

See Also

See the **get dialup-group** command.

Notes

A dialup-group may contain a maximum of 100 remote dialup users.

An Access Policy for a dialup-group applies to all the members in the group; consequently, all the group members must be the in the same category—either IKE dynamic peers (Auto Key), or VPN dialup users (Manual Key).

dip

Description: Use the **set dip** command to set a range for dynamic IP (DIP) addresses.

Syntax

set dip <a.b.c.d> <A.B.C.D>

set dip <a.b.c.d - e.f.g.h>

modify dip <a.b.c.d> <A.B.C.D > <e.f.g.h>

unset dip <number>

Arguments

set dip <a.b.c.d> <A.B.C.D>	Sets a range of dynamic IP (DIP) addresses starting with IP address <a.b.c.d> for the subnet mask <A.B.C.D>.
set dip <a.b.c.d - e.f.g.h>	Sets a range of DIP addresses starting with IP address <a.b.c.d> and ending with IP address <e.f.g.h>.
modify dip	Use this command to change DIP addresses, range of DIP addresses, and subnet masks.

Availability

This feature is supported on all NetScreen device models.

Defaults

None.

Examples:

To configure a DIP address range from 209.111.24.3 to 209.111.24.10:

```
ns-> set dip 209.111.24.3-209.111.24.10
```

To configure a DIP address 255.255.255.255:

```
ns-> set dip 255.255.255.255
```

See Also

See the **get dip** command.

Notes

An IP address configured for DIP cannot be used for VIP or MIP.

dns

Description: Use the **set dns** command to configure Domain Name Services.

Syntax

set dns {forward | host {<dns1 <a.b.c.d> | dns2 <a.b.c.2> | schedule}}

Arguments

forward	Sets up forward DNS requests.
host	Specifies the DNS host.
schedule	Specifies the time of day to refresh DNS entries.

Availability

This feature is supported on all NetScreen device models.

Examples

To set up a host as the primary DNS server at 172.16.10.101:

```
ns-> set dns host dns1 172.16.10.101
```

To schedule a refresh time at 23:59 each day:

```
ns-> set dns host schedule 23:59
```

See Also

See the **get dns**, **clear dns,** and **exec dns** commands.

domain

Description: Use the **set domain** command to set the domain name of the NetScreen device.

Syntax

set domain <domain-name-string>

Arguments

domain-name-string	Defines the domain name of the NetScreen device.

Availability

This feature is available on all NetScreen device models.

Defaults

None.

Example

To set the domain of the NetScreen-100 to “netscreen”:

```
ns100-> set domain netscreen
```

See Also

See the **get domain** and the **unset domain** commands.

envar

Description: Use the **set envar** command to define the location of the environment variables files.

Syntax

set envar {boot | config} = (slot 1 | 2) {file name}

unset envar {boot | config}

Arguments

boot | config	Specifies either the system image for booting the program or the system configuration.
slot 1 | 2	Available on the NetScreen-1000 only. Defines either PCMCIA slot 1 or 2 in the NetScreen-1000 Auxiliary board.
file name	Defines the location for the system image file or the system configuration file.

Availability

This feature is supported on all NetScreen device models except the NetScreen-5.

Defaults

In the NetScreen-1000, the default slot is slot 1.

Examples

To define the location of the system image for booting as file1 in slot1:

```
ns1000-> set envar boot = slot1:file1
```

To define the location of the system configuration as file2.cfg in slot2:

```
ns100-> set envar config = slot2:file2.cfg
```

See Also

See the **get envar** command.

ffilter

Description: Use the **set ffilter** command to create filters for the debug flow output so that only traffic related to one or a combination of the following is displayed: a specific source IP address, destination IP address, source port, destination port, and IP protocol.

Syntax

set ffilter src-ip <a.b.c.d> [dst-ip <a.b.c.d>] [ip-proto <number>] [src-port <number>] [dst-port <number>]

set ffilter dst-ip <a.b.c.d> [ip-proto <number>] [dst-port <number>] [src-port <number>]

set ffilter {[src-port <number>] [dst-port <number>]}

set ffilter ip-proto <number> [src-port <number>] [dst-port <number>]

unset ffilter

Arguments

src-ip <a.b.c.d>	Defines the source IP address.
dst-ip <a.b.c.d>	Defines the destination IP address.
src-port <number>	Defines the port number for the source IP address. Port numbers range from 0 to 65535.
dst-port <number>	Defines the port number for the destination IP address. Port numbers range from 0 to 65535.
ip-proto <number>	Defines the Assigned Internet Protocol Number, where <number> is a value between 0 and 255.

Availability

This feature is supported on all NetScreen device models.

Defaults

None.

Examples

To create a filter for all traffic from a host with IP address 172.16.10.1:

```
ns-> set ffilter src-ip 172.16.10.1
```

To create a filter for all SMTP traffic designated to a host with IP address 209.114.3.2:

```
ns-> set ffilter dst-ip 209.114.3.2 dst-port 25
```

To set a filter for all packets between the source IP address 172.16.10.88 and destination IP 208.10.9.77:

```
ns-> set ffilter src-ip 172.16.10.88 dst-ip 208.10.9.77
```

To set a filter for all packets with the IP protocol number 17, for the User Datagram Protocol (UDP):

```
ns-> set ffilter ip-proto 17
```

To erase all filter settings:

```
ns-> unset ffilter
```

See Also

See the **get ffilter** command.

Notes

You can add more arguments to an existing debug filter. For example, if you have set a filter for packets between a source IP and a destination IP, you can specify the port numbers for the packets later.

Important: *If you add an argument to a filter that already exists, you are modifying that argument parameter. For example, if you have set a filter to trap IP packets with the IP protocol number "51" and then set a trap for IP packets with the IP protocol number "200," you are actually replacing the "51" trap with the "200" trap. To avoid this, create new filters.*

firewall

Description: Use the **set firewall** command to protect your network against various attacks, and to log dropped packets destined for a NetScreen device.

Syntax

The syntax for version 2.0 (for the NetScreen-5, -10, and -100):

set firewall {addr-sweep | applet | bypass-non-ip | bypass-others-ipsec | default-deny | icmp-flood | ip-spoofing | land | log-self | ping-of-death | port-scan | src-route | syn-attack | tear-drop | udp-flood | winnuke}

unset firewall {addr-sweep | applet | bypass-non-ip | bypass-others-ipsec | default-deny | icmp-flood | ip-spoofing | land | log-self | ping-of-death | port-scan | src-route | syn-attack | tear-drop | udp-flood | winnuke}

The syntax for version 1.7 (for the NetScreen-1000):

set firewall {applet | bypass-others-ipsec | default-deny | icmp-flood [threshold <number>] | ip-spoofing | ip-sweep [threshold <microseconds>] | land | log-self | ping-of-death | port-scan [threshold <number>] | src-route | syn-flood [alarm-threshold <number> | queue-size <number> | timeout <number>] | tear-drop | udp-flood [threshold <number>] | winnuke}

unset firewall {applet | bypass-others-ipsec | default-deny | icmp-flood [threshold] | ip-spoofing | ip-sweep [threshold] | land | log-self | ping-of-death | port-scan [threshold] | src-route | syn-flood [alarm-threshold | queue-size | timeout] | tear-drop | udp-flood [threshold] | winnuke}

Arguments

applet	Blocks all embedded Java and ActiveX applets, DOS .exe files, .dll files, and compressed files of types .zip, .gzip, and .tar.
bypass-non-ip	Available at version 2.0 and later. Allows non-IP traffic, such as IPX, to pass through a NetScreen device in Transparent mode. (ARP is a special case for non-IP traffic. It is always passed, even if this feature is disabled.)
bypass-others-ipsec	Openly passes all ESP (IP protocol 50) traffic through a NetScreen device in Transparent mode.
default-deny	Deny all traffic not specifically allowed by a Network Policy.
icmp-flood	An ICMP flood occurs when ICMP pings are broadcast with the purpose of flooding a system with so much data that it first slows down, and then times out and is disconnected. Detects ICMP floods.
icmp-flood [threshold <number>]	For the NetScreen-1000. Defines the number of Internet Control Message Protocol (ICMP) packets per second allowed to ping the same destination address. The range is 1 to 1,000,000.
ip-spoofing	Spoofing attacks occur when unauthorized agents attempt to bypass the firewall security by imitating valid client IP addresses. Invalidates these false IP address connections.
ip-sweep [threshold <microseconds>]	For the NetScreen-1000. Prevents an IP Sweep attack. This kind of attack occurs when packets are sent with different destination addresses in hopes that one of them will reply, thus uncovering the vulnerable host. You can set the IP Sweep threshold in microseconds between 1 and 1,000,000.
land	Prevents Land attacks. Land attacks occur when spoofed packets are sent with the SYN flag set to a system with any port that is listening. If the packets contain the same destination and source IP address as the sending host, the receiving system hangs or reboots.

log-self	Enables the feature that logs dropped packets and pings destined for the NetScreen device.
ping-of-death	Detects and rejects oversized and irregular packet sizes. The TCP/IP specification requires a specific packet size for datagrams being transmitted. Many ping implementations allow the user to specify a larger packet size if desired, which can trigger a range of adverse system reactions including crashing, freezing, and rebooting.
port-scan	Prevents port scan attacks. Port Scan attacks occur when packets are sent with different port numbers for the purpose of scanning the available services. The attacker hopes that one port will respond.
port-scan [threshold <microseconds>]	For the NetScreen-1000. Defines the port-scan threshold value in microseconds.Valid range is 1 to 1,000,000.
src-route	Blocks all IP traffic that uses Source Route Option. Routing information in an IP header can be altered by an attacker to specify different routing information in the IP header. The attacker can enter a different source than the actual header source. Source Route Option can allow an attacker to enter a network with a fake IP address and have data sent back to his real address.
syn-attack	For the NetScreen-5, -10, and -100. SYN attacks occur when the connecting host continuously sends TCP SYN requests without replying to the corresponding ACK responses. Detects SYN Flood attacks.
syn-flood [alarm-threshold <number>]	For the NetScreen-1000. Defines the number of proxied, half-complete connections per second at which an alarm is entered in the Event Alarm log.
syn-flood [queue-size <number>]	For the NetScreen-1000. Defines the number of proxied connection requests held in the proxied connection queue before the system starts rejecting new connection requests.

syn-flood [timeout <number>]	For the NetScreen-1000. Defines the maximum length of time before a half-completed connection is dropped from the queue. You can set it between 1 and 50 seconds.
tear-drop	Tear Drop attacks occur when TCP packets overlap, rendering Windows 95 machines dead. Intercepts these illegal connection requests, shielding valuable corporate computing resources on the internal network.
udp-flood	UDP flooding occurs when UDP packets are sent with the purpose of slowing down the system to the point that it times out and is disconnected. The rising threshold default value is 1000 packets per second.
udp-flood [threshold <number>]	For the NetScreen-1000. The number of packets allowed per second to the same destination IP address/port pair. When this number is exceeded, an alarm will be generated and subsequent packets will be dropped. The valid range is from 1 to 1,000,000.
winnuke	Detects attacks on Windows NetBios communications.

Availability

This feature is supported on all NetScreen device models.

Defaults

All attack protection arguments are enabled by default, except the **bypass-non-ip**, **bypass-others-ipsec**, **log-self**, and **reply-ident-req** arguments, which are disabled by default.

Default firewall option values for all NetScreen device models are:

SYN Flood Protection Timeout value: 20 seconds Alarm threshold: 1024 SYN packets/second Queue size: 10,240 uncompleted SYN connections (1024 for the NetScreen-5 and-10)	**Port Scan Protection** Threshold: 30,000 microseconds per scan attempting to elicit responses from port numbers
ICMP Flood Protection Threshold: 1000 ICMP packets/second to the same IP address	**IP Sweep Protection** Threshold: 30,000 microseconds per scan attempting to elicit responses from IP addresses
UDP Flood Protection Threshold: 1000 UDP packets/second to the same destination IP address/port pair	

Examples

To enable the default-deny firewall protection:

```
ns-> set firewall default-deny
```

To enable detection of ICMP Flood attacks:

```
ns-> set firewall icmp-flood
```

To disable the ip-spoofing firewall protection:

```
ns-> unset firewall ip-spoofing
```

To disable logging of dropped packets and pings destined for the NetScreen device:

```
ns-> unset firewall log-self
```

See Also

See the **get firewall** and **set syn-alarm**, **set syn-qsize**, **set syn-threshold**, **set syn-timeout** commands.

Notes

Only NetScreen devices running in NAT mode can perform the **ip-spoof** feature.

flow

Description: Use the **set flow** command when the NetScreen device is in Transparent mode to adjust the initial session timeout value and avoid packet fragmentation.

Syntax

set flow {initial-timeout <number> | path-mtu | mac-flooding | tcp-mss}

unset flow {initial-timeout | path-mtu | mac-flooding | tcp-mss}

Arguments

initial-timeout <number>	Defines the length of time in minutes that an initial session is kept in the session table before it is dropped or until a FIN or RST packet is received. The range of time is from 1 to 6 minutes.
path-mtu	Enables path-MTU (maximum transmission unit) discovery. If the NetScreen-1000 receives a packet that must be fragmented, it sends an ICMP packet suggesting a smaller packet size.
mac-flooding	Enables the NetScreen device to pass a packet across the firewall even if its destination MAC address is not in the MAC learning table.
tcp-mss	Enables the TCP-MSS (TCP-Maximum Segment Size) option. The NetScreen device modifies the MSS value in the TCP packet to avoid fragmentation caused by the IPSec operation.

Availability

This feature is available only on the NetScreen-1000.

Defaults

The default initial timeout value is 1 minute.

The MAC-flooding feature is enabled by default.

Examples

To change the length of time that an initial session remains in the session table to 2 minutes:

```
ns1000m-> set flow initial-timeout 2
```

To enable the TCP-MSS feature:

```
ns1000m-> set flow tcp-mss
```

Notes

This command can be configured in any mode, but is active only in Transparent mode.

ftp data-port any

Description: Use the **set ftp data-port any** command to allow FTP services for non-port-20 traffic to negotiate any data port number.

Syntax

set ftp data-port any

unset ftp data-port any

Arguments

None.

Availability

This feature is supported on all NetScreen devices at version 1.66 and later.

Defaults

The default condition is unset.

Example

To enable a NetScreen device to negotiate the data port number for a Quick FTP service:

```
ns-> set ftp data-port any
```

Notes

In the unset condition, a NetScreen device does not recognize certain FTP services that negotiate a data port other than port 20. When this feature is enabled, it allows FTP servers to negotiate dynamically any data port that the FTP server proposes. The session continues to be metered by the stateful inspection monitor.

global

Definition: Use the **set global** command to enable the NetScreen device for NetScreen-Global Manager.

Syntax

set global {enable | config-port <number> | listen <number> | report-port <number> | server-name {<a.b.c.d> | <server_name_string>} | keep-alive <number> | send [[log] [network] [resource] [summary]] | vpn}

unset global {enable | config-port | keep-alive | listen | report-port | send | server-name | vpn}

Arguments

enable	Enables the NetScreen device for remote management with NetScreen-Global Manager software.
config-port <number>	Designates the port number for sending configuration information to the management station.
listen <number>	Designates the port number on the NetScreen device for receiving (listening) for configuration information from the management station.
report-port <number>	Designates the port number for sending out “keep-alive” UDP packets to the management station.
server-name {<a.b.c.d> | <server_name_string}>	Designates the IP address or the server name of the management station.
keep-alive <number>	Specifies how often (in seconds) the NetScreen device sends “keep-alive” UDP packets to affirm its existence to the management station. The range is 5–60 seconds.
send [[log] [network] [resource] [summary]]	Specifies the kind of information that the NetScreen device sends to the management station: • **log:** Event logs, self-deny logs, and traffic logs • **network:** Network activities on the Trusted, Untrusted, and DMZ interfaces • **resource:** CPU, flash card, and memory utilization • **summary:** Traffic summary reports showing the total number of sessions and bytes for the following areas: outbound traffic, inbound traffic, services, Access Policies, and VPNs
vpn	Enables communication between the NetScreen device and the management station using a VPN tunnel.

Availability

This feature is currently supported on the NetScreen-5, -10, and -100, and will be supported in a future release of the NetScreen-1000.

Defaults

The NetScreen-Global Manager feature is disabled by default.

The management station IP address is 0.0.0.0.

The management station configuration (TCP) port is 15397.

The management station reporting (UDP) port is 15397.

The NetScreen device local listening port is 15397.

The default frequency for the keep-alive feature is 10 seconds.

VPN encryption is not enabled.

Examples

To specify the management station IP address to 102.10.1.2:

```
ns-> set global server-name 102.10.1.2
```

To enable the NetScreen-Global Manager feature:

```
ns-> set global enable
```

To change the local listening port to 5001:

```
ns-> set global listen 5001
```

To reset the local listening port back to 15397:

```
ns-> unset global listen
```

See Also

See the **get global** command.

Notes

The Configuration port and the Reporting port are used by the NetScreen device to send information to the management station (the workstation running the NetScreen-Global Manager software). The Local listening port is used by the NetScreen device to receive commands from the management station.

If you change the Configuration Listening port and Reporting Listening port for the management station, you must make corresponding changes for the NetScreen devices managed by the NetScreen-Global Manager software. If you change the Listening port for the NetScreen device, you must make the corresponding change at the management station.

To allow the management station to communicate with the NetScreen device through an IPSec tunnel, enable the VPN Encryption feature with the VPN arguments.

Important: *Before enabling a NetScreen device to be managed by NetScreen- Global Manager software, determine the IP address or the server name for the management station.*

global-pro

Definition: Use the **set global-pro** command to configure the NetScreen device for NetScreen Global-Pro.

Syntax

set global-pro config {primary <a.b.c.d> | secondary <a.b.c.d>} enable report {alarm-attack {enable} | alarm-other {enable} | alarm-traffic {enable} | itf-attack-stat {enable} |itf-hardware-stat {enable} | itf-virtual-stat {enable} | log-config {enable} | log-info {enable} | log-self {enable} | log-traffic {enable} | policy-stat {enable} | proto-dist {enable | user-service <name> {ah | esp | gre | icmp | ospf | tcp | udp <low-high>}}

Arguments

config	Configures the Global-Pro Manager on the primary or secondary server.
primary <a.b.c.d>	Specifies the IP address of the primary server.
secondary <a.b.c.d>	Specifies the IP address of the secondary server.
enable	Enables the NetScreen device for remote management with NetScreen-Global Manager software.
report	Enables the specified report.
alarm-attack	Reports all alarm attacks.
alarm-other	Reports all other types of alarms (that is, non attack alarms).
alarm-traffic	Reports all traffic alarms.
itf-attack-stat	Reports all attack statistics.
itf-hardware-stat	Reports ethernet statistics.
itf-virtual-stat	Reports flow statistics.
log-config	Produces the configuration logs.
log-info	Produces information logs.
log-self	Produces self-logs.
log-traffic	Produces traffic logs.
policy-stats	Reports policy statistics.

proto-dist	Reports the distribution of different protocols types.
user-service <name>	Specifies the namestring of the user-defined service.
ah	Adds the Authentication Header from IP to the user-defined service.
esp	Adds the Encapsulating Security Payload from IP to the user-defined service.
gre	Adds the Generic Routing Encapsulation protocol to the user-defined service.
icmp	Adds the Internet Control Message Protocol to the user-defined service.
ospf	Adds the Open Short Path First protocol to the user-defined service.
tcp	Adds the Transmission Control Protocol to the user-defined service.
udp	Adds the User Datagram Protocol to the user-defined service.
low-high	Specifies the port range for the user-defined service.

Availability

This feature is currently supported on the NetScreen-5, -10, and -100.

Examples

To specify that the primary management station IP address is 102.10.1.2:

```
ns-> set global-pro primary 102.10.1.2
```

To enable the Global-Pro feature:

```
ns-> set global-pro enable
```

To enable reporting on the different types of protocols being passed in traffic through the NetScreen:

```
ns-> set global-pro reports proto-dist enable
```

Notes

Because every packet going through the NetScreen device is logged into the protocol table, performance is affected. NetScreen recommends this command be disabled except to obtain protocol-distribution information.

There is a corresponding **unset** command for each option (config, enable, and report).

See Also

See the **get global** command.

group

Description: Use the **set group** command to group several addresses or several services under a single name. A group of addresses or services then can be referenced by its name in an Access Policy.

Syntax

set group address {trust | untrust | dmz} <address-group-name> [add <address-member-name>] [comment <comment-string>]

set group service <group-service-name> [add <service-name>] [comment <comment-string>]

unset group address {trust | untrust | dmz} <address-group-name> [remove <address-member-name> | clear]

unset group service <service-group-name> [remove <service-name> | clear]

Arguments

address	Defines the group as an Address group.
trust | untrust | dmz	Specifies the interface for the Address group or Service group.
<address-group-name>	Defines the name of the Address group.
add <address-member-name>	Adds the Address named <address-member-name> to the Address group.
comment <comment-string>	Adds a comment <comment_string> to the entry.
service	Defines the group as a Service group.
<group-service name>	Defines the name of the Service group.
add <service-name>	Adds the Service named <service-name> to the Service group.
remove <address-member-name>	Removes the Address named <address-member-name> from the Address group. If you do not specify an Address group member, the unset group command deletes the entire Address group.
clear	Removes all the members of an Address or Service group.
remove <service-name>	Removes the Service named <service-member-name> from the Service group. If you do not specify a Service group member, the **unset group service <service-group-name>** command deletes that entire Service group.

Availability

This feature is available on all NetScreen device models at version 2.0 or later.

Defaults

No groups are configured by default.

Examples

To create an empty Address group for the Trusted interface and name it “headquarters”:

```
ns-> set group address trust headquarters
```

To create an empty Service group and name it “web-browsing”;

```
ns-> set group service web-browsing
```

To create an Address group named “engineering” for the Trusted interface and add the address “hw-eng” to the group:

```
ns-> set group address trust engineering add hw-eng
```

To remove the address for “admin-pc” from the “engineering” Address group:

```
ns-> unset group address trust engineering remove admin-pc
```

To create a Service group named “inside-sales” and a Pre-defined Service to the group:

```
ns-> set group service inside-sales add AOL
```

To remove the Service “PC-Anywhere” from the Service group named “inside-sales”:

```
ns-> unset group service inside-sales remove PC-Anywhere
```

To remove the Trusted Address group named “engineering”:

```
ns-> unset group address trust engineering
```

To remove the Service group named “inside-sales”:

```
ns-> unset group service inside-sales
```

See Also

See the **set address**, **set service**, and **get group** commands.

Notes

Addresses for Trusted, Untrusted, and DMZ interfaces may not be included in the same group.

Each Address group and Service group must have a unique name. In other words, you cannot create a Trusted group named “outside-sales” and also create an Untrusted group named “outside-sales.” Similarly, you cannot use an address name for a group name.

You cannot add these Addresses to a group: Inside Any, Outside Any, Dialup VPN, and DMZ Any.

You cannot add the following Service to a group: ANY.

When a group is referenced in an Access Policy, you cannot remove it; you can only modify it.

You can add only one member to a group at a time.

The maximum number of groups that you can create and the maximum number of members for each group varies with the NetScreen device model that you have.

NetScreen device	Number of Address Groups	Number of Members per Group
NetScreen-5	16	16
NetScreen-10	32	32
NetScreen-100	64	64
NetScreen-1000	256 (root) 8 (virtual system)	64 (root) 8 (virtual system)

NetScreen device	Number of Service Groups	Number of Members per Group
NetScreen-5	16	16
NetScreen-10	32	32
NetScreen-100	64	64
NetScreen-1000	256 (root) 8 (virtual system)	64 (root) 16 (virtual system)

ha

Description: Use the **set ha** command to define a high availability (HA) group identification number. NetScreen devices with the same group ID participate in the negotiation process of finding the master unit for the group.

Syntax

set ha encryption password <password>

set ha authentication password <password>

set ha auth <password>

set ha group <number>

set ha priority <number>

set ha arp <number>

set ha interface <trust | untrust | DMZ>

set ha link-up-on-slave

set ha fast mode

set ha monitor [<trust | untrust | DMZ>]

set ha second-path <trust | untrust | DMZ>

set ha session off

unset ha encryption

unset ha authentication

unset ha group

unset ha priority

unset ha arp

unset ha auth

unset ha interface

unset link-up-on-slave

unset ha fast mode

unset ha second-path

unset ha session off

Arguments

encryption password <password>	Specifies that HA encrypt all sessions and configuration packets, and enforce the specified password. Valid passwords contain from 1 to 16 characters.
authentication password <password>	Specifies that HA perform authentication and enforce the specified password. Valid passwords contain from 1 to 16 characters.
auth	Sets authorization using the authentication password.
group <number>	Defines an identification number for the group where <number> is a number between 0 and 255. If you specify 0, high availability (HA) is disabled.
key <number>	Sets the preshared key for both master and slaves. The <number> is an 8-byte hex number. This key value can be any random number, but you should use the same value for all members of a HA cluster.
arp <number>	Sets the number of requests the HA master sends out. The default is 2.
interface <trust | untrust | DMZ>	This is only for the NetScreen-100 model. Specifies the interface on which the NetScreen-100 devices are grouped for HA.
monitor	Sets failover from the master HA to the slave. The default is set to monitor the Trusted, Untrusted, and DMZ interfaces.
link-up-on-slave	Links the Trusted, Untrusted, and DMZ interfaces on the HA slave when the slave is running.

second-path	Defines an alternate route for the slave to continue Heartbeat communications should the primary HA link fail.
session off	Stops the master HA from propagating the session's services. Using this command may improve performance.
priority <number>	Assigns a number to define which system is the master unit when two NetScreen devices in an HA group are powered at the same time. The <number> is a number between 0 and 255. The system with the lower number becomes the master unit.

Availability

Key and encryption are available for the NetScreen-100 and NetScreen-1000 models.

Group, interface, and priority are available for NetScreen-100 and NetScreen-1000 models only.

Defaults

The group ID number is set to 0, which means that HA is disabled.

The default priority number is 100.

Examples

To define the HA group to 3:

```
ns-> set ha group 3
```

To disable high availability:

```
ns-> unset ha group
```

Notes

High availability is available when NetScreen devices are running in Transparent and NAT mode.

If two NetScreen devices have the same priority number, the device with the lowest MAC address becomes the master. The other devices become slaves. The default value is 100.

The color of the Status LED on the NetScreen-100 indicates whether it is operating as a master or a slave. Green indicates the device is running in master mode, and yellow indicates slave mode.

See Also

See the **get ha** and **exec ha file-sync** commands.

ha track ip

Use the **ha track ip** command to define a collection of IP addresses to be monitored (tracked) so if access to these addresses fails, the master device fails over to the slave.

This command detects external conditions that impair the normal operation of the system.

Syntax

set ha track ip

unset ha track ip

Arguments

set ha track ip	Use the **track IP** command to configure one or more IP address to be monitored by the system. The system monitors the IP address(s) by pinging it periodically. An IP address is considered dead if 3 consecutive pings fail. Track IP monitoring is active only when the device is in HA mode, and only when link IP is configured correctly on all interfaces.
unset ha track ip	`Unbinds an interface from a track IP address.`

Availability

The **track ip** command is available only for the NetScreen-1000 model, and only at root level. It is not available in virtual system mode.

Defaults

Important: *Ensure that the specified IP address is configured correctly before adding IP addresses to the monitored list or adjusting intervals or thresholds.*

By default, IP addresses in the monitored list are pinged every second. After three consecutive timeouts, the IP address is considered dead. You can set an interval from 1 to 200 seconds.

The default value for the failover threshold is 3, but it can be set to between 1 and 200 seconds.

By default, the system chooses the correct interface from which to initiate the ping for each track-IP.

Examples

To enable ip tracking for HA failover:

```
ns1000-> set ha track ip
```

To disable IP tracking:

```
ns1000-> unset ha track ip
```

To add an IP address to the list of tracked IP addresses:

```
ns1000-> set ha track ip <ip-address>
```

To customize the pinging interval:

```
ns1000-> set ha track ip <ip-address> interval <seconds>
```

To restore the default interval of a track IP:

```
ns1000-> unset track ip <ip-address> interval
```

To adjust the failover threshold:

```
ns1000-> set ha track ip <ip-address> threshold <number>
```

To restore the default failover threshold:

```
ns1000-> unset ha track ip <ip-address> threshold
```

To force an interface from which the system pings a particular track-IP:

```
ns1000-> set ha track ip <ip-address> interface <name>
```

To unbind an interface from a track IP:

```
ns1000-> unset ha track ip <ip-address> interface
```

Notes

You may add up to 16 IP address for monitoring using the **track IP** command.

Duplicate IP addresses are rejected and result in an error message.

If the interface from which the system pings the addresses on the track-ip list does not have link IP configured, monitoring cannot be performed. The track IP command results in an error message.

Be sure to configure the interface name (main or subinterface) before setting up monitoring.

See Also

get ha track ip

hostname

Description: Use the **set hostname** command to define the name of the NetScreen device. This is the name that appears in the console.

Syntax

set hostname <string>

unset hostname

Arguments

hostname <string>	Set the name of the NetScreen device to <string>.

Availability

This feature is supported on all NetScreen device models.

Defaults

For NetScreen-5: ns5

For NetScreen-10: ns10

For NetScreen-100: ns100

For NetScreen-1000: ns1000

Examples

To change the a NetScreen-100 device hostname to “acme”:

```
ns100-> set hostname acme
```

To reset the NetScreen-100 device hostname to the default value:

```
ns100-> unset hostname acme
```

See Also

See the **get hostname** command.

icmp-threshold

Description: Use the **set icmp-threshold** to set a threshold value for icmp flooding protection.

Syntax

set icmp-threshold <number>

Arguments

<number>	Defines the number of Internet Control Message Protocol (ICMP) packets allowed to ping the same destination address.The range is 1 to 1,000,000.

Availability

This feature is available on the NetScreen-5, -10, and -100. For the NetScreen-1000, use the **set firewall** command to set the threshold.

Defaults

The default is 1000 packets.

Examples

To set the icmp ping threshold to 20,000 packets:

```
ns1000 -> set icmp-threshold 20000
```

To restore the icmp ping threshold to the default of 1000 packets:

```
ns1000 -> set icmp-threshold 1000
```

See Also

See the **set firewall**, **get firewall**, and **get icmp-threshold** commands.

Notes

When the number of ICMP packets pinging the same destination address exceeds the specified number per second, the device generates an alarm and drops subsequent packets. To display the ICMP flood protection threshold, use the **get firewall** or the **get icmp-threshold** command.

ike

Definition: Use the **set ike** command to define the Phase 1 and 2 proposals and the gateway for an Autokey IKE (Internet Key Exchange) VPN configuration. You must use the three **set ike** commands in the Syntax section sequentially, creating the Phase 1 proposal first, the Phase 2 proposal second, and defining the remote gateway third. For the complete sequence of commands needed to create a VPN tunnel, see "Notes" on page 2-68.

Syntax

set ike p1-proposal <name> {preshare | rsa-sig} {group1 | group2 | group5} esp {des | 3des} {md5 | sha-1} [{seconds | minutes | hours | days} <lifetime>]

set ike p2-proposal <name> {no-pfs | group1 | group2 | group5} {ah | {esp {null | des | 3des}}} {null | md5 | sha-1} [{seconds | minutes | hours | days} <lifetime>] [kbytes <lifesize>]

set ike gateway <name> dynamic <peer_id> [local_id] [{main | agressive}] [preshare <preshare <preshare-key>] proposal <p1_proposal> <p1_proposal> <p2-proposal> <p3-proposal>

set ike gateway <name> {ip <peer_ip> [ip <peer_id]} [{main | aggressive} [preshare <preshare_key>] proposal <p1_proposal> <p2-proposal> <p3-proposal>

set ike gateway <name> dialup <user_name> or <group_name} [local <local_id] [{main | aggressive} [preshare <preshare_key>] [{main | aggressive} [preshare <preshare_key>] proposal <p1_proposal> <p2-proposal> <p3-proposal>

set ike accept-all-proposal

set ike id-mode {ip | subnet} | policy-checking}

set ike initiator-set-commit

set ike responder-set-commit

set ike initial-contact {single-gateway <string> | all-peers} single-user <name>

set ike gateway <name> cert my-cert <cert_id>

set ike gateway <name> peer-ca <ca_id>

set ike gateway <name> cert peer-cert-type { x509 | pkcs7 }

unset ike {gateway <name> | p1-proposal <name> | p2-proposal <name> | accept-all-proposals | policy-checking}

unset ike gateway <name> peer-ca

unset ike gateway <name> peer-cert-type

unset ike gateway <name> my-cert

Arguments

proposal <name>	Adds or modifies the IKE phase one proposals, which define the authentication method and security association when doing IKE negotiation with remote gateways.
preshare | rsa-sig	Specifies the authentication method to encrypt IKE messages. preshare refers to a Preshared key; rsa-sig refers to an RSA-signature. Preshared key is the default method.
group1 | group2 | group5	In a Phase 1 proposal, identifies the Diffie-Hellman group, a technique that allows two parties to negotiate encryption keys over an insecure medium; that is, the Internet. Group2 is the default group.
esp	Specifies Encapsulating Security Payload, a protocol that provides both encryption and authentication.
des | 3des	Specifies the encryption algorithm used in ESP protocol. The default encryption algorithm is 3DES.
md5 | sha-1	Specifies the authentication algorithm used in ESP protocol. The default algorithm is SHA-1.

{seconds | minutes | hours | days} <lifetime>	Defines the elapsed time before the NetScreen mechanism renegotiates another security association. The minimum allowable lifetime is 180 seconds. The default lifetime is 28800 seconds.
p2-proposal <name>	Adds or modifies the IKE phase two proposals, which define the secret key and security association for data flow.
no-pfs | group1 | group2 | group5	In a Phase 2 proposal, defines how the encryption key is generated. Perfect Forward Secrecy (PFS) is a method for generating a new encryption key independently from its predecessor. Selecting no-pfs specifies that IKE generates the Phase 2 key from the key generated in the Phase 1 exchange. By selecting one of the Diffie-Hellmen groups, IKE generates the encryption key by doing another Diffie-Hellman key exchange, using PFS. The default is Group 2.
ah | esp	In a Phase 2 proposal, identifies the IPSec protocol—either Authentication Header (AH) or Encapsulating Security Payload (ESP).
null	Specifies either no encryption or no authentication applied.
kilobytes <lifesize>	Indicates the maximum allowable data flow in kilobytes before NetScreen renegotiates another security association. The default value is 0 (infinity).
gateway <name>	Adds or modifies the remote gateway for IKE.

ip <peer_ip>	Defines the IP address of the remote gateway. If the remote gateway is a dynamic remote gateway, enter the string "ID <peer_id>" in this field.
id <peer_id>	(Optional) Identifies the remote gateway. Identification can be in one of these three forms: • IP address (a.b.c.d) • fully qualified domain name (FQDN); for example, www.netscreen.com • RFC822 name; that is, an email name such as joe@netscreen.com. Include the peer ID only when you want to enforce identifying the peer gateway with the specified ID. The NetScreen device checks the peer's ID payload to determine if it matches the specified ID.
dialup <user_name>	Identifies dialup users at dynamic IP addresses. To specify a user's attributes, use the **set user** command. Specifying dialup users requires Aggressive mode.
local <local_id)	Defines the NetScreen identity. Use only when the NetScreen device is a non-fixed IP gateway in Aggressive mode.
main | aggressive	Defines the mode used for remote gateways. The main mode is the recommended key-exchange method because it conceals the identities of the parties during the key exchange. Use Aggressive mode only when you want to initiate an IKE key exchange without ID protection. Aggressive mode also provides faster throughput than Main mode. Main mode is the default.

preshare <preshare_key>	If you use a Preshared key in the Phase 1 proposal, defines that key. If you use an RSA-signature in the Phase 1 proposal, do not include this reference.
proposal <p1_proposalx>	Refers to the Phase 1 proposal.
accept-all-proposal	Accepts all incoming proposals. The default is to accept only those proposals matching predefined or user-defined proposals.
id-mode {ip | subnet}	Defines the IKE ID mode in the Phase 2 exchange as either IP only or subnet. (Use IP when setting up a VPN tunnel between a NetScreen device and a CheckPoint 4.0 device. Otherwise, use the subnet option.)
policy-checking	Checks if the Access Policies of the two VPN participants match before establishing a connection. With release ScreenOS 2.5 or higher, use policy checking to identify configured policies when multiple tunnels are supported between two peer gateways. If you disable policy checking when multiple policies are configured between two peers, the IKE session will fail. For backward compatibility with release ScreenOS 2.0 and earlier, disable policy checking when only one policy is configured between two peers.
initiator-set-commit	Commands the NetScreen device to request that the responder confirm that the new IPSec SA is established. The NetScreen device will not use the new SA until this confirmation is received. The default is unset.

responder-set-commit	Commands the NetScreen device to request that the initiator confirm that the new IPSec SA is established before using it. The default is unset.
initial-contact {single-gateway <string> | all-gateways}	Commands the NetScreen device to send INITIAL_CONTACT notification to each IKE peer gateway during the first IKE sessions after a reset. Specifying single-gateway <name> requests that the NetScreen device delete all SAs associated with the specified IKE gateway, and issue an **INITIAL_CONTACT** notification during the next IKE session. Specifing all-gateways requests that the NetScreen device delete all SAs associated with all IKE gateways, and issue an **INITIAL_CONTACT** notification during the next IKE session. The default is Unset.

Availability

All NetScreen device models at version 2.0 or later that support VPNs and encryption. The NetScreen-1000 at version 1.7 supports IKE for LAN-to-LAN VPNs, but not for IKE dialup users. The NetScreen-1000 also does not support certificates.

Defaults

Main mode is the default key-exchange method.

The default time intervals before the NetScreen mechanism renegotiates another security association are 28,800 seconds for a Phase 1 proposal, and 3600 seconds for a Phase 2 proposal.

The default ID mode is Subnet. (Changing the ID mode to IP is necessary only if the data traffic is between two security gateways, one of which is a CheckPoint 4.0 device.)

The default for the initiator- and responder-set-commit commands is Unset. The default for initiator- and responder-echo-summit is Set.

Examples

To define a Phase 1 proposal named “sf1” with these attributes:

- Preshared key and a group 1 Diffie-Hellman exchange
- Encapsulating Security Payload (ESP) protocol using the Triple Data Encryption Standard (3DES) and Message Digest 5 (MD5) algorithms
- Lifetime of 3 minutes:

```
ns-> set ike p1-proposal sf1 preshare group1 esp 3des md5 minutes 3
```

To define a Phase 2 proposal named “sf2” with these attributes:

- Group 2 Diffie-Hellman exchange
- ESP using 3DES and SHA-1
- Lifetime of 15 minutes:

```
ns-> set ike p2-proposal sf2 group2 esp 3des sha-1 minutes 15
```

To define a remote gateway named “san_fran” with the following attributes:

- Main mode
- Preshared Key with the value “caterwaul”
- Reference to the Phase 1 proposal “sf1”

```
ns-> set ike gateway san_fran main preshare caterwaul proposal sf1
```

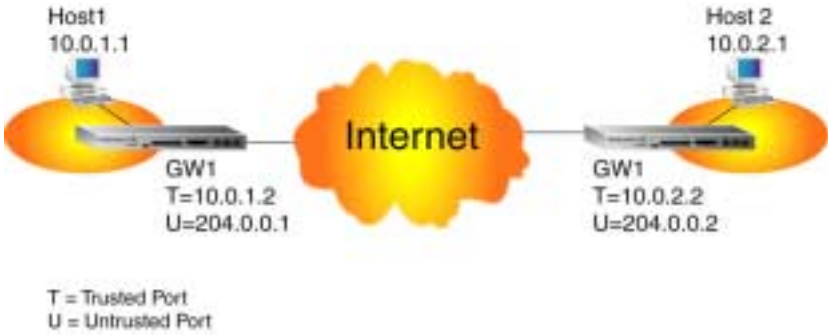
For an example of the complete procedure for setting up a VPN tunnel, see the Notes section below.

See Also

See the **clear ike**, **get ike**, **set policy**, **set user**, **set vpn**, and **get sa** commands.

Notes

The entire procedure for setting up a VPN tunnel for a remote gateway with a static IP address requires up to five steps. To set up the end of a VPN tunnel at the NetScreen device acting as gateway 1 (GW1) in the illustration, follow the steps below.



1. Set the addresses for the Trusted and Untrusted parties at the two ends of the VPN tunnel:

   ns-> **set address trust host1 10.0.1.1 255.255.255.0**

   ns-> **set address untrust host2 10.0.2.1 255.255.255.0**

2. Define the IKE Phase 1 proposal and Phase 2 proposal. If you use the default proposals, you do not need to define Phase 1 and Phase 2 proposals.
3. Define the remote gateway:

   ns-> **set ike gateway gw2 ip 204.0.0.2 preshare netscreen proposal pre-g2-3des-md5**

4. Define the VPN tunnel as AutoKey IKE:

   ns-> **set vpn vpn1 gateway gw2 proposal g2-esp-des-md5**

5. Define the Outgoing Access Policy:

   ns-> **set policy out host1 host2 any encrypt vpn-tunnel vpn1**

The procedure for setting up a VPN tunnel for a remote user with a dynamically assigned IP address requires up to four steps.

1. Define the user as a dialup user. See the **set user** command on page 2-120.
2. Define the IKE Phase 1 proposal, Phase 2 proposal, and remote gateway.

Note: *If you use the default proposals, defining either a Phase 1 or a Phase 2 proposal is unnecessary.*

3. Define the VPN tunnel as AutoKey IKE. See the **set vpn** command on page 2-128.
4. Define the Access Policy, with "Dial-Up VPN" as the destination address. See the **set policy** command on page 2-89.

If the message confirming the establishment of a new IPSec SA is lost, the NetScreen device expecting it will instead receive IPSec traffic following a Phase 2 exchange. Instead of continuing to wait for the (lost) confirmation message, the NetScreen device can verify the received message, consider the SA established, and continue processing.

interface

Description: Use the **set interface** command to define the network interface settings.

If you are configuring a NetScreen-5, use the **set interface untrust dhcp** command to configure the NetScreen-5 as a DHCP client. It will then obtain an IP address for its Untrusted interface from a DHCP server.

If you are using a NetScreen-10 or a NetScreen-100, use the **set interface {trust, untrust, DMZ}** commands below.

If you are configuring a NetScreen-1000, use the **set interface** command to create subinterfaces.

Syntax

set interface {dmz | trust > {nat | route} | untrust}

set interface {dmz | trust > {nat | route} | untrust} {bandwidth <number>}

set interface {dmz | trust > {nat | route} | untrust} {gateway <a.b.c.d>}

set interface {dmz | trust > {nat | route} | untrust} {ident-reset}

set interface {dmz | trust > {nat | route} | untrust} {ip <a.b.c.d>}

set interface {dmz | trust > {nat | route} | untrust} {manage | global | global-pro | ping | scs | snmp | ssl | telnet | web}

set interface {dmz | trust > {nat | route} | untrust} {manage-ip <a.b.c.d>}

set interface {dmz | trust > {nat | route} | untrust} {phy | auto {100mb | 10mb} | full {100mb | 10mb} | half {100mb | 10mb}}

set interface { trust | untrust } vlan trunk

set interface untrust dhcp

set interface untrust manage [<interface_name>]

Arguments

dmz	The DMZ interface (where applicable).
mgt	The Management interface (for the NetScreen-1000 only).
trust	The Trusted interface.
untrust	The Untrusted interface.
interface untrust dhcp	Defines the NetScreen device as a DHCP client. As such, the NetScreen device obtains its IP address for the Untrusted interface from a DHCP server.
bandwidth <number>	The guaranteed maximum bandwidth in kbps for all Access Policies.
ip <a.b.c.d> <A.B.C.D>	The IP address <a.b.c.d> and subnet mask <A.B.C.D> for the Trusted, Untrusted, DMZ, or Management (MGT) interface.
link-ip <a.b.c.d>	Provides management capability for attached slave devices. The link-IP address is not the same as the interface IP. Unlike interface IPs which are always the same for master and slave devices, link-IPs can be different. If you change the interface IP address to be the same as the link-IP address, the link IP is reset to 0.0.0.0 automatically. Likewise, if you change the interface IP and link IP to be in different subnets, the link IP is reset to 0.0.0.0 automatically.
manage	Enables management of interfaces such as Global, SRC, SNMP, and so on.
ping	Enables the ability to ping the IP address of the NetScreen device through the Trusted, Untrusted, DMZ, or MGT interface.
dhcp	The NetScreen-5 and -10 only. Defines the Untrusted IP address of the NetScreen device as one dynamically assigned by the Dynamic Host Configuration Protocol (DHCP)
mng	Enables remote management for that interface.

global	For the NetScreen-5, -10, and -100. Turns NetScreen Global-Manager manageability on or off.
global-pro	For the NetScreen-5, -10, and -100. Turns NetScreen Global-Pro manageability on or off.
ident-reset	If set to "on", enables the NetScreen device to send a TCP Reset announcement in response to an IDENT request to port 113.
scs	Turns the secure command shell (SCS) manageability on or off.
snmp	For the NetScreen-5, -10, and -100. Turns Simple Network Management Protocol (SNMP) manageability on or off.
telnet	Turns Telnet manageability on or off.
web	Turns Web manageability on or off.
vlan trunk	For the NetScreen-100 and -1000. Allows all Port-based VLAN tags to pass through a NetScreen device running in Transparent mode (pending policy approval).
manage-ip <a.b.c.d>	For the NetScreen-100 and -1000. The IP address specified is used to manage the NetScreen device on a per interface basis.
gateway <a.b.c.d>	IP address for the gateway to send packets to that do not belong on the network protected by the NetScreen device. The Untrusted interface is the default gateway.
[no-default-route]	Disables the definition of the default gateway for the NetScreen device as the Untrusted interface.
phy auto	Enables the network autosensing feature. The NetScreen system automatically selects the duplex mode as "full" or "half" based on the connected device.
phy full	Disables the network autosensing feature. Specifies the duplex as "full."
phy half	Disables the network autosensing feature. Specifies the duplex as "half."
100mb | 10mb	For the NetScreen-100 only. Selects a speed for transmission—100mb or 10mb.

set interface trust/id <a.b.c.d.> <A.B.C.D.>	For the NetScreen-1000 only. Specifies a Sub interface (SIF) for a virtual LAN (VLAN). "trust/1" defines the subinterface as being on the Trusted side of the NetScreen-1000 with the identifying number "1." The NetScreen-1000 supports up to 100 SIFs. <a.b.c.d.> represents the IP address of the VLAN subnet. <A.B.C.D.> represents the subnet mask. The NetScreen-1000 supports only one subnet per VLAN.
nat | route	The parameter **nat** is a keyword that means these are private IP addresses; therefore, Network Address Translation is used for the traffic to and from the virtual local area network (VLAN). The parameter **route** is a keyword that means these are public IP addresses; therefore, the NetScreen device operates on traffic to or from the VLAN in Route mode, passing packets with the untranslated destination or source address in the IP header.
vlan name	For the NetScreen-1000 only. The name of the virtual local area network (VLAN) to be associated with this interface.
mip <a.b.c.d>	Sets the mapped IP address.
netmask <A.B.C.D>	Specifies the subnet mask.
dip <a.b.c.d> | <e.f.g.h>	Sets the dynamic IP address range.
port-translation	Specifies if port translation is to be applied.
host <a.b.c.d>	Specifies the trust side host IP address.

Availability

This feature is supported on all NetScreen device models.

The virtual interface feature is supported on NetScreen-1000 devices only.

Defaults

Web management is through the Trusted interface.

You can ping to both the Trusted and DMZ interfaces.

The IP addresses, link-IP addresses, netmasks, and gateways are 0.0.0.0.

For the NetScreen-100, network interfaces are autosensing-enabled.

The ability to reset the application **ident** is disabled by default.

A VLAN on the NetScreen-1000 is private by default.

Examples

Typical implementations of this command are:

To configure a NetScreen-5 as a DHCP client:

```
ns-> set interface untrust dhcp
```

To define bandwidth for the DMZ interface to 1000 kilobits per second:

```
ns-> set interface dmz bandwidth 1000
```

To enable Web management on the Untrusted interface:

```
ns-> set interface untrust web
```

To allow the Untrusted interface to respond to the **ping** command:

```
ns-> set interface untrust ping
```

To manually configure the NetScreen-100 device Untrusted network interface to 100Mb/sec with full duplex:

```
ns-> set interface untrust phy full 100mb
```

To change the “default gateway” of the NetScreen device from the default Untrusted interface gateway 210.23.1.99 to the Trusted interface gateway 192.16.0.8:

```
ns-> set interface untrust gateway 210.23.1.99 no-default-route

ns-> set route 0.0.0.0 0.0.0.0 interface trust gateway 192.16.0.8
```

To enable the ability to reset the application ident on a Trusted interface:

```
ns-> set interface trust ident-resetTo
```

To turn on SCS on the Untrusted interface on a NetScreen-10:

```
ns-> set interface untrust manage scs
```

In this example, a NetScreen-100 and NetScreen-1000 administrator can manage: 1.2.3.4, 2.3.4.100, 3.4.5.100, and 4.5.6.7.

```
ns-> set admin sys-ip 0.0.0.0

ns-> set interface trust ip 1.2.3.4 255.255.255.0

ns-> set interface trust/1 ip 2.3.4.5 255.255.255.0

ns-> set interface trust/1 manage-ip 2.3.4.100

ns-> set interface trust/2 ip 3.4.5.6 255.255.255.0

ns-> set interface trust/2 manage-ip 3.4.5.100

ns-> set interface trust/3 ip 4.5.6.7 255.255.255.0
```

In this example, a NetScreen-100 and NetScreen-1000 administrator can manage 1.2.3.100, 2.3.4.100:

```
ns-> set admin sys-ip 1.2.3.100

ns-> set interface trust ip 1.2.3.4 255.255.255.0

ns-> set interface trust/1 ip 2.3.4.5 255.255.255.0

ns-> set interface trust/1 manage-ip 2.3.4.100

ns-> set interface trust/2 ip 3.4.5.6 255.255.255.0
```

To create a subinterface (SIF) and associate it with a particular VLAN, issue this **set interface** command from the main system of the NetScreen-1000:

```
ns-> set interface trust/<id> ip <a.b.c.d> <A.B.C.D> {route | nat}
[vlan name]
```

To bind an already-created SIF and the VLAN associated with it to a Virtual System, you must be at the command prompt for that Virtual System when you issue the following **set interface** command:

```
ns-> set interface trust/<id>
```

For information about Virtual Systems, see the **set vsys** command on page 2-132.

NetScreen-1000 Examples

To create a sub-interface and associate it with a particular VLAN, issue this **set interface** command from the main system of the NetScreen-1000:

```
ns1000-> set interface trust/<id> ip <a.b.c.d.> <A.B.C.D.> tag
<tag id>
```

To bind an already-created SIF and the VLAN associated with it to a Virtual System, issue this **set interface** command from the command prompt for that Virtual System:

```
ns1000-> set interface trust/<id>
```

For more information on Virtual Systems, see the **set vsys** command on page 2-132.

To set an IP address for the Out-of-Band Management port through which to manage the device:

```
ns1000-> set interface oob 172.16.40.1
```

See Also

See the **get interface**, **unset interface,** and **set vlan** commands.

Notes

The phy parameter is applicable only to NetScreen-100 devices that have a serial number xy99xxxx where “y” is equal to or greater than 4. (The ‘99’ represents the year of manufacture.)

The **no-default-route** option is available with firmware 1.62 and later.

The interface gateway is used by the NetScreen device for management from either HTTP or Telnet. A value of 0.0.0.0 indicates that only systems on the same subnet as the NetScreen device can manage the NetScreen device.

On a NetScreen-1000, the **set interface** command is a privileged command and requires a root-level login and password.

With the NetScreen-5, if you are using DHCP Client for assigning the IP address to the Untrusted port and you want to change to a static IP address, first issue an **unset interface DHCP** command.

If this specific sequence is not followed, you are unable to change from a DHCP-assigned IP address to a static IP address:

1. **unset interface untrust dhcp**
2. **set interface untrust ip <a.b.c.d> <netmask>**

The **manage-ip** option supersedes the **sys-ip** option and applies on a per-interface basis. When set, the IP address is used to manage the device.

If both the per interface **manage-ip** and global **sys-ip** are set to 0.0.0.0, the interface IP is used to manage the device. If **manage-ip** is 0.0.0.0 and **sys-ip** is not 0.0.0.0, the management IP is derived from the **sys-ip** and the interface IP.

Note that **manage-ip** takes precedence over **sys-ip**. If the **sys-ip** is 0.0.0.0, the administrator can use the interfaces IP to manage the device with the exception of those interfaces and subinterfaces set with **manage-ip**.

Both the management IP and the interface IP respond to ICMP (ping) messages. This allows network administrators to debug the network by pinging the real interface IP.

ippool

Definition: Use the **set ippool** command to associate the name of an IP pool with a range of IP addresses.

Syntax

set ippool <poolname> <start address range> <end address range>

unset ippool <poolname>

Arguments

<poolname>	Specifies the name of the IP pool.
<start address range>	The lower limit of the IP addresses in the pool.
<end address range>	The upper limit of the IP addresses in the pool.

Availability

This feature is available on all NetScreen device models.

Defaults

None.

Examples

To configure an IP pool named “office” with the IP addresses 172.16.10.0 through 172.16.10.244:

```
ns-> set ippool office 172.16.10.0 172.16.10.244
```

See Also

See the **set l2tp** and **get ippool** commands.

Notes

The **set ippool** and **get ippool** commands support the l2tp feature on the NetScreen devices.

ipsweep-threshold

Description: Use the **set ipsweep-threshold** command to set a threshold value for ipsweep protection.

Syntax

set ipsweep <micro-seconds>

Arguments

<micro-seconds>	Defines the ipsweep threshold in microseconds. The valid range is from 1 to 1,000,000.

Availability

This feature is available only on NetScreen-1000 device models.

Defaults

The default is 30000 microseconds, restored by the **unset** command.

Examples

To set the ipsweep threshold to 20,000 microseconds:

```
ns1000-> set ipsweep-threshold 20000
```

To restore the ipsweep threshold to the default of 30,000 microseconds:

```
ns1000-> set ipsweep-threshold 30000
```

See Also

See the **get ipsweep-threshold** command.

Notes

The device counts all packets coming from the same source IP address. If the number of packets reaches or exceeds 10 within the configured time range, the device assumes that there is an attack underway. Packets beyond 10 are dropped, and alarms are generated. The alarm reports the suspected source IP that may be responsible for the attack.

mip

Definition: Use the **set mip** command to define and modify Mapped IP (MIP) configurations.

Syntax

set mip <a.b.c.d> [netmask <A.B.C.D>] host <a.b.c.d.>

unset mip <a.b.c.d> [netmask <A.B.C.D>]

Arguments

set mip <a.b.c.d> host <e.f.g.h>	Maps the Untrusted IP address <a.b.c.d> to the actual IP address <e.f.g.h> of the devicereceiving the mapped traffic.
set mip netmask <A.B.C.D>	Defines the subnet mask of the mapped address.

Availability

This feature is supported on all NetScreen device models.

Defaults

The default subnet mask is 255.255.255.255.

Examples

To define a one-to-one Mapped IP configuration for a server with the IP address 172.16.10.92 to the valid external IP address 205.34.192.1:

```
ns-> set mip 205.34.192.1 host 172.16.10.92
```

To define a one-to-one Mapped IP configuration for a machine with IP address 172.16.10.92 to a specific host with an IP address 201.10.175.1:

```
ns-> set mip 201.10.175.1 host 172.16.10.92 netmask 255.255.255.255
```

To set a subnet of Mapped IPs to a subnet of internal hosts, defined by the netmask 255.255.255.248:

```
ns-> set mip 209.125.15.1 host 10.1.1.1 netmask 255.255.255.248
```

See Also

See the **get mip** command.

Notes

Use **unset mip** to delete a Mapped IP configuration.

Mapping is allowed for a one-to-one or subnet-to-subnet relationship. When a subnet-to-subnet Mapped IP configuration is defined, the subnet mask is applied to both the Mapped IP subnet and the actual IP subnet.

ntp

Description: Use the **set ntp** command to configure the NetScreen device for Network Time Protocol (NTP). NetScreen's implementation is based upon Simple Network Time Protocol (SNTP) and is therefore a subset of NTP. It is used to synchronize computer clocks in the Internet. In its simplified version, SNTP is adequate for devices that do not require a high level of synchronization and accuracy.

Syntax

set clock ntp

set ntp {server <a.b.c.d> | interval <number> | zone <number>}

unset clock ntp

unset ntp {server | interval | zone}

Arguments

clock ntp	Enables the SNTP feature.
server <a.b.c.d>	Defines the NTP server with which the NetScreen device synchronizes time. Replace a.b.c.d with the IP address of the NTP server.
interval <number>	Defines in minutes how often the NetScreen device updates its clock time by synchronizing with the NTP server.
zone <number>	Defines the local time zone. The values range from -12 to 12 (in integers) to signify the hours offset from GMT (Greenwich Mean Time).

Availability

This feature is available on the NetScreen-5 at version 1.65 or later and the NetScreen-10, -100, and -100p at version 2.0 or later.

Defaults

- The NTP service is “off” by default
- The IP address for the NTP server is set to 0.0.0.0
- The frequency (time interval) for synchronizing clock time is every 10 minutes
- The Time Zone is set to “0,” which translates to GMT (Greenwich Mean Time)

Examples

To enable NTP:

```
ns-> set clock ntp
```

To define the NTP server with the IP address of 172.10.10.6 with which to synchronize clock time:

```
ns-> set ntp server 172.10.10.6
```

To configure the NetScreen device to synchronize its clock time every 20 minutes:

```
ns-> set ntp interval 20
```

To set the Time Zone to GMT minus eight hours:

```
ns-> set ntp zone -8
```

To disable the NTP feature:

```
ns-> unset clock ntp
```

To disable the NTP server and set its default IP address back to 0.0.0.0:

```
ns-> unset ntp server
```

To set the default synchronization interval back to 10 minutes:

```
ns-> unset ntp interval
```

See Also

See the **get ntp** and **exec ntp** commands.

Notes

The range for the synchronization interval is from 1 to 300 minutes.

pki

Definition: Use the **set pki** command to designate the certificate authority (CA) server's IP and e-mail addresses, and to create new RSA key pairs for public key encryption.

Syntax

set pki ldap {server-name | IP address <string> | crl-url <string>}

set pki x509 default {crl-refresh {default | daily | weekly | monthly} | ns-cert <number> | send-to <string>}

set pki x509 dn {country-name <string> | state-name <string> | local-name <string> | org-name <string> | org-unit-name <string> | name <string> | phone <string> | email <string> | ip <string>}

set pki x509 default cert-path <full | partial>

unset pki ldap {server-name | crl-url}

unset pki x509 default {crl-refresh | send-to}

unset pki x509 dn {country-name | state-name | local-name | org-name | org-unit-name | name | phone | email | ip}

Arguments

ldap server-name <string>	Defines the IP address or domain name of the default Lightweight Directory Access Protocol (LDAP) server for the certificate authority (CA) that validates the X.509 certificate.
crl-url <string>	Sets the default LDAP URL for the CA certificate revocation list (CRL) to be used for X.509 CRL retrieval purposes.
x509 default	Specifies a type of digital certificate with the default X.509 certificate settings.
crl-refresh {default | daily | weekly | monthly}	Sets the refreshment frequency of the X.509 CRL. The default option uses the validation date decided by each CRL.
ns-cert <number>	Specifies the ID number of the digital certificate that appears in the X.509 list displayed by the get pki command.
send-to <string>	Assigns the destination e-mail address where the PKCS10 certificate request file is sent.
dn	Specifies a distinguished name to uniquely identify the user for whom the certificate is being requested.
country-name <string>	Sets the country name as the X.509 certificate subject name of the NetScreen device.
state-name <string>	Sets the state name as the X.509 certificate subject name of the NetScreen device.
local-name <string>	Sets the name of the locality as the X.509 certificate subject name of the NetScreen device.
org-name <string>	Sets the organization name as the X.509 certificate subject name of the NetScreen device.
org-unit-name <string>	Sets the organization unit name as the X.509 certificate subject name of the NetScreen device.

name <string>	Sets the name of the NetScreen device as its X.509 certificate subject name. It is used to differentiate the NetScreen X.509 certificates with the same RSA key but issued by different Certificate Authorities.
phone <string>	Sets the contact phone number of the NetScreen device administrator as the X.509 certificate subject name of the NetScreen device.
email <string>	Sets the contact e-mail address of the NetScreen device administrator as the X.509 certificate subject name of the NetScreen device.
ip <string>	Sets the IP address of the NetScreen device as its X.509 certificate subject name.

Availability

This feature is supported on all NetScreen device models at version 2.0 or later.

Defaults

The RSA key length is set to 1024 bits.

Examples

To set the CA server's IP address to 162.128.20.12:

```
ns-> set pki ldap caServer 162.128.20.12
```

To set the destination e-mail address where the PKCS10 certificate request is sent:

```
ns-> set pki x509 default send-to caServer@somewhere.com
```

To refresh the certificate revocation list on a daily basis:

```
ns-> set pki x509 default crl-refresh daily
```

To define a distinguished name for Ed Jones who works in marketing at NetScreen Technologies in Santa Clara, California:

```
ns-> set pki x509 dn country-name “united states”

ns-> set pki x509 dn state-name california

ns-> set pki x509 dn local-name “santa clara”

ns-> set pki x509 dn org-name “netscreen technologies”

ns-> set pki x509 dn org-unit-name marketing

ns-> set pki x509 dn name “ed jones”
```

See Also

See the **get pki** and **exec pki** commands.

policy

Description: Use the **set policy** command to define policies to control network traffic.

Syntax

set policy default-permit-all

set policy [name <string>] [id <number>] [before <number>] {incoming | outgoing | fromdmz | todmz} <string1> <string2> <string3> {permit | deny | tunnel {auth} | nat} [count | log | alarm <second-threshold> <minute-threshold>] [traffic gbw <kbps> priority <number> mbw <kbps>] [dscp enable | disable]

set policy [id <number>] [dip {ip <a.b.c.d> | <e.f.g.h>} | mip <a.b.c.d> netmask <A.B.C.D>]

set policy move <number> {before | after} <number>

set policy outgoing <src_addr> <dst_addr> <service> tunnel [vpn <IKE>] [l2tp <name>]

unset policy <number>

unset policy [id <number>] [dip {ip <a.b.c.d> | <e.f.g.h>} | mip <a.b.c.d> | netmask <A.B.C.D>]

Arguments

default-permit-all	Allows all outbound network traffic to flow through the NetScreen device.
name <string>	Names the Access Policy.
id <number>	Specifies an Access Policy I.D. number.
before <number>	Specifies the position of the Access Policy in the list before another Policy.
incoming	Defines the traffic coming in through the Untrusted port.
outgoing	Defines the traffic going out through the Trusted port.
fromdmz	Defines the traffic going out through the DMZ port.
todmz	Defines the traffic coming in through the DMZ port.
<string1>	Name of the source address.
<string2>	Name of the destination address.
<string3>	Name of the service.
auth	Network traffic must be authenticated before passing through the NetScreen device.
permit	Network traffic is permitted to pass through the NetScreen device.
deny	Network traffic is denied passage through the NetScreen device.
encrypt	Network traffic is encrypted by the NetScreen device.
count	Maintains a count in bytes of all network traffic to which the Access Policy is applied.
log	Maintains a log of all connections to which the Access Policy is applied.
alarm	Enables the alarm feature so that you can view alarms. Enter the number of bytes per second or bytes per minute, or both, when you want to trigger an alarm.

<second-threshold>	Use with the alarm argument. Defines the number of bytes per second to trigger an alarm.
<minute-threshold>	Use with the alarm argument. Defines the number of bytes per minute to trigger an alarm.
schedule <name>	If the Access Policy should be enforced during certain times, enter the name of the Schedule to apply to it.
traffic gbw <kbps>	Guaranteed bandwidth at *n* kilobits per second. Traffic below this threshold is passed with highest priority without being subject to any traffic management or shaping.
priority <number>	There are eight priority levels. Traffic with higher priority is passed first, and lower priority traffic is passed only if there is no other higher priority traffic for a certain period of time.
mbw <kbps>	Maximum bandwidth, in kilobits per second. The bandwidth is available to the type of connection specified. Traffic beyond this threshold is dropped.
move <number> {before | after} <number>	Repositions an Access Policy before or after a specified Access Policy in the list.
dip {ip <a.b.c.d> | <e.f.g.h>}	Specifies the dynamic IP address range.
mip <a.b.c.d> netmask <A.B.C.D>	Specifies the mapped IP address and subnet mask.
<src_addr>	Specifies the source address for a tunnel connection.
<dst_addr>	Specifies the termination address for a tunnel connection.
<service>	Specifies the type of service supported.
encrypt	Specifies that the connection be encrypted.
vpn <IKE>	Specifies that the connection is an IKE-class VPN tunnel.
l2tp <name>	Specifies that the connection is an l2tp tunnel with the specified name.

Availability

This feature is supported on all NetScreen device models.

Defaults

No Access Policy is defined.

Examples

To define an Access Policy for an encrypted l2tp tunnel named Desire:

```
ns-> set policy outgoing “Inside Any” “Outside Any” “HTTP” enc l2tp
desire
```

See Also

See the **clear l2tp** command.

port-scan-threshold

Description: Use the **set port-scan-threshold** command to set the threshold value for port scan protection.

Syntax

set port-scan-threshold <micro-seconds>

Arguments

<micro-seconds>	Defines the port-scan threshold in microseconds. The valid range is from 1 to 1,000,000.

Availability

This feature is available on the NetScreen-5, -10, and -100. For the NetScreen-1000, use the **set firewall** command to set the threshold.

Defaults

The default is 30000 microseconds, restored by the **unset** command.

Examples

To set the port scan threshold to 20000 microseconds:

```
ns100-> set port-scan-threshold 20000
```

To restore the port-scan-threshold to the default of 30000 microseconds:

```
ns100-> unset port-scan-threshold
```

See Also

See the **get port-scan-threshold** command.

Notes

This feature counts packets to different destination ports at the same IP. If the number of packets reaches or exceeds 10 within the configured time range, then the device assumes that there is port scan attack and generates alarms. All packets beyond 10 are dropped.

The previously used syntax, **set pscan-threshold**, is hidden for backward compatibility.

pppoe

Description: Use the **set pppoe** command to configure PPPoE.

Syntax

set pppoe {interface <name> | ac <name> | service <name> | static-ip}

set pppoe {authentication {pap | chap | any} | username <string> password <string>}

set pppoe idle-interval <number>

unset pppoe {interface <name> | ac <name> | service <name> | static-ip}

unset pppoe {authentication {pap | chap | any} | username <string> password <string>}

unset pppoe idle-interval <number>

Arguments

interface <name>	Specifies the interface for PPPoE encapsulation.
ac <name>	Allows the interface to connect only to the specified AC.
service <name>	Allows the interface to connect only to the specified service.
static-ip	Specifies that your connection uses the IP addresses assigned by the AC.
authentication {pap | chap | any}	Sets the authentication methods to CHAP, or PAP, or both.
username <string>	Sets the user name.
password <string>	Sets the user password.
idle-interval <number>	Sets the idle timeout—the number of minutes of no activity before the NetScreen takes down the tunnel. Specifying 0 turns off the idle timeout and your tunnel is not taken down because of lack of activity.

Availability

This feature is available on NetScreen-5 device model only.

Defaults

The command is disabled by default. The default authentication method is Any. The default idle timeout is 30 minutes.

Examples

To set the username to Phred, and Phred's password to !@%)&&:

```
ns5-> set pppoe username Phred password !@%)&&
```

See Also

See **get pppoe**, **exec pppoe**, and **clear pppoe** commands.

route

Description: Use the **set route** command to define a static route entry. Static routes help the NetScreen device direct data to different subnets.

Syntax

set route <a.b.c.d> <A.B.C.D> interface {trust | untrust | dmz} [gateway <ip-addr> [metric <number>]]

unset route <a.b.c.d> <A.B.C.D> [gateway <a.b.c.d>]

Arguments

interface	Defines a route to the Trusted, Untrusted, or DMZ in applicable interfaces on the NetScreen device.
trust	The Trusted interface.
untrust	The Untrusted interface.
dmz	The DMZ interface.
gateway <ip-addr>	The IP address of the router that forwards all traffic on the same subnet.
metric <number>	A predefined parameter that defines the priority of the route. Predefined routes have the value “0” and user-defined routes have a value of “1.”

Availability

This feature is supported on all NetScreen device models.

Defaults

By default, one static route entry is defined for each network interface (Trusted, Untrusted, and DMZ) for a NetScreen device running in NAT mode. No entry is defined for a NetScreen device running in Transparent mode.

Examples

To define a static route for an internal subnet with IP address 172.16.15.0 and netmask 255.255.255.0 using an internal router with IP address 172.16.10.4:

```
ns-> set route 172.16.15.0 255.255.255.0 interface trust gateway
172.16.10.4
```

To delete a static route entry for network 244.1.2.0 with netmask 255.255.255.0:

```
ns-> unset route 244.1.2.0 255.255.255.0
```

See Also

See the **get route** command.

Notes

The gateway, or next hop, IP address is optional; if it is absent, the device uses the interface default gateway IP address. The metric is optional; if it is absent, the device sets its value to 1.

When there are multiple route entries for the same subnet in the route table, the NetScreen device uses the one with the lowest metric value.

Note: *The device does not fail over automatically to the other entries, even when the selected route does not work.*

scheduler

Description: Use the **set scheduler** command to create or modify a schedule. Schedules are used to enforce Access Policies at certain times.

Syntax

set scheduler <string>

set scheduler <string> [once start mm/dd/yyyy hh:mm stop mm/dd/yyyy hh:mm [comment <string>]]

set scheduler <string> [recurrent {monday | tuesday | wednesday thursday | friday | saturday | sunday} | start hh:mm stop hh:mm [comment <string>]]

unset scheduler <string> [once | recurrent]

Arguments

<string>	Defines a name for the schedule.
once	Apply the schedule once, starting on the day, month, year, hour, and minute defined, and stopping on the month, day, year, hour, and minute defined.
start	Defines when to start the schedule.
stop	Defines when to stop the schedule.
mm/dd/yyyy	Defines the day, month, and year.
hh:mm	Defines the hour and minutes in the 24-hour clock format.
recurrent	Repeat the schedule according to the defined day of the week, hour, and minutes.
monday	Repeat every Monday.
tuesday	Repeat every Tuesday.
wednesday	Repeat every Wednesday.
thursday	Repeat every Thursday.
friday	Repeat every Friday.
saturday	Repeat every Saturday.
sunday	Repeat every Sunday.

Availability

This feature is supported on all NetScreen device models.

Defaults

None.

Examples

To create a schedule definition named “mytime” which starts on 1/10/1999 at 11:00 AM and ends on 2/12/1999 at 7:00 PM:

```
ns-> set scheduler mytime once start 1/10/1999 11:00 stop 2/12/1999
19:00
```

To create a schedule definition named “weekend” which starts at 8:00 AM and ends at 5:00 PM and repeats every Saturday and Sunday:

```
ns-> set scheduler weekend recurrent saturday start 8:00 stop 17:00

ns-> set scheduler weekend recurrent sunday start 8:00 stop 17:00
```

See Also

See the **get scheduler** command.

SCS

Description: Use the **set scs** command to enable a secure command shell to display information or to configure a NetScreen device from a remote system.

Syntax

set scs enable

set scs key_gen_time <number>

unset scs enable

unset scs key_gen_time

Arguments

enable	Enables the secure shell feature.
key_gen_time <number>	Changes the SCS key regenerating time. The value is set in minutes.

Availability

This feature is available on the NetScreen-100 and NetScreen-1000 models in version 2.0 or later.

Defaults

This feature is disabled by default.

The default key generation time is 60 minutes.

Examples

To enable the secure command shell feature on a NetScreen device:

```
ns-> set scs enable
```

To set the key regeneration time to 15 minutes:

```
ns-> set scs key-gen-time 15
```

See Also

See the **get scs** command.

service

Description: Use the **set service** command to create custom services for use in Access Policies.

Syntax

set service <service_name> [+ | [group {email | info | other | remote | security} | protocol] {<ip_proto_number> | tcp | udp} [src <low_number-high_number> | dst <low_number-high_number>]

set service <service_name> [clear]

set service <service_name> [timeout {<minutes> | never}]

unset service <service_name>

Arguments

<service_name>	Defines a name for the service.
[+]	Appends a service entry to the custom services list.
group {email | info | other | remote | security}	Assigns the service entry to one of these groups or categories: • **email:** Services used for sending and receiving e-mail; for example, IMAP and POP3. • **info:** Services used for seeking and retrieving information; for example, HTTP and DNS. • **other:** Services used for traffic other than that covered by the other four groups; for example, SNMP for network management. • **remote:** Services used for remote access; for example, FTP or RLOGIN. • **security:** Services used for security-related traffic such as encryption, decryption, and authentication; for example, HTTPS and PPTP.
protocol	Defines the service by IP protocol.
<ip_proto_number>	Defines a protocol number for the specified service.
tcp	Defines a TCP-based service.
udp	Defines a UDP-based service.
src-port <low_number-high_number>	Defines a range of source port numbers valid for the service. For example, 100-250.
dst-port <low_number-high_number>	Defines a range of destination port numbers that receive the service request; for example, 300-400.
clear	Clears all service entries.
timeout {<minutes> | never}	Defines the session timeout value for the service in minutes or as “never.”
unset service <service-name>	Removes the specified service from the custom services list.

Availability

This feature is supported on all NetScreen device models.

Defaults

The timeout for TCP connections is 30 minutes.

The timeout for UDP connections is 1 minute.

Examples

To clear all service entries named “test”:

```
ns1000-> set service test clear
```

To set a service named “ipsec” that uses protocol 50:

```
ns1000-> set service ipsec protocol 50
```

To set a service named “test1” that uses destination tcp port 1001:

```
ns1000-> set service test1 protocol tcp src-port 0-65535 dst-port
1001-1001
```

To set a service named “test2” that is categorized as a service for remote access and that uses tcp with a port number 10115:

```
ns1000-> set service test2 group remote tcp src-port 0-65535 dst-port
10115-10115
```

```
ns1000-> set service test2 + udp src-port 0-65535 dst-port 10115-10115
```

To set a service named “telnet” with a timeout value of 10 minutes:

```
ns1000-> set service timeout telnet 10
```

To unset a service named “test”:

```
ns1000-> unset service test
```

See Also

See the **get service** command.

Notes

The maximum timeout value for TCP connections is 40 minutes.

The maximum timeout value for UDP connections is 40 minutes.

snmp

Description: Use the **set snmp** command to configure the NetScreen device for Simple Network Management Protocol (SNMP), which gathers statistical information from the NetScreen device and receives notification when events of interest occur.

Syntax

set snmp auth-trap enable

set snmp {community <community_name> {read-only | read-write} [trap-on [traffic] | trap-off] | contact <contact_name> | host <community_name> <a.b.c.d> | location <location_name> | name <system_name>}

set snmp vpn trust ip <a.b.c.d>

unset snmp {auth-trap enable | community <community_name> | contact | host {<community_name> <a.b.c.d>} | location | name}

Arguments

auth-trap enable	Enables SNMP authentication traps.
community <community_name>	Defines the name for the SNMP community.
read-only	Defines the permission for the community as "read-only."
read-write	Defines the permission for the community as "read-write."
trap-on	Enables SNMP traps for the community.
traffic	Includes traffic alarms as SNMP traps.
trap-off	Disables SNMP traps for the community.
trust	The Trusted interface on the NetSceen device.
contact <contact_name>	Defines the system contact.
host <community_name> <a.b.c.d>	Defines the IP address of the SNMP host.
location <location_name>	Defines the location of the system.
name <system_name>	Defines the name of the system.
vpn	The Virtual Private Network on the remote NetScreen device.

Availability

This feature is available for all NetScreen device models.

Examples

To configure a community named "public" that allows hosts to read Management Information Base II (MIB II) data, as defined in RFC-1213, and receive traps:

```
ns-> set snmp community public read-only trap-on
```

To configure an SNMP host with the IP address 10.20.25.30 for the community named "public":

```
ns-> set snmp host public 10.20.25.30
```

To configure an SNMP host with the IP address 10.40.40.15 for a community named “netscreen” with read and write permission, and allow traps to be sent to all hosts in this community:

```
ns-> set snmp community netscreen read-write trap-on

ns-> set snmp host netscreen 10.40.40.15
```

To allow SNMP packets to pass through a VPN using the Trusted IP address 172.10.40.45 on the remote NetScreen device:

```
ns-> set snmp trust 172.10.40.45
```

See Also

See the **get snmp** command.

Notes

Important: *You must create the community before you can add a host to it.*

To browse the MIB II data and receive traps, obtain an SNMP manager application, such as HP OpenView™. Many shareware and freeware SNMP manager applications are available from the Internet.

syn-threshold

Description: Use the **set syn-threshold** command to set the SYN flood protection threshold, after which the NetScreen device begins to proxy incoming SYN packets.

Syntax

set syn-threshold <number>

unset syn-threshold

Arguments

<number>	The number of SYN requests per second required to activate the firewall SYN proxying protection mechanism.

Availability

This feature is supported on all NetScreen device models, except the NetScreen -1000, which proxies all sessions.

Defaults

The default is 200 SYN requests per second.

Use the **unset** command to restore the default value.

Examples

To set the SYN flood protection threshold to 1000 per second:

```
ns-> set syn-threshold 1000
```

To reset the SYN flood protection threshold to 200 per second:

```
ns-> unset syn-threshold
```

See Also

See the **set firewall**, **set syn-alarm**, **set syn-qsize**, **set syn-timeout**, **get syn-flood**, **get syn-threshold**, and **get firewall** commands.

Notes

When TCP SYN packets exceed the set threshold, subsequent TCP SYN packets are handled by the TCP proxy mechanism in the NetScreen device.

The syn-attack firewall protection takes effect after the number of SYN requests exceeds the specified threshold value within 1 second.

The NetScreen device checks this threshold in one-second intervals. Once the number of SYN requests falls below the threshold, the syn-attack firewall protection switches off.

When the threshold is reached again, the syn-attack firewall protection feature is enabled.

This parameter has no effect if the syn-attack firewall protection is not enabled.

ssl

Description: Use the **set ssl** command to configure a Secure Sockets Layer connection.

Syntax

set ssl {cert <name> | enable | encrypt | port}

unset ssl

Arguments

cert <name>	Specifies that the named certificate is required.
enable	Turns on SSL.
encrypt	Enables encryption over the SSL connection.
port	Specifies the SSL port number.

Availability

This feature is supported on all NetScreen device models.

Defaults

The default SSL port is 443.

Examples

To change the port to 11533:

```
ns-> set ssl port 11533
```

See Also

See the **get ssl** command.

syslog

Description: Use the **set syslog** command to configure the NetScreen device to send traffic and event messages to the Syslog host.

Syntax

set syslog config <a.b.c.d> {auth/sec | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7} {auth/sec | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7} {debug | info | notice | warn | error | crit | alert | emer}

set syslog enable

set syslog vpn

set syslog traffic

set syslog port <number>

set syslog webtrends {enable | hostname {<a.b.c.d> | <name>} | port <number>}

unset syslog

Arguments

config	Defines the configuration settings for the Syslog.
a.b.c.d	Defines the IP address of the Syslog host device.
auth/sec | local0...7	First defines the security facility level, and then the regular facility level. The security facility classifies and sends messages to the Syslog host for security-related actions such as attacks. The regular facility classifies and sends messages for events unrelated to security, such as user logins and logouts, and system status reports.
debug...emer	Specifies the level of Syslog messages to log. Syslog messages are organized hierarchically, and a set level includes that level and all levels above it. For example, an alert setting generates messages for alert and emergency levels, whereas a debug setting generates messages for all levels. The Syslog hierarchy from the lowest level is: **debug**: Logs all messages. **info**: Logs any kind of message not specified in other categories. **notice**: Logs messages for link status changes, load balance server status changes, and traffic logs. **warn**: Logs messages for admin logins and logouts, failures to log in and log out, and user authentication failures, successes, and timeouts. **error**: Logs messages for admin name and password changes. **crit**: Logs messages for url blocks, hsa status changes, and global communications. **alert**: Logs messages for multiple user authentication failures and other firewall attacks not included in the **emer** category. **emer**: Logs messages on syn attacks, tear-drop attacks, and ping-of-death attacks.

enable	Enables the NetScreen device to send messages to the Syslog host.
traffic	Enables the NetScreen device to send traffic logs to the Syslog host.
port <number>	Defines the port number on the Syslog host that receives the User Datagram Protocol (UDP) packets from the NetScreen device.
websense enable	Enables the sending of messages to the Websense server.
hostname <a.b.c.d> | <name>	Defines the IP address or name of the WebTrends server.
port <number>	Defines the port number for the WebTrends Syslog UDP packets.
vpn	The Virtual Private Network IP address on the remote NetScreen.

Availability

This feature is supported on all NetScreen device models.

Defaults

This feature is disabled by default.

The default Syslog port number is 514, and the default WebTrends port number is 514.

Examples

To set the Syslog host configuration with the ability to report all logs:

```
ns1000-> set syslog config 172.16.20.249 auth/sec local0 debug
```

To turn on the Syslog feature:

```
ns1000-> set syslog enable
```

Important: *You must configure the Syslog host before you can enable Syslog.*

To change the Syslog port number to 911:

```
ns1000-> set syslog port 911
```

To set the IP address of the WebTrends server:

```
ns1000-> set syslog webtrends hostname 172.16.20.249
```

To change the port number for the WebTrends server to 715:

```
ns1000-> set syslog webtrends port 715
```

To enable logging to the Websense server:

```
ns1000-> set syslog websense enable
```

Important: *Configure the Websense host IP address before enabling the Websense feature.*

To set a VPN on the Trusted interface for **Syslog**:

```
ns1000-> set syslog vpn trust 172.10.15.40
```

See Also

See the **get syslog** command.

timer

Description: Use the **set timer** command to configure the NetScreen device to automatically execute a management or diagnosis function at a specified time.

Syntax

set timer <mm/dd/yyyy> <hh:mm> action <action>

unset timer <id-number>

Arguments

<mm/dd/yyyy>	Specifies the date when the NetScreen device executes the defined action.
<hh:mm>	Specifies the time when the NetScreen device executes the defined action.
action <action>	Defines the event that the command triggers at the given date and time.
<id-number>	Identifies the specific action by its ID number in the list of timer settings generated by the **set timer** command.

Availability

This feature is supported on all NetScreen devices except the NetScreen-1000.

Examples

To configure NetScreen to reset at a given time and date:

```
ns-> set timer 1/31/2000 19:00 action reset
```

See Also

See the **get timer** command.

Notes

All timer settings remain in the configuration script even after the specified time has expired.

traffic-shaping mode

Description: Use the **set traffic-shaping mode** command to determine the settings for the system-wide traffic-shaping function.

Syntax

set traffic-shaping mode {on | off | auto}

Arguments

{on | off | auto}	Defines the mode settings for the system wide traffic- shaping function. If you select {auto}, the system automatically determines the mode settings. If there is at least one policy in the system with traffic-shaping turned on, the system automatically sets the mode to “on.” If there is no such policy, the automode default setting is “off.”

Availability

This feature is available on all devices except the Netscreen-1000 device model.

Defaults

By default, the traffic-shaping function is set to automatic mode.

Examples

To turn on the traffic shaping function:

```
ns-> set traffic-shaping mode on
```

udp-threshold

Description: Use the **set udp-threshold** command to set a threshold value for udp flooding protection.

Syntax

set udp-threshold <number>

Arguments

<number>	The number of packets allowed per second in a session. When this number is exceeded an alarm is generated, and subsequent packets are dropped. The valid range is from 1 to 1,000,000

Availability

This feature is available on the NetScreen-5, -10, and -100. For the NetScreen-1000, use the **set firewall** command to set the threshold.

Defaults

The default value is 1000, restored by the **unset** command.

Examples

To set the udp threshold to 8000 packets per second:

```
ns1000-> set udp-threshold 8000
```

See Also

See the **get firewall** command.

Notes

Use the **get firewall** command to display the udp flood-protection threshold.

url

Description: Use the **set url** command to enable URL blocking. URL blocking is provided by the WebSense server.

Syntax

set url config {disable | enable}

set url message <string>

set url msg-type {0 | 1}

set url server {<domain_name> | <a.b.c.d>} <port> <timeout>

unset url

Arguments

config {disable}	Disables URL blocking by the Websense server.
config {enable}	Enables URL blocking by the Websense server.
message <string>	Defines a custom message to send to the client who is blocked from reaching a URL.
msg-type {0 | 1}	A "0" uses the message sent by the Websense server. A "1" uses the message configured on the NetScreen device.
server {<domain_name> | <a.b.c.d>} <port> <timeout>	Defines communication with a Websense server with a domain name or IP address <a.b.c.d>, using port number <port> with a timeout value <timeout> in seconds.

Availability

This feature is supported on all NetScreen device models.

Defaults

The default port number for a Websense server is 15868.

Examples

To enable the URL blocking feature:

```
ns-> set url config enable
```

To define the URL blocking message to “This site is blocked”:

```
ns-> set url message “This site is blocked”
```

To use the message from the Websense server:

```
ns-> set url msg-type 0
```

To specify communication with a Websense server with the IP address 209.44.150.6 at port 15868 and a timeout value of 10 seconds:

```
ns-> set url server 209.44.150.6 15868 10
```

See Also

See the **get url** command.

user

Description: Use the **set user** command to create entries in the internal User authentication database.

Syntax

set user <user-name> <password>

set user + <user-name> [dialup <local-spi> <remote-spi> esp {3des {key <192-bit hex> | password <string>} | des {key <64-bit hex> | password <string>} | null} [auth {md5 {key <16-byte hex> | password <string>} | sha-1 {key <20-byte hex> | password <string>}}] | ah {md5 {key <16-byte hex> | password <string>} | sha-1 {key <20-byte hex> | password <string>}}]]

set user <user-name> id <user_id>

set user timeout <number>

set user <username> disable | enable

setuser <username> ike-id <string>

set user <username> password <string>

set user <username> type ike

unset user <user-name>

Arguments

<user-name> <password>	Adds a user name <user_name> and password <password> to the database.
dialup <local-spi> <remote-spi>	For the Manual Key VPN method only. Defines a security parameter index (SPI) number that uniquely distinguishes a particular encrypted tunnel from the others being used at the same time. Only a hexidecimal value between 1000 and 2fffffff is accepted. The local SPI number at one end serves as the remote SPI number at the other end and vice-versa.
esp	For VPN dialup users and dynamic peers. Defines the use of the Encapsulating Security Payload (ESP) protocol.
3des	Specifies the Triple Data Encryption Standard (3DES) algorithm.
key <192-bit hex>	Defines the 192-bit hexidecimal key used in the 3DES algorithm.
password <string>	Defines a password for the generation of a hexidecimal key. The NetScreen device creates a hexidecimal key for the user based upon the password string that the user provides.
des	Specifies the DES encryption algorithm.
key <64-bit hex>	Defines the 64-bit hexidecimal key used in the DES algorithm.
null	Defines “no encryption method” for the ESP protocol.
auth	Defines the use of an authentication method. Choices are MD5 or SHA-1. (Note: Some NetScreen devices do not support SHA-1.)
ah	Defines the use of the Authentication Header (AH) protocol. Choices are MD5 and SHA-1. (Note: Some NetScreen devices do not support SHA-1.)
md5	Sets the device to use the Message Digest version 5 (MD5) algorithm for authentication.
key <16-byte hex>	Defines the 16-byte hexidecimal key used in the MD5 algorithm.

sha-1	Sets the device to use the Secure Hash Algorithm (SHA-1) algorithm for authentication.
key <20-byte hex>	Defines the 20-byte hexidecimal key used in the SHA-1 algorithm.
id <user_id>	Adds and defines an AutoKey IKE dialup user. The ID may be in the form of an IP address (a.b.c.d), a fully qualified domain name (FQDN), or an e-mail name (see RFC822).
timeout <number>	Sets the amount of idle time, in minutes, that the NetScreen device maintains an authenticated status before disengaging the connection.
dns1 <string>	Specifies the name of the primary DNS server.
dns2 <string>	Specifies the name of the secondary DNS server.
id <string>	Configures AutoKey IKE.
ippool <string>	Creates the IP pool with the name specified.
password <string>	Sets the user password.
type <string>	Sets the user type.
wins1 <string>	Specifies the primary WINS server.
wins2 <string>	Specifies the secondary WINS server.

Availability

This feature is supported on all NetScreen device models.

Defaults

None.

Examples

To create a user account in the NetScreen database for user “guest” with the password “testing”:

```
ns-> set user + guest testing 1
```

To create a dialup user account for the user “maryj” using DES encryption based on the password “ipsecmaryj”, with a local-spi defined as 3456 and a remote-spi defined as 7890:

```
ns-> set user + maryj dialup 3456 7890 esp des password ipsecmaryj
```

To create a dynamic peer named “branchsf” with the ID number 12 for an AutoKey IKE VPN tunnel:

```
ns-> set user + branchsf id 12
```

To delete the user account named “maryj”:

```
ns-> unset user maryj
```

See Also

See the **get user**, **set ike**, and **set vpn** commands.

Notes

There are three types of entries for the database: authentication users, VPN dialup users, and IKE dynamic peers. Authentication user entries are used for authentication, while the VPN dialup user and IKE dynamic peer entries are used when defining the Manual Key and AutoKey IKE VPN tunnels. For more information, see the **set vpn** command on page 2-128.

vip

Definition: Use the **set vip** command to define a virtual IP (VIP) address and a virtual port number, and to configure load balancing.

Syntax

set vip {<a.b.c.d> | untrust-ip} [+] <port number> <service> {<e.f.g.h> | <load_balancing_string> <e.f.g.h>/<weight>} [manual]

set vip <a.b.c.d> [+] <port number> <service> <load_balancing_string> <e.f.g.h>/<weight> [manual]

unset vip {<a.b.c.d> | untrust-ip} [port <port number>]

Arguments

<a.b.c.d>	Defines the virtual IP (VIP) address.
untrust-ip	For the NetScreen-5 only. Defines the Untrusted Interface IP address as the VIP.
+	Appends a service to an existing VIP.
<port number>	Defines the virtual port on the VIP address. A mapped IP (MIP) allows you to map the address; however, a VIP allows you to map both the address and the port.
<service>	Specifies one of the 21 predefined services for traffic to the VIP address, including BGP, DNS, Finger, FTP, Gopher, HTTP, HTTPS, IMAP, LDAP, MAIL, NFS, NNTP, NTP, POP3, RIP, SNMP, ssh, Syslog, Telnet, UUCP, and WAIS. The NetScreen-5 also allows you to specify custom services.
ntp	Defines the actual IP address to which the virtual IP address (and port) is mapped.

<load_balancing_string>	For NetScreen-100 only. Specifies one of these load-balancing methods: • **least-conns:** Distributes connection requests to the server that has the fewest active connections. • **none:** No load balancing is applied. • **round-robin:** Distributes connection requests to servers in a rotational sequence. • **weighted-least-conns:** Distributes connection requests to the server that has proportionally the fewest active connections considering overall server capacity. • **weighted-round-robin:** Distributes connection requests to servers in a rotational sequence, but each server is allotted a number of requests in proportion to its overall capacity.
<e.f.g.h>/<weight>	For NetScreen-5, -10, and -100. Defines the weight (percentage) of connection requests sent to the device with the actual IP address <e.f.g.h> for load balancing.
manual	Prevents the NetScreen device from automatically pinging the actual IP address periodically to verify that it is alive and in service.

Availability

The VIP feature is supported on all NetScreen device models. Load balancing is not available on the NetScreen-5, -10, or -1000 models.

Defaults

None.

Examples

To define a VIP for a NetScreen-5 mapping port 8080 for HTTP on the Untrusted IP interface to the actual Trusted IP address 10.1.1.3, and disabling the automatic server detection feature:

```
ns5-> set vip untrust-ip 8080 http 10.1.1.3 manual
```

To define a VIP for a NetScreen-100 mapping the Untrusted IP address 209.125.11.2 to the Trusted IP address 10.1.1.2 for FTP services on port 21:

```
ns100-> set vip 209.125.11.2 21 ftp none 10.1.1.2/1
```

To add HTTP services on port 5050 to an existing VIP that maps traffic from 209.125.11.2 to a server at 10.1.1.2 with a static weight value of 3, using the Weighted Least Conns method for load balancing:

```
ns100-> set vip 209.125.11.2 + 21 http weighted-least-conns 10.1.1.2/3
```

See Also

See the **get vip** command.

Notes

The maximum number of VIPs and the maximum number of services and servers per VIP supported by each NetScreen device are:

	VIPs	Services/VIP	Servers/VIP
NetScreen-5	1	64	64
NetScreen-10	2	64	64
NetScreen-100	4	8	64 (8 server pools with 8 servers in each pool)
NetScreen-1000	6	1	1

vlan

Description: Use the **set vlan** command to create virtual LANs for a NetScreen-1000 device. Later you can define Trusted interfaces and IP addresses for the virtual LANs.

Syntax

set vlan <vlan-name> tag <vlan-tag>

Arguments

vlan-name	Creates a name for the VLAN. This optional argument is designed to help you remember the VLANs you create. A VLAN name must be unique and is limited to 16 characters.
vlan-tag	A VLAN tag is the VLAN identifier (VID). The tag must be a unique value between 1 and 4,096.

Availability

This feature is available only on NetScreen-1000 device models.

Examples

To create a VLAN named “corporate1” with tag number 15:

```
ns1000-> set vlan corporate1 tag 15
```

See Also

See the **set interface**, **get interface**, and **get vlan** commands.

Notes

The NetScreen-1000 supports up to 100 VLANs.

vpn

Description: Use the **set vpn** command to create a Virtual Private Network (VPN). NetScreen devices support two key methods for VPNs—AutoKey IKE and Manual Key. The Internet Key Exchange (IKE) provides a standard method to automatically regenerate encryption keys at user-defined intervals. Manual Key VPNs, on the other hand, use keys that are fixed until they are changed.

Syntax

set vpn <vpn_name> gateway <string> [replay | no-replay | idletime <value>] [tunnel | transport] [idletime <number>] proposal <first P2 string> [second P2 string] [third P2 string] [fourth P2 string]

set vpn <vpn_name> [untrust | trust] manual <local-spi> <remote-spi> gateway <a.b.c.d> [ah {md5 {key <16-byte hex> | password <string>} | sha-1 {key <20-byte hex> | password <string>}] [esp {des {key <64-bit hex> | password <string>} | 3des {key <192-bit hex> | password <string>} | null} [auth {md5 {key <16-byte hex> | password <string>} | sha-1 {key <20-byte hex> | password <string>}]]

set vpn <vpn_name> monitor

unset vpn <vpn_name> monitor

set vpn <vpn_name>

unset vpn <vpn_name>

set vpn single-ike-tunnel

unset vpn single-ike-tunnel

Arguments

<vpn_name>	Defines a name for the VPN.
gateway <a.b.c.d> | <domain_name>	Defines the Untrusted IP address or the domain name of the remote security gateway. This can be a NetScreen unit or any other IPSec-compatible device.
replay | no-replay	Specifies whether replay protection is enabled or disabled. The default setting is no-replay.
proposal <p2_proposalx>	Defines the Security Association for a Phase 2 proposal.
manual	Specifies a Manual Key key method. When in Manual mode, you can choose to encrypt and authenticate by either HEX key or password.
<local-spi>	For a Manual Key VPN only. Defines a security parameters index (SPI) number that uniquely distinguishes a particular tunnel from the others being used at the same time. Only a hexidecimal value between 3000 and 2fffffff is accepted. The Local Security Index serves as the Remote Security Index at the other end and vice-versa.
<remote-spi>	For a Manual Key VPN only. Defines an SPI number that uniquely distinguishes a particular tunnel from the others being used at the same time. Only a hexidecimal value between 3000 and 2fffffff is accepted. The Remote Security Index serves as the Local Security Index at the other end and vice-versa.
gateway <a.b.c.d>	Defines the Untrusted IP address of the remote security gateway. This can be a NetScreen unit or any other IPSec-compatible device.
esp	Specifies the use of the Encapsulating Security Payload (ESP) protocol to encrypt and authenticate the encapsulated IP packet. Choices are NULL (for “no encryption”), DES, or 3DES.
des	Specifies the Data Encryption Standard (DES) algorithm.
key <64-bit hex>	Defines a 64-bit hexidecimal encryption key.

password <string>	Specifies a password that the NetScreen device uses to generate an encryption or authentication key automatically.
3des	Specifies the Triple Data Encryption Standard (3DES) algorithm.
key <192-bit hex>	Defines a 192-bit encryption key.
null	When used with ESP, defines "no encryption method." When used with auth, defines "no authentication method."
auth	Specifies the use of an authentication method. Choices are MD5 or SHA-1. (Some NetScreen devices do not support SHA-1.)
md5	Specifies the Message Digest (version) 5 (MD5) algorithm for authentication.
key <16-byte hex>	Defines a 16-byte hexidecimal key, used to produce a 128-bit message digest (or hash) from a message of arbitrary length.
sha-1	Specifies the Secure Hash Algorithm (version) 1 (SHA-1) algorithm for authentication.
key <20-byte hex>	Defines a 20-bit hexidecimal key, used to produce a 160-bit message digest.
ah	Specifies the use of the Authentication Header (AH) protocol to authenticate the encapsulated IP packet. Choices are MD5 and SHA-1.
monitor	Monitors the specified VPN.
single-ike-tunnel	Limits a single IKE tunnel between two VPN gateways. This feature is disabled by default, which allows multiple IKE tunnels between two VPN gateways in release ScreenOS 2.5 or higher.

Availability

This feature is supported on all NetScreen models that support encryption.

3-DES is not available on NetScreen-10e and NetScreen-100e.

SHA-1 is not available on NetScreen-10s with serial numbers xyzzaaaa where y<2 and zz<99, or on NetScreen-100s with serial numbers xyzzaaaa where y<2 and zz<99.

The **monitor** argument is available on NetScreen models at version 2.0 or later.

Defaults

The key lifetime is set to 3600 seconds.

The default ESP authentication algorithm is NULL.

Examples

To create a manual VPN named “judy” with the local and remote SPIs defined as 00001111 and 00002222, the remote gateway IP address set at 170.45.33.2, ESP with DES and MD5 using keys generated from the password “judyvpn”:

```
ns-> set vpn judy manual 00001111 00002222 gateway 170.45.33.2 esp des
password judyvpn auth md5 password judyvpn
```

To create an AutoKey IKE VPN named “tuvalu” with the remote gateway defined by its domain name, “funafuti.com”, replay protection enabled, and a Phase 2 proposal consisting of a Diffie-Hellman Group 2 exchange, and ESP with Triple DES and SHA-1:

```
ns-> set vpn tuvalu gateway funafuti.com replay proposal g2-esp-3des-
sha
```

See Also

See the **get vpn** and **set ike** commands.

Notes

If you try to use the SHA-1 parameter with a NetScreen device that does not support it, the error message “This device doesn't support SHA-1 Authentication” appears.

If you enter the **set vpn <name1> trust gateway** command, the error message “AutoKey VPN is not supported on trust interface” appears.

VPN users having different IPSec parameters can be grouped and specified by a single VPN policy.

vsys

Description: Use the **set vsys** command to create Virtual Systems on a NetScreen-1000 device. The NetScreen-1000 provides multi-tenant services through Virtual Systems, each of which is a unique security domain with its own management. You can configure up to 100 Virtual Systems on a single NetScreen-1000 device to set up independent, configurable functions for up to 100 different organizations.

Syntax

set vsys <virtual_system_name>

unset vsys <virtual_system_name>

Arguments

<virtual_system_name>	Creates a Virtual System with the name <virtual_system_name>. Automatically places the console within the Virtual System so that subsequent commands configure the new Virtual System.

Availability

This feature is available only on NetScreen-1000 devices.

Examples

To create a Virtual System named “organization3” and switch the console to the new Virtual System:

```
ns-> set vsys organization3
```

See Also

See the **get vsys**, **enter vsys**, and **exit** commands.

Notes

To access a Virtual System, issue the **enter vsys** command. Use the **unset vsys** command to remove all configuration settings for a specific Virtual System and thus free the resources associated with that Virtual System.

Get Commands 3

Use the Get commands to display system configuration parameters and data on the console.

To redirect the output of a Get command to a tftp server as a text file, enter a greater-than sign (>) for every Get command.

get address > tftp <a.b.c.d> <filename>

Example

ns-> **get address > tftp 1.2.3.4 addr.txt**

active-user

Description: Use the **get active-user** command to display a list of all trusted IP addresses with incoming or outgoing sessions passing through the NetScreen device.

Syntax

get active-user

Arguments

None.

Availability

This feature is available only on the NetScreen-5 device model.

Examples

To display a list of the trusted IP addresses, their incoming and outgoing sessions, and release timeout for the NetScreen device:

```
ns-> get active-user
```

See Also

See the **clear active-user** command.

address

Description: Use the **get address** command to display all entries in the Address Book.

Syntax

get address [dmz | trust | untrust] [group <group name>]

Arguments

dmz	Displays the addresses for the DMZ interface (if applicable).
group	Displays the address groups for each respective interface.
trust	Displays the addresses for the Trust interface.
untrust	Displays the addresses for the Untrust interface.

Availability

This feature is supported on all NetScreen device models. However, the DMZ option is not supported on the NS-5 device.

Examples

To display Address Book entries for the DMZ interface:

```
ns-> get address dmz
```

To display Address Book entries for the Trusted interface:

```
ns-> get address trust
```

To display Address Book entries for the Untrusted interface:

```
ns-> get address untrust
```

To display the Trusted address groups:

```
ns-> get address trust group <group name>
```

See Also

See the **set address** command.

Notes

The display for each Address Book entry shows the name, IP address, netmask, flag, and comments for the entry.

admin

Description: Use the **get admin** command to display the system administration parameters.

Syntax

get admin [mng-ip | user | current-user]

Arguments

mng-ip	Displays the IP address and subnet mask of the management workstation.
user	Lists the names of all users of the device.
current-user	Lists only the name of the current user of the device; that is, the user entering the command.

Availability

This feature is supported on all NetScreen device models.

Examples

To show all the administrative parameters for the NetScreen device:

```
ns-> get admin
```

To show the names of the administrators:

```
ns-> get admin user
```

See Also

See the **set admin** command.

Notes

The **get admin** command displays these system administration configuration parameters:

- system IP address and port number for Web management
- mail alert status
- e-mail server IP address or server name
- remote e-mail address or addresses for the recipients of e-mail alert notification
- status for sending the traffic log through e-mail
- configuration format—DOS or UNIX

alarm

Description: Use the **get alarm** command to display alarm entries.

Syntax

get alarm

get alarm event [start-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>] [end-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>] [include <include_string>] [exclude <exclude_string>] [begin <begin_string>]

get alarm traffic [policy {<policy_id> | <policy_id_range>}] [service <service_name>] [src <address_string>] [dst <address_string>] [detail [start-time <dd/mm/yyyy-hh:mm:ss>] [end-time <dd/mm-hh:mm>] [{second | minute} [threshold <value> | <range>] [rate <value> | <range>]]]

Arguments

event	Specifies event alarm entries.
start-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>	Displays event alarm entries that occurred at and after the time specified—day/month/year hour:minute:second. You can omit the year, in which case the current year is assumed, or you can write the year with either the last two digits only or with all four. Also, the hour, minute, and second can be omitted. You can separate the date from the time with a space, a dash, or an underscore: • "12/31/2001 23:59:00" • 12/31/2001-23:59:00 • 12/31/2001_23:59:00
end-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>	Displays event alarm entries that occurred at and before the time specified.
include <include_string>	Displays event alarm entries that include the detail specified.
exclude <exclude_string>	Displays event alarm entries that exclude the detail specified.
begin <begin_string>	Displays event alarm entries that follow a specified alarm event.

traffic	Specifies traffic alarm entries.
policy <policy_id> | <policy_id_range>	Displays traffic alarm entries for an Access Policy specified by its ID number or for several Access Policies specified by a range of ID numbers. The ID number can be any value between 0 and the total number of established Access Policies. To define a range, enter the starting and ending ID numbers as follows: **<policy_id>-<policy_id>**
service <service_name>	Displays traffic alarm entries for a specified Service, such as TCP, ICMP, or FTP. (Type "**Any**" to display all services.) The name does not have to be complete; for example, both "TC" and "CP" are recognized as "TCP". Although you cannot specify a Service group, note that because "TP" is recognized as "FTP", "HTTP", and "TFTP", entering "TP" displays traffic alarm entries for all three of these Services.
src <address_string>	Displays traffic alarm entries originating from a specified IP address or from a specified direction, such as "Inside_Any" or "Outside_Any".
dst <address_string>	Displays traffic alarm entries destined for a specified IP address or for a specified direction, such as "inside_any" or "outside_any".
detail	Displays detailed information for each Access Policy, including all the traffic alarm entries that occurred under it. If this argument is not included in the command, the output contains only general information about Access Policies and only the time of the most recent alarm for each Access Policy.
start time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>	Displays traffic alarm entries that occurred at and after the time specified—day/month/year-hour:minute:second.
end-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>	Displays traffic alarm entries that occurred at and before the time specified—day/month-hour:minute.

second | minute	Displays traffic alarm entries for Access Policies with threshold settings at bytes/second or bytes/minute.
threshold <value> | <range>	Displays traffic alarm entries for Access Policies with threshold settings at a specified value or within a specified range.
rate <value> | <range>	Displays traffic alarm entries for Access Policies with a flow rate at a specified value or within a specified range.

Availability

This feature is completely supported on the NetScreen-1000. All other NetScreen device models support this basic element of the command:

get alarm

Defaults

If you do not include any arguments, the **get alarm** command displays all alarm entries and Access Policy information, the **get alarm event** command displays all event alarm entries, and the **get alarm traffic** command displays all traffic alarm entries.

Examples

To display all alarm entries:

```
ns-> get alarm
```

To show event alarm entries:

```
ns-> get alarm event
```

To show all traffic alarm entries:

```
ns-> get alarm traffic
```

To show traffic alarm entries for an Access Policy with ID number 4:

```
ns-> get alarm traffic policy 4
```

To show all event alarm entries from 1:30 P.M. on February 28, 2000:

```
ns1000m-> get alarm event start-time 02/28/2000-13:30
```

To show all event alarm entries from 1:30 P.M. to 1:39:59 P.M. on February 28, 2000:

```
ns1000m-> get alarm event start-time 02/28/00_13:30 end-time 02/28
13:39:59
```

To show all event alarm entries from 1:30 P.M. to 1:39:59 P.M. on February 28, 2000 except for Access Policy changes:

```
ns1000m-> get alarm event start-time 02/28/00_13:30 end-time 02/28
13:39:59 exclude "policy change"
```

To show all event alarm entries on traffic originating from the Trusted side:

```
ns1000m-> get alarm event include trust exclude untrust
```

Because strings are not considered as whole words, ***include trust*** *shows all events for the "Trusted" as well as "Untrusted" sides. To restrict the display to only events from the Trusted side, add the* ***exclude untrust*** *string.*

To show event alarm entries that occurred after the entry "At least one fan is not functioning properly":

```
ns1000m-> get alarm event begin fan
```

To show traffic alarm entries for HTTP service:

```
ns1000m-> get alarm traffic service http
```

To show traffic alarm entries for all traffic originating from the Untrusted side:

```
ns1000m-> get alarm traffic src outside_any
```

To show traffic alarm entries for all incoming traffic destined for the server with IP address 162.40.1.24:

```
ns1000m-> get alarm traffic src outside_any dst 162.40.1.24
```

To show detailed information on all traffic alarm entries:

```
ns1000m-> get alarm traffic detail
```

To show detailed information on traffic alarm entries for all Access Policies with alarm thresholds set within the range of 1000–20,000 bytes/second:

```
ns1000m-> get alarm traffic detail second threshold 1000-20000
```

To show detailed information on all traffic alarm entries for outgoing traffic using TCP operating under Access Policies within the ID range of 3–7 on May 27, 2000 from 4:00 P.M. to 4:59:59 P.M:

```
ns1000m-> get alarm traffic policy 3-7 service TCP src inside_any
detail start-time 05/27/00_16:00 end-time 05/27_16:59:59
```

See Also

See the **clear alarm** command.

Notes

The console displays the maximum number of alarms that the NetScreen device can maintain and the current number of entries in the table.

When getting alarm entries from within a Virtual System or from within the main system on the NetScreen-1000, only the entries from that particular Virtual System or main system are displayed. Alarm entries from other Virtual Systems are not displayed.

arp

Description: Use the **get arp** command to display the entries in the Address Resolution Protocol (ARP) table.

Syntax

get arp

Arguments

None.

Availability

This feature is supported on all NetScreen device models.

Examples

To display all the entries in the arp table:

```
ns-> get arp
```

See Also

See the **set arp** and **clear arp** commands.

Notes

The **get arp** command displays the entries in the ARP table in this format:

- the IP address for the system sending network traffic through the NetScreen device
- the corresponding MAC address for the system
- the type of interface to which the system is connected: Trusted, Untrusted, or DMZ
- the age of the entry in seconds

The ARP table may contain a maximum of 256 entries.

auth

Description: Use the **get auth** command to display the user authentication configuration settings.

Syntax

get auth [queue | settings | table]

Arguments

queue	Applies only if using a RADIUS server or SecurID server to authenticate users. Displays a list of authentication requests waiting to be processed.
settings	The display varies depending upon the authentication method being used. When using the NetScreen internal database, displays the timeout value for the authenticated entry. When using the RADIUS server, displays the timeout value for the authenticated entry, the IP address for the RADIUS server, and the shared secret. When using the SecurID server, displays these values: • The authentication port number • The number of bad PRNs and PINs • The SecurID Master server name, and the SecurID Slave server name, if used • Whether duress is used • The type of encryption • The maximum number of retries • The communication timeout value • The authenticated entry timeout value. When using the LDAP server, displays the authenticated entry timeout value, the IP address of the LDAP server, and its listening port. Displays the distinguished name and common name identifier.
table	Displays a table of IP addresses from which authentication requests are originating, and how much time each entry has before being deleted. Also displays whether authentication attempt is successful or not.

Availability

This feature is supported on all NetScreen device models.

Examples

To display the authentication queue:

```
ns-> get auth queue
```

To display the authentication settings:

```
ns-> get auth settings
```

To display the authentication table:

```
ns-> get auth table
```

See Also

See the **set auth** and **clear auth** commands.

Notes

When a user authentication attempt is successful, an entry is created in the NetScreen authentication table. Each entry is assigned a timeout value. Once the entry reaches its timeout value it is deleted, and any new traffic initiated from the same machine requires new authentication.

NetScreen supports a maximum number of 4096 entries in this table. If the table is full, new attempts at authentication are rejected and must be retried.

chassis

Description: Use the **get chassis** command to display the status of the processing board's slot occupation and activity, the power supply, the fan, and the temperature in both Celsius and Fahrenheit.

Syntax

get chassis

Arguments

None.

Availability

This feature is supported only on the NetScreen-1000.

Example

To display the status of board slot 1:

```
ns-> get chassis slot1
```

clock

Description: Use the **get clock** command to display the system time on the NetScreen device.

Syntax

get clock

Arguments

None.

Availability

This feature is supported on all NetScreen device models.

Examples

To display the system time for the NetScreen device:

```
ns-> get clock
```

See Also

See the **set clock** command.

Notes

The display includes the current date in calendar format as well as the number of seconds since 1/1/1970 GMT. It calculates the uptime for the NetScreen device since the device was last powered.

config

Description: Use the **get config** command to display the current or saved configuration settings for a NetScreen device.

On the NetScreen-1000, use this command to copy the configuration settings from the root system or from a Virtual System of the NetScreen device to a TFTP server connected to the Trusted or Untrusted interface. Also, use the **get config** command to download a configuration file from a TFTP server to the PCMCIA card in slot 1 or 2 of the device.

Syntax

get config [saved]

For the NetScreen-1000:

get config [saved] [# {slot <slot_number>}]

get config [slot1 <file_name> | [# {slot <slot_number> | vsys <virtual-system_name>} | >tftp <a.b.c.d> <file_name>]

get config [slot2 <file_name> | [#{slot <slot_number> | vsys <virtual-system_name>} | >tftp <a.b.c.d> <file_name>]

Arguments

saved	Displays the configuration file saved in flash memory.
# slot <slot_number> | vsys <virtual-system_name>	For the NetScreen-1000. Selects output from the PCMCIA card in slot 1 or 2, or from the Virtual System <virtual-system_name>.
> tftp <a.b.c.d> <file_name>	For the NetScreen-1000. Redirects output to the file <file_name> on the Trivial File Transfer Protocol (TFTP) server at IP address <a.b.c.d>.
slot1 <file_name>	For the NetScreen-1000. Specifies the configuration file <file_name> in slot 1.
slot2 <file_name>	For the NetScreen-1000. Specifies the configuration file <file_name> in slot 2.

Availability

This feature is supported on all NetScreen device models.

Examples

To display the current runtime configuration on the console:

```
ns-> get config
```

To display the configuration saved in the flash memory:

```
ns-> get config saved
```

To download a configuration file named “new_cnfg” from a TFTP server at 156.24.54.9 to the PCMCIA card in slot 1 on the NetScreen-1000:

```
ns1000-> get config tftp 156.24.54.9 new_cnfg # slot 1
```

To download a configuration file named “ns_cnfg” from a TFTP server at 156.24.54.9 to a Virtual System named “cyborg”:

```
ns1000-> get config tftp 156.24.54.9 ns_cnfg # vsys cyborg
```

To copy a configuration file named “cnfg5” from the PCMCIA card in slot 1 to a file named “ns_cnfg5” in a TFTP server at 125.34.156.9:

```
ns1000-> get config slot1 cnfg5 >tftp 125.34.156.9 ns_cnfg5
```

See Also

See the **save** command.

console

Description: Use the **get console** command to display the console parameters.

Syntax

get console

Arguments

None.

Availability

This feature is supported on all NetScreen device models.

Examples

To display all console parameters:

```
ns-> get console
```

See Also

See the **set console** command.

Notes

The **get console** command displays this console configuration information:

- the timeout value
- the number of lines to display per screen
- where the debug messages are displayed
- the number of active connections to the NetScreen device through the console or Telnet, and the duration of these connections
- for a Telnet connection, the IP address for the client machine

counter

Description: Use the **get counter** command to display system and traffic information on the NetScreen interfaces.

Syntax

get counter {flow [slot# <number>] | interface [slot# <number>] | policy <number> {day | hour | minute | month | second}}

Arguments

flow	Specifies counters for packets inspected at the flow level. A flow-level inspection examines various aspects of a packet to gauge its nature and intent.
slot# <number>	For the NetScreen-1000 only. Specifies the slot number of a processing board.
interface	Specifies counters for packets inspected at the interface level. An interface-level inspection checks for packet errors and monitors the quantity of packets in light of established threshold settings.
policy <number>	Identifies a particular Access Policy, allowing the administrator to monitor the amount of traffic it permits.
day | minute | month | second	For the NetScreen-1000 only. Specifies the period of time for monitoring traffic permitted by a particular Access Policy.

Availability

This feature is supported on all NetScreen device models. Monitoring traffic by slot number or by Access Policy is possible only on the NetScreen-1000.

Notes

Use this command for technical support only.

This system information is displayed for flow-level counters:

- tiny frag – the number of tiny fragmented packets received
- tear drop – the number of oversize Internet Control Message Protocol (ICMP) packets received
- src route – the number of packets dropped when using the filter source route option
- pingdeath – the number of suspected ping-of-death attack packets received
- addr spf – the number of suspected address spoofing attack packets received
- land att – the number of suspected land attack packets received
- no route – the number of unroutable packets received
- no conn – the number of packets dropped due to unavailable Network Address Translation (NAT) connections
- poli deny – the number of packets denied by a defined Access Policy
- auth fail – the number of times user authentication failed
- no dip – the number of packets dropped because no Dynamic IP (DIP) addresses were available
- no map – the number of packets dropped because no map to the Trusted side existed
- url block – the number of HTTP requests blocked
- tcp proxy – the number of packets dropped when using a tcp proxy, such as syn flood protection or user authentication
- no gate – the number of packets dropped because no gate was available
- no parent – the number of packets dropped because the parent connection could not be found
- no g-gate – the number of packets dropped because the Network Address Translation (NAT) connection was unavailable for the gate

- nvec err – the number of packets dropped due to NAT vector error
- trmn drp – the number of packets dropped by traffic management
- trmng que – the number of packets waiting in the queue
- big bkstr – an excessively large number of Address Resolution Protocol (ARP) packets attempting to uncover the Media Access Control (MAC) address for an IP address
- enc fai – the number of failed Point-to-Point Tunneling Protocol (PPTP) packets
- lpbk deny – the number of packets dropped because the packets can't be looped back
- no sa – the number of packets dropped because no Security Associations (SA) was defined
- no sapoli – the number of packets dropped because no Access Policy was associated with an SA
- sa inact – the number of packets dropped because of an inactive SA
- sapoli dn – the number of packets denied by an SA policy
- illegal – the number of packets dropped because they are illegal packets

This traffic information is displayed for interface-level counters:

- in pak – the number of packets received
- in vpn – the number of IPSec packets received
- out pak – the number of packets sent
- out bpak – the number of packets held in back store while searching for an unknown MAC address
- in crc – the number of incoming packets with a cyclic redundancy check (CRC) error
- in alg – the number of incoming packets with an alignment error in the bit stream
- in nobuf – the number of unreceivable packets because of unavailable buffers
- in short – the number of incoming packets with an "in-short" error

- in err – the number of incoming packets that have at least one error
- in coll – the number of incoming collision packets
- out unr – the number of transmitted underrun packets
- early fr – counters used in an ethernet driver buffer descriptor management
- late fr – counters used in an ethernet driver buffer descriptor management
- in icmp – the number of Internet Control Message Protocol (ICMP) packets received
- in self – the number of packets addressed to the NetScreen Management IP address
- in unk – the number of UNKNOWN packets received
- connection – the number of sessions established since the last boot

dhcp client

Description: Use the **get dhcp client** command to display the IP address for the Untrusted interface for the NetScreen device, its Dynamic Host Configuration Protocol (DHCP) server IP address, and the status of the NetScreen device.

Syntax

get dhcp client

Arguments

None.

Availability

This feature is available on the NetScreen-5 and -10 at version 1.65 or later.

Examples

To display information relevant to the DHCP client:

```
ns-> get dhcp client
```

See Also

See the **set dhcp client**, **clear dhcp client ip**, and **exec dhcp client renew** commands.

dhcp server

Description: Use the **get dhcp server** command to display the current Dynamic Host Configuration Protocol (DHCP) settings.

Syntax

get dhcp server

get dhcp server ip [idle | allocate | committed]

Arguments

server	Displays all the DHCP parameters and settings.
server ip	Displays all the IP addresses used by the DHCP server. The information includes the range of IP addresses being used, whether the status is “idle” or “allocate”, the lease time, and a MAC address, if applicable. An asterisk (*) next to an IP address indicates that it is reserved. An asterisk (*) next to a MAC address indicates the unregistered user for this IP (when the share-ip option is enabled).
server ip idle	Displays only the idle IP addresses in the range for the DHCP server.
server ip allocate	Displays only the allocated IP addresses in the range for the DHCP server.
server ip committed	Indicates the IP address is taken by a user.

Availability

This feature is available on the NetScreen-5 and -10 at version 1.63 or later.

Examples

To display the range of IP addresses used by the DHCP server:

```
ns-> get dhcp server ip
```

To display the IP addresses that are idle for the DHCP server:

```
ns-> get dhcp server ip idle
```

To display the IP addresses that are being used by the DHCP server:

```
ns-> get dhcp server ip allocate
```

See Also

See the **clear dhcp** and **set dhcp** commands.

Notes

An asterisk (*) next to an IP address indicates it is reserved. An asterisk next to a Media Access Control (MAC) address indicates it is assigned to an unregistered user.

dialup-group

Description: Use the **get dialup-group** command to display the dialup group configuration parameters.

Syntax

get dialup-group [all | id <number>]

Arguments

all	Displays the dialup group ID, name, and the total number of members for all the configured dialup groups.
id <number>	Displays detailed information for a specific dialup group with ID <number>. The information includes the names of the members in the group, and their SPI values for the manual key dialup user, or the ID and ID-type for the the IKE dialup user.

Availability

This feature is available on all NetScreen models that support encryption and Virtual Private Networking.

Examples

To display all dialup-group configurations:

```
ns-> get dialup-up all
```

To display the configuration settings for the dialup-group with ID number 4:

```
ns-> get dialup-up id 4
```

See Also

See the **set dialup-group** command.

dip

Description: Use the **get dip** command to display the dynamic IP (DIP) configuration for the NetScreen device.

Syntax

get dip [id <number>]

Arguments

id <number>	Displays the dynamic IP (DIP) settings for the DIP with the specified ID number <number>. If you do not specify an ID number, the **get dip** command displays all the DIP settings.

Availability

This feature is supported on all NetScreen device models.

Examples

To show a specific DIP configuration with ID number 4:

```
ns-> get dip id 4
```

To display all DIP configurations:

```
ns-> get dip
```

See Also

See the **set dip** command.

domain

Description: Use the **get domain** command to view the domain name of the NetScreen device.

Syntax

get domain

Arguments

None.

Availability

This feature is available on all NetScreen device models.

Example

To get the domain name of the NetScreen-1000:

```
ns1000-> get domain
```

See Also

See the **set domain** command.

envar

Description: Use the **get envar** command to display the environment variable settings.

Syntax

get envar

Arguments

None.

Availability

This feature is available on all device models except the NetScreen-5.

Example

To display the environment variable settings you specified with the **set envar** command:

```
ns1000-> get envar
```

See Also

See the **set envar** command.

file

Description: Use the **get file** command to display information for files stored in the flash memory. If you have a NetScreen-1000, the **get file** command also displays the configuration settings stored on the PCMCIA cards in the device.

Syntax

get file [<file_name>]

get file [<device> [:<file_name>]]

Arguments

file name	Defines the file name stored in the flash card memory.
device	Defines the PCMCIA slot number in the NetScreen-1000: "slot1" for the card in slot 1 or "slot2" for the card in slot 2.

Availability

This feature is available on all NetScreen device models.

Examples

To display information for the file named "corpnet" from the flash card memory:

```
ns-> get file corpnet
```

To display the configuration files stored in flash memory, as well as those on the PCMCIA cards in the NetScreen-1000 device:

```
ns-> get file
```

To display all configuration files stored on the PCMCIA card in slot 1 in the NetScreen-1000 device:

```
ns-> get file slot1
```

To display the configuration file named "config100" stored on the PCMCIA card in slot 2 on the NetScreen-1000 device:

```
ns-> get file slot2:config100
```

See Also

See the **clear file** and **save** commands.

firewall

Description: Use the **get firewall** command to display firewall protection settings and to display whether log-self-deny is enabled or not.

Syntax

get firewall

Availability

This feature is supported on all NetScreen device models.

Examples

To display the firewall protection settings:

```
ns-> get firewall
```

See Also

See the **set firewall** command.

Notes

"On" means the feature is enabled. "Off" means the feature is disabled.

The **get firewall** command displays whether the logging of dropped packets feature is enabled or not.

global

Description: Use the **get global** command to display the NetScreen-Global Manager settings.

Syntax

get global

Arguments

None.

Availability

This feature is available on the NetScreen-5, -10, and -100, and the NetScreen-1000.

Examples

To display the NetScreen-Global Manager settings:

```
ns-> get global
```

See Also

See the **set global** command.

Notes

The **get global** command displays:

- If the NetScreen-Global Manager feature is enabled
- the IP address of the NetScreen-Global Manager station
- the NetScreen-Global Manager server configuration port and the server reporting port
- the local listening port for the NetScreen device
- if the VPN encryption feature is enabled or not
- the type of reports that the NetScreen-Global Manager station requests

group

Description: Use the **get group** command to display the address groups and service groups configured on the NetScreen device.

Syntax

get group address {trust | untrust | dmz} [<address-group-name>]

get group service [<service-group-name>]

Arguments

address	Defines the group as an Address group.
trust | untrust | dmz	Specifies the Trusted, Untrusted, or DMZ interface for the Address or Service group.
<address-group-name>	Specifies the name of an Address group.
service	Defines the group as a Service group.
<service-group-name>	Specifies the name of a Service group.

Availability

This feature is available on all NetScreen device models at version 2.0 or later. The DMZ interface option is available only on the NetScreen-10 and -100.

Examples

To display an Address group named “engineering” for the Trusted interface:

```
ns-> get group address trust engineering
```

To display a Service group named “inside-sales”:

```
ns-> get group service inside-sales
```

To display all Address groups for the Untrusted interface:

```
ns-> get group address untrust
```

To display all Service groups:

```
ns-> get group service
```

See Also

See the **set group** command.

hostname

Description: Use the **get hostname** command to display the hostname of the NetScreen device.

Syntax

get hostname

Arguments

None.

Availability

This feature is available on all NetScreen device models.

Examples

To display the name of the NetScreen device:

```
ns-> get hostname
```

See Also

See the **set hostname** command.

ha

Description: Use the **get ha** command to display the configuration settings for high availability.

Syntax

get ha

Arguments

None.

Availability

This feature is available on all NetScreen-100 and NetScreen-1000 device models.

Examples

To display the high availability group information:

```
ns-> get ha
```

Notes

The **get ha** command displays:

- to which high availability groups the NetScreen device belongs
- whether the NetScreen device is designated as “master” or “slave”
- the MAC addresses for the devices in the group

ha track ip

Description: Use the **get ha track ip** command to view the status of the IP addresses included in the list of tracked IP addresses configured on the system.

Syntax

get ha track ip

Arguments

None.

Availability

The **get ha track ip** command is available on the NetScreen-1000 model only.

Example

This table displays the result of a **get ha track ip** command for two tracked IP addresses.

```
ns-> get ha track ip
```

ip address	interval	threshold	interface	fail-count	success-rate
172.16.20.100	1	20	trust	3	95%
172.16.20.101	5	100	none	0	98%

See Also

See the **set ha** command.

Notes

The **get ha track IP** command is available only at root level, and not in virtual system mode.

You can issue the command using the domain name instead of the IP address.

You can allow multiple classes of track-IPs and set different parameters for each of them. For example, you might allow only one death in a critical class before failover occurs, but allow 15 deaths in a non-critical class before failover.

See Also

See the **set ha track ip** and **set ha** commands.

icmp-threshold

Description: Use the **get icmp-threshold** to display the threshold value for icmp flooding protection.

Syntax

get icmp-threshold

Arguments

None.

Availability

This feature is available on all NetScreen models.

Examples

To display the icmp ping threshold:

```
ns1000-> get icmp-threshold
```

See Also

See also **set icmp-threshold**.

ike

Description: Use the **get ike** command to display the current connections, cookies, and the preshared key ring for Internet Key Exchange (IKE).

Syntax

get ike {accept-all-proposal | conn-entry | cookies | id-mode | policy-checking | p1-proposal <name> | p2-proposal <name> | gateway <name>}

Arguments

accept-all-proposal	Shows if all incoming proposals are accepted or not.
conn-entry	Displays the current connections.
cookies	Displays all IKE cookies.
id-mode	Shows if the IKE ID mode is the IP address only or is includes the subnet.
policy-checking	Shows if the Access Policies for both VPN participants must match before a VPN connection is established.
p1-proposal <name>	Shows the details of the phase one proposal.
p2-proposal <name>	Shows the details of the phase two proposal.
gateway <name>	Shows the details of the remote gateways.

Availability

This feature is available on NetScreen devices that include firewall and VPN encryption features.

Examples

To display all the details of the Phase 1 proposal “sf1”:

```
ns-> get p1-proposal sf1
```

To display all the currently running Phase 2 IKE connections:

```
ns-> get ike conn-entry
```

To display all IKE cookies:

```
ns-> get ike cookies
```

See Also

See the **set ike** and **clear ike** commands.

interface

Description: Use the **get interface** command to display the network interface settings for the NetScreen device.

Syntax

get interface [dmz | trust | untrust]

Arguments

None.

Availability

This feature is supported on all NetScreen device models.

Examples

To display general information for all network interfaces:

```
ns-> get interface
```

To display detailed information for a trusted interface:

```
ns-> get interface trust
```

See Also

See the **set interface** command.

Notes

The **get interface** command displays this information:

- the System IP address, which is the IP address used for system administration either through the Web management interface or the Telnet protocol.
- the Web management interface port number.
- the Admin IP address, which specifies either a single machine or a network of machines from which the administrator can access the Web management interface.
- the User name, which is the login name the administrator enters to log on to the NetScreen device for system administration either through the Web management interface or the Telnet protocol.

- the MAC address, IP address, and netmask for each interface
- the status of the interface, including the speed obtained through auto-sensing
- the ability to respond to the **ping** command for each interface
- the Manage IP address (the IP address used to perform Web management from a specific interface)
- the IP addresses and netmasks for the gateways used by the Trusted and Untrusted interfaces
- on the NetScreen-1000, all configured virtual interfaces on the device

ipsec

Description: Applies to NetScreen-1000 devices only. Use the **get ipsec** command to display the SPI (Security Parameter Index) keys for Virtual Private Networking for a virtual system.

Syntax

get ipsec

Arguments

None.

Availability

This feature is available only on NetScreen-1000 device models.

Example

```
ns1000-> get ipsec
```

See Also

See the **set virtual-system** and **set vpn** commands.

ipsweep-threshold

Description: Use the **get ipsweep-threshold** command to display the ipsweep protection threshold value.

Syntax

get ipsweep-threshold

Arguments

None.

Availability

This feature is available on all NetScreen models.

Examples

To display the ipsweep threshold value:

```
ns1000-> get ipsweep-threshold
```

See Also

See the **set ipsweep-threshold** command.

log

Description: Use the **get log** command to display all the entries in the log table.

Syntax

get log

get log event [start time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>] [end-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>] [include <include_string>] [exclude <exclude_string>] [begin <begin_string>]

get log traffic [policy {<policy_number> | <policy_range>}] [start time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>] [end-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>] [min-duration <hh[:mm[:ss]]>] [max-duration <hh[:mm[:ss]]>] [service <service_name>] [src-ip {<ip_ address> [src-netmask <net_mask>] | <ip_range>}] [src-port {<port_number> | <port_range>}] [dst-ip {<ip_ address> [dst-netmask <net_mask>] | <ip_range>}] [no-rule-displayed]

Arguments

event	Specifies event log entries.
start time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>	Displays event log entries that occurred at and after the time specified—day/month/year hour:minute:second. You can omit the year, in which case the current year is assumed, and you can choose to write the year with either just the last two digits or with all four. The hour, minute, and second may be omitted. Separate the date from the time with a space, a dash, or an underscore: • 12/31/2001 23:59:00 • 12/31/2001-23:59:00 • 12/31/2001_23:59:00
end-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>	Displays event log entries that occurred at and before the time specified.
include <include_string>	Displays event log entries that include the detail specified.
exclude <exclude_string>	Displays event log entries that exclude the detail specified.

begin <begin_string>	Displays event log entries that follow a specified event.
traffic	Specifies traffic log entries.
policy <policy_id> | <policy_id_range>	Displays traffic log entries for an Access Policy specified by its ID number or for several Access Policies specified by a range of ID numbers. The ID number can be any value between 0 and the total number of established Access Policies. To define a range, enter the starting and ending ID numbers using this syntax: <policy_id>-<policy_id>
min-duration <hh[:mm[:ss]]>	Displays traffic log entries for traffic whose duration was longer than or equal to the minimum duration specified.
max-duration <hh[:mm[:ss]]>	Displays traffic log entries for traffic whose duration was shorter than or equal to the maximum duration specified.
service <service_name>	Displays traffic log entries for a specified Service, such as TCP, ICMP, FTP, or Any. The name does not have to be complete; for example, both TC and CP are recognized as TCP. ***Note**: Because TP is recognized as FTP, HTTP, and TFTP, entering TP displays log entries for all three Services. However, no particular Service group may be specified.*
src-ip {<ip_ address> [src-netmask <net_mask>] | <ip_range>	Displays traffic log entries for a specified source IP address or range of source IP addresses. Include the subnet mask for a source IP address to display traffic entries for all IP addresses in the same subnet as the specified source IP address. You cannot specify a source IP range and source subnet mask simultaneously.

src-port {<port_number> | <port_range>}	Displays traffic log entries for a specified port number or range of source port numbers.
dst-ip {<ip_ address> [dst-netmask <net_mask>] | <ip_range>	Displays traffic log entries for a specified destination IP address or range of destination IP addresses. You can specify the subnet mask for a destination IP address, but you cannot specify a destination IP range and destination subnet mask simultaneously.
no-rule-displayed	Displays only traffic log entries, but does not display Access Policy information.

Availability

All arguments for the **get log** command are completely supported on the NetScreen-1000. Other NetScreen device models support only the basic element:

get log

Defaults

If you include no arguments, the **get log** command displays all log entries.

Examples

To display all entries in the log table:

```
ns-> get log
```

To display the entries in the traffic log table for an Access Policy with ID 3:

```
ns-> get log traffic policy 3
```

To display event log entries from 3:00 P.M. on March 4, 2001:

```
ns1000m-> get log event start-time 03/04/01_15:00
```

To display event log entries from 3:00 P.M. on March 4, 2001 to 2:59:59 P.M. on March 6:

```
ns1000m-> get log event start-time “03/04/01 15” end-time “03/06
14:59:59”
```

To display traffic log entries for traffic for a period between 5 minutes and 1 hour:

```
ns1000m-> get log traffic min-duration 00:05:00 max-duration 01:00:00
```

To display traffic log entries for the range of destination IP addresses 164.20.20.5–164.20.20.200:

```
ns1000m-> get log traffic dst-ip 164.20.20.5-164.20.20.200
```

To display traffic log entries from the source port 8081:

```
ns1000m-> get log traffic src-port 8081
```

To display traffic log entries without displaying Access Policy information:

```
ns1000m-> get log traffic no-rule-displayed
```

See Also

See the **clear log** command.

mac-count

Description: Use the **get mac-count** command to display the counters of the packets received and transmitted through the NetScreen-1000 switching board**.**

Syntax

get mac-count

Arguments

None.

Availability

This command is supported only on the NetScreen-1000.

Example

To get the counters:

```
ns-> get mac-count
```

See Also

See the **clear mac-count** command.

Notes

The **get mac-count** command displays all counters of packets received and transmitted through the Switching board, including the various error counters.

mac-learn

Description: Use the **get mac-learn** command to display the entries in the MAC learning table.

Syntax

get mac-learn

Arguments

None.

Availability

This feature is available on all NetScreen device models.

Examples

To display all entries in the MAC learning table:

```
ns-> get mac-learn
```

See Also

See the **clear mac-learn** command.

Notes

The **get mac-learn** command displays the total number of entries in the MAC learning table and details for each entry.

Important: *Use this command only when the NetScreen device is in Transparent mode.*

memory

Description: Use the **get memory** command to display the memory allocation status.

Syntax

get memory

Arguments

None.

Availability

This feature is supported on all NetScreen device models.

Example

To display the memory usage status:

```
ns1000-> get memory
```

Notes

The **get memory** command displays information about the amount of memory allocated, the amount remaining, and the number of fragments.

mpsess

Description: Use the **get mpsess** command to display the session allocation status on the NetScreen-1000 main processing board.

Syntax

get mpsess

Arguments

None.

Availability

This feature is supported only on the NetScreen-1000.

Example

To display the session allocation status on the NetScreen-1000 main processing board:

```
ns1000-> get mpsess
```

Notes

The **get mpsess** command displays the total allocated sessions, the total freed sessions, the total free sessions in the free-session pool, and some debugging counters. It also displays session-related slot information and pseudo-port allocation information.

mip

Description: Use the **get mip** command to display the Mapped IP (MIP) configurations.

Syntax

get mip

Arguments

None.

Availability

This feature is available on all NetScreen device models.

Examples

To display all Mapped IP configuration settings:

```
ns-> get mip
```

See Also

See the **set mip** command.

Notes

The **get mip** command displays the IP address, the host IP address, and the subnet mask address for the Mapped IP.

ntp

Description: Use the **get ntp** command to display the settings for the Network Time Protocol (NTP).

Syntax

get ntp

Arguments

None.

Availability

This feature is available on NetScreen-5 devices at version 1.65 or later and NetScreen-10, -100, and -100p devices at version 2.0 or later.

Examples

To display the settings for NTP on the NetScreen device:

```
ns-> get ntp
```

See Also

See the **set ntp** and **exec ntp** commands.

pki

Description: Use the **get pki** command to show the CA (certificate authority) server's IP address and e-mail address, the certificate administrator's e-mail address, and the RSA key length.

Syntax

get pki ldap

get pki rsa

get pki x509 {crl-refresh | dn | list {ca-cert | cert | local-cert | ns-cert} | pkcs10}

get pki x509 cert-path

Arguments

ldap	Shows the default certificate authority server's address and the default LDAP URL for the certificate revocation list (CRL) retrieval.
rsa	Displays the current RSA key length in bits.
x509	Specifies an International Telecommunications Union (ITU-T) X.509/PKCS digital certificate. (PKCS: Public Key Cryptography Standard)
crl-refresh	Displays the X.509 CRL refresh frequency rate.
dn	Displays the distinguished name on the NetScreen X.509 digital certificate.
list	Displays the X.509 object list loaded in the NetScreen device.
ca-cert	Shows the certificate authority (CA) X.509 certificates currently loaded in the NetScreen device.
cert	Displays the X.509 certificates currently loaded in the NetScreen device.

local-cert	Displays the non-CA (that is, local) X.509 certificates currently loaded in the NetScreen device.
ns-cert	Shows the default X.509 certificate contents used by the NetScreen device.
pkcs10	Shows the destination of the PKCS10 file and generates the file in that location.

Availability

This feature is available on all NetScreen device models at version 2.0 or later.

Examples

To display the RSA key length in bits:

```
ns-> get pki rsa
```

To display the URL and the IP address or name of the default certificate authority's LDAP server:

```
ns-> get pki ldap
```

To display a list of certificate authority (CA) certificates loaded in the NetScreen device:

```
ns-> get pki x509 dn list ca-cert
```

See Also

See the **set pki** command.

policy

Description: Use the **get policy** command to display Access Policy configuration information.

Syntax

get policy [all | incoming | outgoing| todmz| fromdmz | <number>]

Arguments

all	Displays a summary of Access Policies for all the interfaces.
incoming	Displays a summary of Incoming Access Policies.
outgoing	Displays a summary of Outgoing Access Policies.
todmz	Displays a summary of Access Policies to the DMZ interface, if applicable.
fromdmz	Displays a summary of Access Policies from the DMZ interface, if applicable.
number	Displays detailed information for the Access Policy with the ID number <number>.

Availability

This feature is available on all NetScreen device models.

Examples

To display all Access Policy configurations:

```
ns-> get policy all
```

To display all Incoming Access Policy configurations:

```
ns-> get policy incoming
```

To display detailed information for an Access Policy with ID number 5:

```
ns-> get policy 5
```

See Also

See the **set policy** command.

port-scan-threshold

Description: Use the **get port-scan-threshold** command to display the threshold value for port scan protection.

Syntax

get port-scan-threshold

Arguments

None.

Availability

This feature is available on all NetScreen models.

Examples

To display the port-scan threshold value:

```
ns-> get port-scan-threshold
```

See Also

See the **set port-scan-threshold** command.

Notes

The previously used syntax, **get pscan-threshold**, is hidden for backward compatibility.

proto-dist

Description: Use the **get proto-dist** command to display the protocol distribution table.

Syntax

get proto-dist state

get proto-dist user-service

get proto-dist table {bytes|packets}

Arguments

None.

Availability

This feature is available on all NetScreen models.

Examples

To check whether the protocol table is enabled or disabled:

```
ns-> get proto-dist state
```

To display the defined user services :

```
ns-> get proto-dist user-service
```

Service Name	IP Protocol	Port Range
UserDefined_1	ah	4020-4022
UserDefined_2	esp	4023-4030

To list all the protocol table entries:

Hash	Application	Itf	Port	Bytes In	Bytes Out	Last Changed
0x020	rexec	0	512	0	0	1/1/1999 12:02:00
0x021	rlogin	0	512	0	0	1/1/1999 12:34:00

See Also

See the **set proto-dist** command.

route

Description: Use the **get route** command to display entries in the static route table.

Syntax

get route

get route [ip <a.b.c.d>}

Arguments

ip <a.b.c.d>	Displays a specific static route for the IP address <a.b.c.d>.

Availability

This feature is available on all NetScreen device models.

Defaults

The **get route** command displays all entries in the static route table unless a particular IP address is specified.

Examples

To display all the entries in the static route table:

```
ns-> get route
```

To display the static route information for a machine with the IP address 24.1.60.1:

```
ns-> get route ip 24.1.60.1
```

See Also

See the **set route** command.

Notes

The **get route** command displays:

- the IP address, Netmask, Interface, Gateway, Metric, Flag, and Memory

Notes

The Flag value is “8000” for a well-known route generated from the interface IP address and interface gateway.

The Flag value is “0800” if the entry uses the gateway from the interface listed of a specified IP address.

When you specify an IP address, the display appears in this format:

```
<ip-addr>=><interface>/<gateway>,<metric>
```

Use the **get route** command to discover if a packet with a particular IP address is routed by the NetScreen device to the correct interface.

sa

Description: Use the **get sa** command to display the IPSec security associations (SA) when you define VPN policies for a manual VPN.

Syntax

get sa [id <number> | statics]

Arguments

id <number>	Displays a specific IPSec security association (SA) entry with the ID number <number>.
statics	For the NetScreen-1000 only. Displays the following statics of an SA: • **fragment:** the total number of fragmented incoming and outgoing packets • **auth-fail:** the total number of packets for which authentication has failed • **other:** the total number of miscellaneous internal error conditions other than those listed in the auth-fail category • **total bytes:** The amount of active incoming and outgoing traffic

Availability

This feature is available on all NetScreen device models that support encryption. The statics argument is currently supported only on the NetScreen-1000.

Examples

To display all IPSec security association entries:

```
ns-> get sa
```

To display a specific IPSec security association entry with ID number 5:

```
ns-> get sa id 5
```

See Also

See the **set vpn** and **set ike** commands.

scheduler

Description: Use the **get scheduler** command to display the schedules configured for the NetScreen device.

Syntax

get scheduler {all | id <number>}

Arguments

all	Displays all the schedules configured on the NetScreen device.
id <number>	Displays a specific schedule with ID number <number>

Availability

This feature is available on all NetScreen device models.

Examples

To display all schedule definitions:

```
ns-> get scheduler all
```

To display a specific schedule definition with ID number 0:

```
ns-> get scheduler id 0
```

See Also

See the **set scheduler** command.

SCS

Description: Use the **get scs** command to display the user names and keys used to establish a secure command shell (scs) to a NetScreen device from a remote system.

Syntax

get scs

unset scs <key_id>

Arguments

scs	Displays all users and keys. Each key is identified by a number; only the key identification number, not the entire key, necessary when the **unset scs** command is issued.
<key_id>	Each key's identification number, used when unsetting a particular key or user.

Availability

This feature is available on the NetScreen-100 at version 2.0 or later, and on the NetScreen-1000 at version 1.7 and later.

Examples

To display all users and keys for the secure command shell feature on a NetScreen device:

```
ns-> get scs
```

See Also

See the **set scs** command.

service

Description: Use the **get service** command to display the entries in the Service Book.

Syntax

get service [all | <string> | user]

Arguments

all	Displays all the entries in the Service Book.
<string>	Displays a specific Service named <string>.
user	Displays all user-defined Services.

Availability

This feature is available on all NetScreen device models.

Defaults

Using the **get service** command without any arguments yields the same output as does the command **get service all**: all entries in the Service Book are displayed.

Examples

To display all entries in the Service Book:

```
ns-> get service all
```

To display all user-defined entries in the Service Book:

```
ns-> get service user
```

To display a specific service named “ftp”:

```
ns-> get service ftp
```

See Also

See the **set service** command.

session

Description: Use the **get session** command to display the entries in the session table.

Syntax

get session [ip <a.b.c.d>] [protocol <number>] [port <number>] [id <number>]

Arguments

ip <a.b.c.d>	Displays the entries in the session table for the IP address <a.b.c.d>.
protocol <number>	Displays the entries in the session table for a specific protocol number.
port <number>	Displays the entries in the session table for a specific port number.
id <number>	Displays the entries in the session table for a specific session ID number.

Availability

This feature is available on all NetScreen device models.

Defaults

If no arguments are specified, the **get session** command displays information for all entries in the session table.

Examples

To display all the entries in the session table:

```
ns-> get session
```

To display all the entries in the session table for the IP address "172.16.10.92":

```
ns-> get session ip 172.16.10.92
```

To display all the entries in the session table for port 80:

```
ns-> get session port 80
```

To display all the entries in the session table for protocol 5:

```
ns-> get session protocol 5
```

To display the session table entry for the session with ID 5116:

```
ns-> get session id 5116
```

See Also

See the **clear session** command.

Notes

The **get session** command displays:

- the Network Address Translation (NAT) mode
- the sessions in the normal session table
- the sessions in the external session table
- the packets coming into the session's Trusted IP address
- the packets going out of the Untrusted IP address
- the currently active normal and external sessions
- the session's ID number in the session table
- the pseudo port, flag, and PID for the session
- the load-balancing server index
- the vector ID (VID)
- the session timeout specification
- The Gateway IP address
- The session's security association

snmp

Description: Use the **get snmp** command to display the NetScreen device settings for Simple Network Management Protocol (SNMP).

Syntax

get snmp {all | auth-trap | community <name> | settings}

Arguments

all	Displays all communities and their hosts.
auth-trap	Displays the status of SNMP authentication traps.
community <name>	Displays the permissions assigned to the named <SNMP community>.
settings	Displays the name of the contact person, and the name and physical location of the NetScreen device.

Availability

This feature is available for all NetScreen device models.

Examples

To display the settings for an SNMP community named “public”:

```
ns-> get snmp community public
```

To display the settings for all communities:

```
ns-> get snmp all
```

To display the name of the contact person and the name and physical location of the NetScreen device:

```
ns-> get snmp settings
```

See Also

See the **set snmp** command.

syn-flood

Description: Use the **get syn-flood** command to display the current parameter settings for syn-flood protection.

Syntax

get syn-flood

Arguments

None.

Availability

This feature is supported on all NetScreen device models.

Example

To view the syn-flood protection parameters:

```
ns-> get syn-flood
```

Notes

The **get syn-flood** command displays all syn-flood protection parameters, including the syn-flood alarm threshold, queue size, and protection-timeout value.

The **get syn-threshold** command is not supported on the NetScreen-1000.

syslog

Description: Use the **get syslog** command to display the syslog configuration.

Syntax

get syslog

get syslog [config | enable | port | traffic | webtrends]

Arguments

config	Shows whether the syslog mechanism is configured or not.
enable	Shows whether syslog is enabled or not.
port	Displays the port used to communicate with the syslog server.
traffic	Indicates whether the traffic log is sent to syslog.
websense	Shows whether the Websense server is sending messages to the syslog server or not.

Availability

This feature is available on all NetScreen device models.

Examples

To display all syslog configuration information:

```
ns-> get syslog
```

To display whether the syslog mechanism has been configured or not:

```
ns-> get syslog config
```

To display whether the syslog mechanism is enabled or not:

```
ns-> get syslog enable
```

To display the port used to communicated with the syslog server:

```
ns-> get syslog port
```

To display if sending the traffic log through syslog is enabled or not:

```
ns-> get syslog traffic
```

To display if communication with the Websense server is enabled or not:

```
ns-> get syslog websense
```

See Also

See the **set syslog** command.

system

Description: Use the **get system** command to display general system information.

Syntax

get system

Arguments

None.

Availability

This feature is available on all NetScreen devices.

Examples

To display the general system information:

```
ns-> get system
```

See Also

See the **set admin** and **set interface** commands.

tech-support

Description: Use the **get tech-support** command to display system information for troubleshooting the NetScreen device.

Syntax

get tech-support

Arguments

None.

Availability

This feature is available on all NetScreen device models.

Examples

To display information for troubleshooting purposes:

```
ns-> get tech-support
```

timer

Description: Use the **get timer** command to display the current timer settings.

Syntax

get timer

Arguments

None.

Availability

This feature is supported on all NetScreen devices except the NetScreen-5 device model.

Examples

To display the timer settings:

```
ns-> get timer
```

See Also

See also the **set timer** command.

traffic-shaping interface

Description: Use the **get traffic-shaping interface** command to show traffic management information for a named interface. If no name is specified, the information for all interfaces is displayed.

Syntax

get traffic-shaping interface <name>

Arguments

<name>	Defines the name of the interface.

Availability

This feature is available on all devices except the NetScreen-1000 device model.

Defaults

{}

Examples

To display traffic management information for all interfaces:

```
ns-> get traffic-shaping interface
```

udp-threshold

Description: Use the **get udp-threshold** command to display the threshold value for udp flooding protection.

get udp-threshold

Arguments

None.

Availability

This feature is available on all NetScreen models.

Examples

To display the udp threshold value:

```
ns100-> get udp-threshold
```

See Also

See the **set udp-threshold** command.

url

Description: Use the **get url** command to display the URL filtering configuration settings.

Syntax

get url

Arguments

None.

Availability

This feature is available on all NetScreen device models.

Examples

To display information about the URL filtering settings:

```
ns-> get url
```

See Also

See the **set url** command.

Notes

NetScreen monitors the status of the Websense server once each minute. When the Websense server does not respond, this is reported in the Web User Interface (WebUI). Also, an entry is added to the Event Alarm log in the status line of the CLI, and all URL requests are blocked.

All sessions waiting to be acknowledged by the Websense server are listed in the order the request is received. The waiting queue can contain a maximum of 256 requests.

user

Description: Use the **get user** command to display the user authentication database.

Syntax

get user [all | id <number>]

Arguments

all	Displays all the entries in the User database.
id <number>	Displays a specific user with ID <number>.

Availability

This feature is available on all NetScreen device models.

Examples

To display all the entries in the User database:

```
ns-> get user all
```

To display a particular user entry with ID 10:

```
ns-> get user id 10
```

See Also

See the **set user** command.

vip

Description: Use the **get vip** command to display the Virtual IP (VIP) configuration settings.

Syntax

get vip [server | session]

Arguments

server	Displays the load balance status of servers receiving traffic to VIPs.
session	Displays the load balance session table, which shows balanced distribution of currently active VIP sessions.

Availability

This feature is available on all NetScreen device models.

Defaults

If no **server** or **session** is specified, the **get vip** command displays all configured VIPs by default.

Examples

To display all the configured VIPs:

```
ns-> get vip
```

See Also

See the **set vip** command.

vsys

Description: Use the **get vsys** command to display a specific virtual system or all the virtual systems on a NetScreen-1000 device.

Syntax

get vsys

get vsys <virtual_system_name>

Arguments

<virtual_system_name>	Displays the configuration settings for a virtual system with the name <virtual_system_name>.

Availability

This feature is available only on the NetScreen-1000.

Examples

To display all virtual systems on the NetScreen-1000 device:

```
ns-> get vsys
```

To display the subinterface (SIF) identifying number, the name of the VLAN associated with the SIF, and the IP address and subnet mask for a virtual system named “organization3”:

```
ns-> get vsys organization3
```

See Also

See the **set vsys**, **enter vsys**, and **exit** commands.

vlan

Description: Use the **get vlan** command to view information about an established Virtual LAN (VLAN).

Syntax

get vlan [<vlan-name>]

Arguments

vlan-name	Displays this information about the VLAN named: • VLAN identifier (VID) • Priority • Canonical Format Indicator (CFI) • Sub interface IP address and subnet mask

Availability

This feature is only available on the NetScreen-1000.

Defaults

If you do not specify a VLAN name, this command displays this information on all established VLANs:

- VLAN name
- VLAN identifier
- Sub interface name

Examples

To view information about a VLAN named “abc”:

```
ns1000m-> get vlan abc
```

To view information on all established VLANs:

```
ns1000m-> get vlan
```

See Also

See the **set vlan** command.

Notes

Because the NetScreen-1000 currently does not support priority settings for packets, the output for priority is always "0". Also, Canonical Format Indicators (CFI) currently are not configurable, so the output for CFI is always "off".

vpn

Description: Use the **get vpn** command to display all Virtual Private Network (VPN) configurations.

Syntax

get vpn [manual | auto]

get vpn <vpn_name>

Arguments

manual	Displays the VPNs defined to use the Manual Key method for encryption and authentication.
auto	Displays the VPNs defined to use the AutoKey IKE method for encryption and authentication.
<vpn_name>	Displays information for a specific VPN with the name <vpn_name>.

Availability

This feature is available on NetScreen devices that include firewall and VPN encryption features.

Examples

To display all VPN definitions:

```
ns-> get vpn
```

To display a VPN definition named “mary-home”:

```
ns-> get vpn mary-home
```

To display all AutoKey IKE VPN definitions:

```
ns-> get vpn auto
```

To display all Manual Key IKE VPN definitions:

```
ns-> get vpn manual
```

See Also

See the **set vpn** command.

Clear Commands 4

Use the Clear commands to remove data stored in log tables, remove information stored in memory, and remove information stored on the flash card.

active-user

Description: Use the **clear active-user** command to remove a single IP address and its sessions or all IP addresses and their incoming or outgoing sessions passing through the NetScreen device.

Syntax

clear active-user {<a.b.c.d> | all}

Arguments

<a.b.c.d>	Removes the IP address <a.b.c.d> and its sessions from the pool of addresses passing through the NetScreen device.
all	Removes all IP addresses and their sessions from the pool of addresses passing through the NetScreen device.

Availability

This feature is available only on the NetScreen-5 device model.

Examples

To remove a single IP address and its incoming and outgoing sessions from the NetScreen device:

```
ns-> clear active-user ip 10.10.20.24
```

To remove all IP addresses and their sessions from the NetScreen device:

```
ns-> clear active-user all
```

See Also

See the **get active-user** command.

admin

Description: Use the **clear admin** command to remove remote administrator profiles.

Syntax

clear admin user cache

Arguments

None

Availability

This feature is available only on all models.

Examples

To clear the profiles for all remote administrators:

```
ns-> clear admin user cache
```

See Also

See the **get admin** command.

alarm

Description: Use the **clear alarm** command to clear the entries in the alarm table.

Syntax

clear alarm

clear alarm event [end-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>]

clear alarm traffic [policy {<policy_id> [end-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>] | <policy_range> [end-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>]}]
[end-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>]

Arguments

event	Specifies entries in the event alarm table.
end-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>	Clears alarm entries that occurred at and before the time specified—day/month/year hour:minute:second. You can omit the year, in which case the current year is assumed, or write the year with either just the last two digits or with all four. Also, the hour, minute, and second can be omitted. You can separate the date from the time with a space, a dash, or an underscore: • "12/31/2001 23:59:00" • 12/31/2001-23:59:00 • 12/31/2001_23:59:00
traffic	Specifies entries in the traffic alarm table.
policy <policy_id | policy_range>	Clears entries from the traffic alarm table for an Access Policy specified by its ID number or for several Access Policies specified by a range of ID numbers. The ID number can be any value between 0 and the total number of established Access Policies. To define a range, enter the starting and ending ID numbers as follows: <policy_id>-<policy_id>

Availability

This feature is completely supported on all models.

Defaults

If you do not include any arguments, the **clear alarm** command removes all entries from the event alarm table and the traffic alarm table.

Examples

To clear all entries in the event alarm and traffic alarm tables:

```
ns-> clear alarm
```

To clear all entries in the event alarm table:

```
ns-> clear alarm event
```

To clear all entries in the traffic alarm table:

```
ns-> clear alarm traffic
```

To clear alarm entries for an Access Policy with ID number 4 from the traffic alarm table:

```
ns-> clear alarm traffic policy 4
```

To clear alarm entries for Access Policies within the ID range of 5–8 from the traffic alarm table:

```
ns1000m-> clear alarm traffic policy 5-8
```

To clear alarm entries at or before July 15, 2000 11:00 A.M. from the traffic alarm table:

```
ns1000m-> clear alarm traffic end-time 07/15/00-11:00
```

See Also

See the **get alarm** command.

arp

Description: Use the **clear arp** command to clear entries in the Address Resolution Protocol (ARP) table.

Syntax

clear arp

Arguments

None.

Availability

This feature is supported on all NetScreen device models.

Examples

To clear the entries in the ARP table:

```
ns-> clear arp
```

See Also

See the **get arp** command.

auth

Description: Use the **clear auth** command to clear the user authentication information stored in memory.

Syntax

clear auth [history]

Arguments

history	Clears the user authentication history.

Availability

This feature is supported on all NetScreen device models.

Examples

To clear all entries in the authentication table:

```
ns-> clear auth
```

To clear user authentication history:

```
ns-> clear auth history
```

See Also

See the **get auth** and **set auth** commands.

counter

Description: Use the **clear counter** command to clear interface and flow counters.

Syntax

clear counter {flow | ha | interface}

Arguments

flow	Specifies counters for packets inspected at the flow level. A flow-level inspection examines various aspects of a packet to gauge its nature and intent.
ha	Specifies counters for packets transmitted across a high-availability (HA) link between two NetScreen devices. An HA-level inspection keeps count of the number of packets and packet errors.
interface	Specifies counters for packets inspected at the interface level. An interface-level inspection checks for packet errors and monitors the quantity of packets in light of established threshold settings.

Availability

This feature is supported on all NetScreen device models.

Examples

To clear interface counters:

```
ns1000-> clear counter interface
```

To clear flow counters:

```
ns1000-> clear counter flow
```

See Also

See the **get counter** command.

dbuf

Description: Use the **clear dbuf** command to clear the contents of the debug buffer.

Syntax

clear dbuf

Arguments

None.

Availability

This feature is supported on all NetScreen device models.

Examples

To clear the contents of the debug buffer:

```
ns-> clear dbuf
```

See Also

See the **get dbuf** and **set console** commands.

dhcp

Description: Use the **clear dhcp** command to release the IP address the NetScreen device is using for its Untrusted interface. This IP address is obtained from the DHCP server. Or to return a specific IP address to the Dynamic Host Configuration Protocol (DHCP) pool of IP addresses, or to return all IP addresses to the pool.

Syntax

clear dhcp {client ip | server ip {<a.b.c.d> | all}}

Arguments

client ip	Release the IP address assigned to the NetScreen device.
server ip	Reset the server IP address.
a.b.c.d	Returns the IP address <a.b.c.d> to the DHCP server pool.
all	Returns all IP addresses to the DHCP server pool.

Availability

This feature is supported on the NetScreen-5 at version 1.63 or later and the NetScreen-10 at version 2.0 or later.

Examples

To release the IP address that the NetScreen device obtained from the DHCP server:

```
ns-> clear dhcp client ip
```

To return a specific IP address of 209.122.17.1 to the DHCP server pool:

```
ns-> clear dhcp server ip 209.122.17.1
```

To return all IP addresses to the DHCP server pool:

```
ns-> clear dhcp server ip all
```

See Also

See the **get dhcp, set dhcp**, and **exec dhcp client renew** commands.

dns

Description: Use the **clear dns** command to clear the dns cache.

Syntax

clear dns

Arguments

None.

Availability

This feature is supported on all NetScreen device models.

Examples

To clear the dns cache:

```
ns-> clear dns
```

See Also

See the **get dns, set dns**, and **exec dns** commands.

file

Description: Use the **clear file** command to delete a specific file from the flash card memory.

Syntax

clear file <string>

Arguments

<string>	Deletes the file with the name <string> from the flash card memory.

Availability

This feature is supported on all NetScreen device models.

Examples

To delete a file named “myconfig” in the flash card memory:

```
ns-> clear file flash:myconfig
```

See Also

See the **get file** command.

ike cookie

Description: Use the **clear ike cookie** command to clear the entries in the Internet Key Exchange (IKE) cookie table.

Syntax

clear ike cookie [<a.b.c.d> | all]

Arguments

a.b.c.d	Clear the entries for IP address a.b.c.d in the IKE cookie table.
all	Clears all entries in the IKE cookie table.

Availability

This feature is supported on all NetScreen device models.

Examples

To clear all entries in the IKE cookie table:

```
ns-> clear ike cookie all
```

To clear entries for IP address 100.2.30.1 in the IKE cookies table:

```
ns-> clear ike cookie all 100.2.30.1
```

See Also

See the **get vpn** command.

log

Description: Use the **clear log** command to clear the entries in the log table.

Syntax

clear log event [end-time <mm/dd [/yy | yyyy] [- hh[:mm[:ss]]]>]

clear log traffic [policy {<policy_id> [end-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>] | <policy_range> [end-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>]}] [end-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>]

Arguments

event	Clears event entries from the log.
end-time <dd/mm[/yy | yyyy] [hh[:mm[:ss]]]>	Clears log entries that occurred at and before the time specified—day/month/year hour:minute:second. You can omit the year, in which case the current year is assumed, or write the year with either just the last two digits or with all four. Also, the hour, minute, and second can be omitted. You can separate the date from the time with a space, a dash, or an underscore: • "12/31/2001 23:59:00" • 12/31/2001-23:59:00 • 12/31/2001_23:59:00
traffic	Clears traffic entries from the log.
policy <policy_id> | <policy_range>	Clears the traffic entries in the log table for the Access Policy with ID number <policy_id> or for Access Policies within the range of specified ID numbers.

Availability

This feature is completely supported on the NetScreen-1000. All other NetScreen device models support these elements of the **clear log** command:

Defaults

If you do not include any arguments, the **clear log** command removes all entries from the event and traffic logs.

Examples

To clear entries in the event log:

```
ns-> clear log event
```

To clear entries in the traffic log:

```
ns-> clear log traffic
```

To clear entries for an Access Policy with ID number 4 in the traffic log:

```
ns-> clear log traffic policy 4
```

To clear event log entries that occurred at or before 5:00 P.M. April 10, 2000:

```
ns1000m-> clear log event end-time 04/10/00-17:00
```

To clear traffic log entries that occurred at or before 3:15 P.M. on June 3, 2001 for Access Policies ranging from ID 5–10:

```
ns1000m-> clear log traffic policy 5-10 end-time 06/03/01 15:15
```

See Also

See the **get log** command.

mac-count

Description: Use the **clear mac-count** command to clear all counters of the packets received and transmitted through the NetScreen-1000 Switching board.

Syntax

clear mac-count

Arguments

None.

Availability

This feature is supported on the NetScreen-1000.

Example

To clear the packet counters:

```
ns1000-> clear mac-count
```

See Also

See the **get mac-count** command.

mac-learn

Description: Use the **clear mac-learn** command to clear the entries in the Media Access Control (MAC) learning table.

Syntax

clear mac-learn [stats]

Arguments

stats	Clears MAC learning table statistics.

Availability

This feature is supported on all NetScreen device models.

Examples

To clear the statistics in the MAC learning table:

```
ns-> clear mac-learn stats
```

See Also

See the **get mac-learn** command.

This command only functions when the NetScreen device is in Transparent mode.

node_secret

Description: Use the **clear node_secret** command when the NetScreen device is using SecurID to authenticate users and is not communicating properly with the ACE Server.

Syntax

clear node_secret

Arguments

None.

Availability

This feature is available on all NetScreen device models.

Defaults

None.

Examples

To clear and prompt the NetScreen device to request the node secret from the ACE server:

```
ns-> clear node_secret
```

Notes

If you remove, move, or reconfigure a NetScreen device, it may stop communicating with the ACE Server. If this happens, the ACE Server log displays a message that says the node secret is invalid. Use the **clear node_secret** command to re-synchronize communication between the two.

The node secret bit tells the ACE server to negotiate an encryption secret as soon as possible. When the first successful authentication happens, the ACE server will negotiate an encryption secret. This node secret is stored in the NetScreen device in nonvolatile memory.

If the NetScreen device's Self IP (or system IP or interface IP) ever changes, the node secret must be cleared on the NetScreen device as well as on the ACE Server.

pppoe

Description: Use the **clear pppoe** command to reset PPPoE statistical registers.

Syntax

clear pppoe

Arguments

None.

Availability

This feature is available on NetScreen-5 device models.

Examples

To reset the statistics for your PPPoE connection:

```
ns1000 -> clear pppoe
```

See Also

See **get pppoe**, **exec pppoe**, and **set pppoe** commands.

sa

Description: Use the **clear sa** command to clear the IKE value for the specified Security Association.

Syntax

clear sa {<number>}

Arguments

<number>	The SA index number.

Availability

This feature is available on all NetScreen models.

Examples

To clear the IKE value for SA 2:

```
ns1000 -> clear sa 2
```

See Also

See the **clear sa-statistics** and the **get sa** commands.

sa-statistics

Description: Use the **clear l2tp** command to close specified calls in an L2TP tunnel.

Syntax

clear sa-statistics [id <number>]

Arguments

id <number>

Availability

This feature is available on all NetScreen models.

Examples

To clear the SA statistics for SA 2:

```
ns1000 -> clear sa-statistics id 2
```

To clear the SA statistics for all Security Associations:

```
ns1000 -> clear sa-statistics
```

See Also

See the **clear sa** and the **get sa** commands.

session

Description: Use the **clear session** command to clear the entries in the session table.

Syntax

clear session

Arguments

None.

Availability

This feature is supported on all NetScreen device models.

Examples

To clear all entries in the session table:

```
ns-> clear session
```

See Also

See the **get session** command.

Miscellaneous Commands 5

This chapter contains miscellaneous commands that do not fit into the other categories in previous chapters.

enter vsys

Description: Use the **enter vsys** command to enter a virtual system on the NetScreen-1000.

Syntax

enter vsys <virtual_system_name>

Arguments

virtual system name	Defines the virtual system to be entered.

Availability

This feature is available only on the NetScreen-1000.

Examples

To enter the virtual system named “cloister”:

```
ns1000-> enter vsys cloister
```

See Also

See the **set vsys** command.

exec dns

Description: Use the **exec dns** command to refresh all DNS entries.

Syntax

exec dns refresh

Arguments

None.

Availability

This feature is available on all NetScreen models.

Examples

To refresh DNS entries:

```
ns-> exec dns refresh
```

See Also

See the **set dns**, **get dns**, and **clear dns** commands.

exec dhcp client renew

Description: Use the **exec dhcp client renew** command to renew the lease for an IP address from a DHCP server.

Syntax

exec dhcp client renew

Arguments

None.

Availability

This feature is available on the NetScreen-5 at version 1.65 or later and the NetScreen-10 at version 2.0 or later.

Examples

To renew a lease for an IP address from the DHCP server immediately:

```
ns-> exec dhcp client renew
```

See Also

See the **set dhcp client**, **get dhcp client**, and **clear dhcp client ip** commands.

Notes

The **exec dhcp client renew** command is useful, for example, if the DHCP server has gone down. A system administrator who knows this can immediately request a new lease for the NetScreen device once the DHCP server reboots. The NetScreen device may or may not obtain the same IP address it was using.

exec ha file-sync

Description: Use the **exec ha file-sync** command to copy files from a master unit to a slave unit. Execute this command in the master unit.

Syntax

exec ha file-sync [file_name]

Arguments

file_name	Specifies the name of a particular file to copy from the master unit to a slave unit. Executing this command without specifying a file name copies all the files.

Availability

This feature is available on the NetScreen-100 at version 2.0 or later and the NetScreen-1000.

Examples

To copy all files from the master unit to a slave unit:

```
ns1000-> exec ha file-sync
```

To copy the environment variable records from the master unit to a slave unit:

```
ns100-> exec ha file-sync envar.rec
```

See Also

See the **set ha** command.

exec ntp update

Description: Use the **exec ntp update** command to immediately update the NetScreen device clock using Network Time Protocol (NTP).

Syntax

exec ntp update

Arguments

None.

Availability

This feature is available on NetScreen-5 devices at version 1.65 or later and NetScreen-10, -100, and -100p devices at version 2.0 or later.

Examples

To update the NetScreen device time by synchronizing it with the NTP server:

```
ns-> exec ntp update
```

See Also

See the **set ntp** and **get ntp** commands.

exec pki

Description: Use the **exec pki** commands to manage RSA key pair generation and X.509 certificate requests and removals for public-key infrastructure (PKI).

Syntax

exec pki {dsa new-key <number> | rsa new-key <number> | x509 {delete <number> | pkcs10 | tftp <a.b.c.d> {cert-name <name> | crl-name <name>

Arguments

dsa new-key <number>	Generates a new DSA key pair with a specified bit length.
rsa new-key <number>	Generates a new RSA key pair with a specified bit length.
x509 pkcs10	Generates a PKCS10 file for a X.509 certificate request for the NetScreen device.
x509 delete <number>	Removes a specified X.509 certificate from a NetScreen device.
x509 tftp <a.b.c.d>	Upload the specified certificate or CRL file for the specified TFTP server.
cert-name <name>	Specifies the name of the certificate.
crl-name <name>	Specifies the name of the revocation list.

Availability

This feature is supported on all NetScreen devices at version 2.0 or later.

Examples

To create a new RSA key pair with a length of 1024 bits:

```
ns-> exec pki rsa new-key 1024
```

To remove an X.509 certificate with the ID number 3 from the NetScreen device:

```
ns-> exec pki x509 delete 3
```

See Also

See also the **set pki** and **get pki** commands.

exec pppoe

Description: Use the **exec pppoe** command to set up or take down a PPPoE connection.

Syntax

exec pppoe connect | disconnect

Arguments

None

Availability

This feature is available on NetScreen-5 device models.

Examples

To setup your pppoe connection:

```
ns1000-> exec  pppoe
```

See Also

See **get pppoe**, **set pppoe**, and **clear pppoe** commands.

exit

Description: (1) Use the **exit** command to exit from the console and command-line interface; (2) Additionally, for a NetScreen-1000 device, use the **exit** command to exit from a virtual system console.

Syntax

exit

Arguments

None.

Availability

This feature is supported on all NetScreen device models. However, virtual systems are only supported on the NetScreen-1000.

Examples

To log off the console:

```
ns-> exit
```

To log off the virtual system console on the NetScreen-1000:

```
ns(organizationA)-> exit
```

See Also

See the **set vsys** command.

Notes

All devices

After using the **exit** command, you must log back in to the console to configure a NetScreen device.

NetScreen-1000

After using the **exit** command, you must log back in to the virtual system console to configure a NetScreen-1000 device.

If you use the **exit** command as *root*, you exit the virtual system and remain logged in to the console.

If you use the **exit** command at the console, you log off the console.

ping

Description: Use the **ping** command to check the network connection to another system.

Syntax

ping <a.b.c.d> [from {trust-ip | {mip <e.f.g.h>}}]

Arguments

<a.b.c.d>	Pings the host with IP address <a.b.c.d>
from {trust-ip | {mip <e.f.g.h>}}]	NetScreen-5 only. Defines the source IP to which the ping will reply. Because this destination is on the untrusted side, the source IP can only be the Mapped IP address or an untrusted interface IP address. Also known as “extended ping.”

Availability

This feature is supported on all NetScreen device models.

Examples

To ping a host with IP address 209.192.11.2:

```
ns-> ping 209.192.11.2
```

To ping a host with IP address 209.192.11.2 and have the results sent to 10.1.1.3:

```
ns-> ping 209.192.11.2 from mip 10.1.1.3
```

Notes

Extended **ping** allows the user to ping a host on the untrusted network from any of the MIPs or from the trusted interface IP.

reset

Description: Use the **reset** command to reboot the NetScreen device.

Syntax

reset

Arguments

None.

Availability

This feature is supported on all NetScreen device models.

Examples

To reboot a NetScreen device:

```
ns-> reset
```

save

Description: Use the **save** command to save the NetScreen device configuration settings either to the flash card memory or to a Trivial File Transfer Protocol (TFTP) server connected to the Trusted interface on the NetScreen device.

NetScreen-100 and NetScreen-1000 only: When you add a second device for high availability, you use the **save ha-master** command on the Slave unit to save the configuration settings from the Master unit to the Slave unit in order to pass control messages and synchronize the two devices.

NetScreen-1000 only: Use the **save vsys** command to save a single virtual system setting, or all the virtual system settings on the NetScreen device to a file or to the TFTP server.

Syntax

save

save [config {from | to} tftp <a.b.c.d> <filename> [append]] [to {slot1 | slot2}:<file_name_new>]

save [software from tftp <a.b.c.d> <filename>]

save config {ha-master | ha-slave}

save [vsys <virtual_system_name> | all] [tftp <a.b.c.d> <filename>]

Arguments

config to tftp <a.b.c.d> <filename>	Saves the configuration settings to a TFTP server with the IP address <a.b.c.d> and names the file <filename>.
config from tftp <a.b.c.d> <file_name>	Downloads a configuration file named <file_name> from the TFTP server with the IP address <a.b.c.d> overwriting the current configuration file on the NetScreen device.
config from tftp <a.b.c.d> <file_name> append	Downloads a configuration file named <file_name> from the TFTP server with the IP address <a.b.c.d>. Appends the configuration information to the current configuration file on the NetScreen device.

software from tftp <a.b.c.d> <file_name>	Downloads the software file with the name <file_name> from the TFTP server with the IP address <a.b.c.d> to the NetScreen device.
config ha-master	At the Slave unit console, use this command to pass the configuration settings from the Master unit to the Slave unit. Reset the Slave unit after the configuration settings are passed.
config ha-slave	At the Master unit console, this command forces the Slave unit to execute a save command that stores the configuration settings in the Slave unit.
save vsys <virtual_system_name> tftp <a.b.c.d> <filename>	Applies only to NetScreen-1000. This command saves the configuration settings for virtual system <virtual_system_name> to the TFTP server with an IP address <a.b.c.d> and names the configuration file <filename>.
save vsys <virtual_system_name> <filename>	Applies only to NetScreen-1000. This command saves the configuration settings for virtual system <virtual_system_name> to a file <filename>.
save all tftp <a.b.c.d> <filename>	Applies only to NetScreen-1000. This command saves the configuration settings for all virtual systems on the device to the TFTP server with an IP address <a.b.c.d> and names the configuration file <filename>.
{slot1 | slot2}	Applies only to NetScreen-1000. This variable specifies which of the two PCMCIA cards in the device model will store the configuration file that is downloaded from the TFTP server.
<file_name_new>	Applies only to NetScreen-1000. Refers to the file containing the configuration information from the TFTP server that will be stored in one of the device's PCMCIA cards.

Availability

This feature is supported on all NetScreen device models.

The **save vsys** command applies only to NetScreen-1000 device models.

Examples

To save the current configuration settings to the flash card memory:

```
ns-> save
```

To save the current configuration settings to a file named “myconfig” on a TFTP server with IP address 184.23.11.9:

```
ns-> save to tftp 184.23.11.9 myconfig
```

To download a configuration file named “my_config” from a TFTP server with the IP address 171.12.30.10 and *overwrite* the current saved configuration settings on the NetScreen device:

```
ns-> save config from tftp 171.12.30.10 my_config
```

To download a configuration file named “my_config” from a TFTP server with the IP address 171.20.30.10 and *append* the current configuration settings on the NetScreen device:

```
ns-> save config from tftp 171.20.30.10 my_config append
```

To download the software file “ns5.165” from a TFTP server with the IP address 170.20.20.10:

```
ns-> save software from tftp 170.20.20.10 ns5.165
```

To download a configuration file named “my_config” from a TFTP server with the IP address 171.12.30.10 to the PCMCIA card in slot 1 of the NetScreen-1000 device and give it the name “new_config”:

```
ns-> save config from tftp 171.12.30.10 my_config to slot1:new_config
```

To download a configuration file named “ns_cnfg” from a TFTP server at 156.24.54.9 to a Virtual System named “cyborg”:

```
ns1000-> save config tftp 156.24.54.9 ns_cnfg #vsys cyborg
```

To copy a configuration file named “cnfg5” from the PCMCIA card in slot 1 to a file named “ns_cnfg5” in a TFTP server at 125.34.156.9:

```
ns1000-> save config from slot 1 cnfg5 to tftp 125.34.156.9 ns_cnfg
```

See Also

See the **get config** command.

Notes

The TFTP server option is available only with firmware version 1.6 or above.

The NetScreen-5 device saves to the TFTP server. The NetScreen-10, -100, and -1000 save to either the flash memory card or to a TFTP server.

snoop

Description: Use the **snoop** command to display the current filter settings and review specified traffic flows.

Syntax

snoop info

snoop ethernet {<number> | [arp]} | ip {[proto <number>] [src-ip <a.b.c.d>] [src-port <number>] [dst-ip <a.b.c.d>] [dst-port <number>]}

snoop direction {both | incoming | outgoing}

snoop interface {all | trust | untrust | dmz}

Arguments

info	Displays the current filter settings.
ethernet <number>	Specifies the 2-byte value in the ethernet header. (For an IP packet, it is 0x800. For an ARP packet, it is 0x806.)
arp	Specifies the Address Resolution Protocol (ARP), a low-level TCP/IP protocol used to obtain the MAC address for a machine when only its IP address is known.
ip proto <number>	Specifies the protocol number in IP packet headers, allowing you to direct snooping by protocol type. (For example, TCP is 6, UDP is 17, and IPSec is 50.)
ip src-ip <a.b.c.d>	Specifies the source IP address of the packets to be snooped.
ip src-port <number>	Specifies the source IP port number of the packets to be snooped.
ip dst-ip <a.b.c.d>	Specifies the destination IP address of the packets to be snooped.
ip dst-port <number>	Specifies the destination IP port number of the packets to be snooped.
direction	Specifies the packet flow to which snoop is applied: both incoming and outgoing traffic, incoming traffic only, or outgoing traffic only.

interface {all | trust | untrust | dmz}	Specifies the interface traffic to which snoop is applied: all interfaces, the Trusted interface, the Untrusted interface, or the DMZ interface (available on the NetScreen-5).

Availability

This feature is available on the NetScreen-5, -10, and -100 at version 2.0, and the NetScreen-1000 at version 1.7.

Defaults

This feature is off by default. When enabled, the default direction is “incoming” and the default interface is “all.”

Examples

To snoop ARP packets only:

```
ns1000-> snoop ethernet arp
```

To snoop TCP traffic only:

```
ns1000-> snoop ip proto 6
```

To snoop all packets transmitted to IP address 209.122.17.40:

```
ns1000-> snoop ip dst-ip 209.122.17.40
```

To snoop all outgoing packets:

```
ns1000-> snoop direction outgoing
```

Notes

To turn off the snoop feature, press the ESC key.

sock

Description: Use the **get sock** command to display the socket status for the system.

Syntax

get sock

Arguments

None.

Availability

This feature is available on all NetScreen device models.

Example

To display the socket status for the system:

```
ns1000 -> get sock
```

unset all

Description: Use the **unset all** command to remove all the configuration settings you added and restore the NetScreen device to its factory default settings.

Syntax

unset all

Arguments

None.

Availability

This feature is supported on all NetScreen device models.

Examples

To restore the NetScreen device to its default factory settings:

```
ns-> unset all
```

See Also

See the unset counterpart for each **set** command.

Index

A

B

C

D

E

F

G

H

I

L

M

N

P

R

S

T

U

V

W